Regional Partnerships: Enabling Regional Critical Infrastructure Resilience

Sponsored by the
Regional Consortium Coordinating Council (RCCC)

Version #1

March 2011

Table of Contents

Appendices:

Regional Partnerships: Enabling Regional Critical Infrastructure Resilience

I. Executive Summary

Summary

In April 2010, the Regional Consortium Coordinating Council (RCCC) initiated a study with the Department of Homeland Security (DHS) Office of Infrastructure (IP) to examine regional critical infrastructure partnerships in the United States, recognizing that partnerships among regional critical infrastructure stakeholders play an important role in promoting and enhancing regional resilience. The publication of the study supports the RCCC's mission of strengthening regional collaboration to enhance protection, response, recovery, and resilience of critical infrastructure throughout the Nation and the increased emphasis IP has placed on regional approaches to critical infrastructure resilience and protection to support the public-private sector framework established by the National Infrastructure Protection Plan (NIPP).

The RCCC recognizes that partnerships play a critical role in promoting and enhancing regional resilience and was interested in learning about the specific nature of these regional critical infrastructure partnerships by answering three key questions:

- Which regional critical infrastructure partnerships are active and what are their main focus areas and concerns?
- What are the main characteristics of effective regional critical infrastructure partnerships?
- How do effective regional partnerships enable activities that support and enhance regional critical infrastructure resilience?

The information obtained during the data collection and identification of specific case study phase of the study revealed a range of potential answers to these questions. This study is intended to inform readers, rather than to prescribe specific actions or policies. It serves as a guide for both newly developing and mature regional critical infrastructure partnerships.

Summary of Findings

It is widely accepted that regional stakeholders must work together, share information, plan and prepare for disasters and emergencies, and train and conduct exercises to test those plans. The study identifies these basic capabilities as well as the challenges that regional critical infrastructure partnerships face, to include developing collaboration across multiple jurisdictions, establishing a common understanding of regional risk, and overcoming the complex challenge of identifying and mitigating regional critical infrastructure interdependencies.

The value of the study is not in identifying these challenges and capabilities but in demonstrating how regional critical infrastructure partners are implementing innovative solutions to common problems and difficult challenges. This study identifies some basic capabilities that contribute to regional resilience and provides insight into how regional partnership leaders can work with regional stakeholders to make critical infrastructure and their region more resilient against all hazards. Although these activities are undertaken for a variety of reasons, *in toto,* they can be

seen as "regionalizing" the NIPP based on their unique regional circumstances and stakeholder needs.

Each regional partnership takes a unique approach toward building and sustaining regional resilience. Regardless of the approach, interview participants repeatedly highlighted five capabilities they believe to be essential to a resilient region:

- Regional stakeholders **engage in partnerships and collaborate** to promote resilience of regionally important critical infrastructure.
- Regional stakeholders **share information and intelligence** through an information sharing network.
- Regional stakeholders **assess critical infrastructure risks and identify interdependencies**.
- Critical infrastructure owners and operators are **integrated into regional emergency response and recovery planning and operations**.
- Regional stakeholders **participate in education and training.**

Significant challenges complicate the achievement of each of the above capabilities, and regional partnership organizations adopt various approaches to meet those challenges. While there is great variety and ingenuity in the solutions used to overcome these challenges, regional partnerships often face similar challenges when developing these capabilities in their region. Each of the capabilities is supported by a case study, based on interviews with regional participants, demonstrating how regional partnership organizations meet and address many of the challenges common to enhancing regional resilience.

Regional Partnerships:
Enabling Regional Critical Infrastructure Resilience

II. Introduction

Critical Infrastructure Regionalism

In recent years, the President, Congress, and leadership within the Department of Homeland Security (DHS) have placed an increasingly greater emphasis on the resilience of critical infrastructure[1] and the ability of regional stakeholders to prepare for and respond to terrorist attacks and natural disasters. This progression was largely motivated by the catastrophic critical infrastructure failures in New Orleans following Hurricane Katrina, and also by an increasing recognition of the limitations of the dominant critical infrastructure protection strategy. The Quadrennial Homeland Security Review (QHSR)[2] identified these issues and established the following two relevant objectives:

1. **Make critical infrastructure resilient:** Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.
2. **Promote regional response capacity:** Promote mutual aid agreements for response requirements that exceed local capacity.

Todd Keil, DHS Assistant Secretary for Infrastructure Protection (IP), is implementing these tenets. To this end, Assistant Secretary Keil is refocusing IP by placing greater stress on regional approaches to critical infrastructure resilience and protection, an approach that will complement the national framework established by the National Infrastructure Protection Plan (NIPP).[3]

A regional resilience and overarching risk management focus promotes closer collaboration, integration, and coordination among stakeholders in regions across the country. This regional focus supports the goal of enhancing overarching national-level critical infrastructure resilience. Regional stakeholders include not only Federal, State, local, tribal, and territorial governments, but also critical infrastructure owners and operators, as well as non-governmental organizations, emergency responders, academia, community leaders, faith-based organizations, and law enforcement personnel.

Critical infrastructure assets and systems provide essential regional services and functions, such as electricity, water, food, communications, transportation, finance, and healthcare. Regional resilience requires these commodities and services to continue in the face of disruptions. Critical

[1] It should be noted that this study explicitly focuses on resilience of critical infrastructure, rather than community or other types of resilience. See the following page for further explanation.
[2] "The primary purpose for the QHSR is to outline the strategic framework to guide the activities of participants in homeland security toward a common end. The report identifies the principal goals, essential objectives, and key strategic outcomes necessary for the strategic approach to succeed." QHSR was released in February 2010.
[3] http://www.executivegov.com/2010/04/todd-keil-of-dhs-talks-partnerships-priorities/
http://cip.gmu.edu/archive/cip_report_9.2.pdf

infrastructure owners and operators play a significant role in regional response operations, and they can provide valuable assistance to law enforcement, regional emergency responders, and government representatives during an emergency.

Purpose of the Study

In April 2010, the Regional Consortium Coordinating Council[4] (RCCC) and IP initiated a study to examine current regional critical infrastructure partnerships in the United States. Typically, these partnerships are comprised of regional stakeholders from both the public and private sectors and may focus on a single metropolitan area or community or span multiple cities, States, and even across international boundaries. Consistent with the RCCC's mission "to strengthen regional collaborations that enhance protection, response, recovery, and resilience of the Nation's critical infrastructure and key resources,"[5] this study highlights the activities of regional partnerships that facilitate regional critical infrastructure resilience.

DHS and the RCCC both recognize that partnerships among regional critical infrastructure stakeholders play an important role in promoting and enhancing regional resilience. However, the RCCC was interested in learning more about the specific nature of these regional critical infrastructure partnerships by answering three key questions:

- Which regional critical infrastructure partnerships are active and what are their main focus areas and concerns?
- What are the main characteristics of effective regional critical infrastructure partnerships?
- How do effective regional partnerships enable activities that support and enhance regional critical infrastructure resilience?

The information obtained during the data collection phase of the study revealed a range of potential answers to the questions above. However, this study is intended to inform readers, rather than prescribe specific actions or policies. It serves as a guide for both newly developing and mature regional critical infrastructure partnerships by:

- Creating awareness of other partnerships and their activities;
- Inspiring new ideas and models, which promote critical infrastructure resilience;
- Providing options for overcoming common challenges; and
- Connecting regional critical infrastructure stakeholders so they can share information and collaborate with each other.

It is widely accepted that regional stakeholders must work together, share information, plan and prepare for disasters and emergencies, and train and conduct exercises to test those plans. The

[4] The RCCC formed in 2008 to provide members of regional partnerships across the U.S. that focus on critical infrastructure protection and regional resilience with a way to share best practices and increase collaboration. The RCCC serves as a single point of contact for the Federal government, particularly DHS.

[5] Regional Consortium Coordinating Council Executive Charter.

study identifies these basic capabilities as well as the challenges that regional critical infrastructure partnerships face. The value of the study is not in identifying these challenges and capabilities, but in demonstrating how regional critical infrastructure partners are implementing innovative solutions to common problems and difficult challenges. Regional stakeholders and those individuals running or forming regional partnerships can then leverage this information to enhance their own partnership operations. This study identifies some basic capabilities that contribute to regional resilience. Moreover, it provides insight into how regional partnership leaders can work with regional stakeholders to make critical infrastructure and their region more resilient against all hazards.

Scope and Methodology

This report was based on more than 30 90-minute interviews with regional partnership stakeholders, representing 11 multi-State, nine State-wide, and 10 local/metropolitan area partnerships across 40 States within all 10 FEMA regions. During each interview, the RCCC asked participants to consider the following four questions:

1. How does each partnership support the resilience of its region's critical infrastructure?
2. What is the role of regional critical infrastructure partnerships?
3. What are the challenges and how have partnerships met and overcome these challenges?
4. What makes a region's critical infrastructure resilient?

Participants described the creation of their partnerships, the geographic area their partnerships encompass, and the contribution their activities make to enable regional critical infrastructure resilience. A complete list of the participating organizations is contained in *Appendix A: Compendium of Regional Partnerships*. *Appendix A* provides key information for each of the participating regional organizations, including: region of focus, date founded, type of partnership (operational, educational, and/or networking), representative contact information (phone, email, partnership Web site), and a description of the partnership mission including a list of key partnership activities and initiatives.

While the structure, size, and scope of regional infrastructure partnerships vary, all partnerships promote critical infrastructure resilience through a wide range of activities. The RCCC did not attempt to interview every regional critical infrastructure partnership in the United States. Instead, the RCCC reached out to a representative group in different parts of the country. In addition, this study does not make assumptions or reach conclusions about what constitutes a region and what regional stakeholders consider to be their region's critical infrastructure assets.

For the purposes of this study, regions can be large urban areas, small communities, or multi-State entities. The geographic scope of partnership "regions" varies significantly, with some partnerships spanning large multi-State regions and others focusing on single metropolitan areas. While the organizational structure and key initiatives of regional critical infrastructure partnerships vary, all partnerships foster engagement and collaboration between critical infrastructure owners and operators, government, and other key regional stakeholders.

The RCCC did not develop a new definition or interpretation of critical infrastructure resilience, and interview participants rarely raised the issue. The study uses the NIPP definition of

resilience: "The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions."[5]

[5] 2009 NIPP, p11.

III. Enabling Regional Resilience

Regional Capabilities

This report highlights several regional partnerships and the innovative ways they have enhanced the resilience of critical infrastructure within specific geographic areas. Although these activities are undertaken for a variety of reasons, *in toto*, they can be seen as "regionalizing" the NIPP, based on their unique regional circumstances and stakeholder needs. Each regional partnership takes a unique approach toward building and sustaining regional resilience. For example, the Pacific Northwest Economic Region (PNWER) developed the following "regional resilience tautology" to help guide and motivate its partnership's mission and objectives:

- Resilient assets and infrastructures require resilient regions.
- Resiliency requires understanding which assets are critical in any specific scenario.
- Understanding criticality depends upon understanding the interdependencies between and among critical infrastructures (*i.e.*, criticality is dynamic).
- Understanding interdependencies requires cross sector information sharing.
- Cross sector and public/private information sharing requires the creation of an environment of trust where stakeholders feel "safe" to share their vulnerabilities.

Regardless of the approach, interview participants repeatedly highlighted five capabilities they believe to be essential to a resilient region. The study's structure is consistent with the following five capabilities:

1. Regional stakeholders engage in partnerships and collaborate to promote resilience of regionally important critical infrastructure.
2. Regional stakeholders share information and intelligence through an information sharing network.
3. Regional stakeholders assess critical infrastructure risks and identify interdependencies.
4. Critical infrastructure owners and operators are integrated into regional emergency response and recovery planning and operations.
5. Regional stakeholders participate in education and training.

To achieve these capabilities, stakeholders must be fully engaged in addressing regional issues, actions should be targeted and have clear expectations of desired results, and stakeholders should regularly collaborate. These and other important characteristics of the capability are described at the beginning of each section.

Significant challenges complicate the achievement of each of the above capabilities, and regional partnership organizations adopt various approaches to meet those challenges. While there is great variety and ingenuity in the solutions used to overcome these challenges, regional partnerships often face similar challenges when developing these capabilities in their region. Each of the following capabilities is supported by a case study, based on interview outcomes, demonstrating

how regional partnership organizations meet and address many of the challenges common to enhancing regional resilience. The table below provides a summary of the capabilities section by linking each of the five capabilities with their associated challenges and case studies.

Regional Critical Infrastructure Resilience Capabilities, Challenges, and Case Studies		
Capability 1: Regional stakeholders engage in partnerships and collaborate to promote resilience of regionally important critical infrastructure.		
Challenge	**Description**	**Case Study**
Challenge 1.1	Developing collaboration across multiple jurisdictions.	All Hazards Consortium
Challenge 1.2	Fostering regional public-private partnerships.	ReadySanDiego Business Alliance; MOP3
Challenge 1.3	Creating value for members of a regional partnership.	PNWER
Capability 2: Regional stakeholders share information and intelligence through an information sharing network.		
Challenge	**Description**	**Case Study**
Challenge 2.1	Overcoming stakeholder mistrust.	CRA
Challenge 2.2	Involving small- to mid-sized critical infrastructure stakeholders in the regional information sharing network.	NEDRIX
Challenge 2.3	Developing information requirements and setting expectations of regional stakeholders.	LA InfraGard; NJBEOC
Capability 3: Regional stakeholders assess critical infrastructure risks and identify interdependencies.		
Challenge	**Description**	**Case Study**
Challenge 3.1	Assisting resource-constrained small- to mid-size businesses with risk assessments.	PA Region 13 Task Force
Challenge 3.2	Establishing a common understanding of regional risk.	ChicagoFIRST
Challenge 3.3	Overcoming the complex challenge of identifying and mitigating regional critical infrastructure interdependencies.	PNWER; APIP
Capability 4: Critical infrastructure owners and operators are integrated into regional emergency response and recovery planning and operations.		
Challenge	**Description**	**Case Study**
Challenge 4.1	Establishing a mechanism where the public and private-sector representatives can effectively collaborate during an emergency.	NJBEOC; ChicagoFIRST
Challenge 4.2	Understanding and leveraging available private-sector resources for use during and following emergencies.	SIP; PRBCHS
Challenge 4.3	Establishing a process to credential critical infrastructure owners and operators before a disruption.	ChicagoFIRST
Capability 5: Regional stakeholders participate in education and training.		
Challenge	**Description**	**Case Study**
Challenge 5.1	Ensuring subject matter is relevant to stakeholder needs.	SERRI
Challenge 5.2	Leveraging public-sector resources to help support or make available training and education opportunities.	ArizonaFIRST; CPAC
Challenge 5.3	Engaging small and mid-sized critical infrastructure owners and operators in training and education.	Washington EMD

IV. Capability 1

Regional stakeholders engage in partnerships and collaborate to promote resiliency of regionally important critical infrastructure

Capability Description
Homeland Security Presidential Directive 7 (HSPD-7) and the NIPP, along with efforts to implement these documents, establish a framework, at the national level, for the public and private sector to work together to protect critical infrastructure. The implementation of the NIPP, in coordination with other programs and activities, has successfully increased collaboration among critical infrastructure protection stakeholders. At the regional level, the development of effective partnerships between public and private-sector stakeholders has been principally driven by regional partnerships.

For a regional partnership to succeed, it requires the full and active engagement of a diverse group of stakeholders across multiple jurisdictions, including key members of the public and private sector. These stakeholders must actively collaborate, and sustain that collaboration over time, to address the numerous challenges of protecting and enhancing the resilience of a region's critical infrastructure. Regional stakeholders may include critical infrastructure owners and operators, non-critical infrastructure members of the private sector, law enforcement, government representatives (Federal, State, local, tribal), academia, community leaders (faith-based and government), and emergency response personnel (fire, EMS, public health), among others. As Dr. Mike Chumer of the New Jersey Institute of Technology commented, "Resilience depends on the full fabric of the region," and getting these diverse stakeholders to meet regularly at the same table is critical to achieving sustained regional resilience.

There is no one-size-fits-all approach, ideal structure, or preferred method for how stakeholders should collaborate through a regional partnership. Interview participants suggest that successful collaboration might include the following:

- Sharing successes and challenges;
- Highlighting emerging threats or suspicious activities;
- Previewing new preparedness and response related technologies;
- Scheduling and conducting joint exercises;
- Forming working groups around specific regional topics of interest;
- Sharing information and intelligence; and
- Pursuing targeted initiatives focused on improving regional resilience.

Engaging stakeholders and encouraging collaboration builds trust and allows stakeholders to tackle regionally significant issues in a more productive manner. Several interview participants cited the axiom, "an emergency is not the time to exchange business cards," to emphasize the idea that regional stakeholders should develop strong working relationships prior to a disruptive event to prevent unneeded delays and maximize the use of stakeholder capabilities during emergencies.

Each region faces unique challenges associated with establishing and sustaining regular stakeholder coordination. Regional partnership organizations reference several common challenges to engaging stakeholders and developing mechanisms for collaboration. In particular, organizations stressed three distinct challenges:

1. Developing collaboration across multiple jurisdictions;
2. Increasing communication, collaboration, and coordination between the public and private sector; and
3. Creating value that provides an incentive for continued member participation.

Challenge 1.1: Developing collaboration across multiple jurisdictions.

Description of the Challenge
Regional partnerships usually need to encompass multiple political jurisdictions, often crossing borders among municipalities, States, and even Nations. Regional organizations cite the difficulty of establishing, promoting and enhancing collaboration among these different jurisdictions. As geographic distance between jurisdictions in a defined region increases, the difficulty becomes even more acute. In some cases governmental officials and agencies in one jurisdiction might have different priorities or operate under different laws and regulations than their counterparts in other jurisdictions, and the benefits of working through this and collaborating with a distant jurisdiction might not be clear to them. Accordingly, regional partnerships must clearly articulate the shared interests, goals and responsibilities of the jurisdictions that they encompass. They must identify — and communicate to their participating partners — the reasons that collaboration and engagement among jurisdictions can improve coordination and enhance complementary responses to events that could potentially disrupt their region.

Meeting the Challenge
Effective regional partnerships can provide a trusted environment for jurisdictions to exchange information, identify common problems, and collaborate on shared goals. Regional partnerships can serve as the "convener," bringing together and providing a level playing field for disparate jurisdictions. These types of settings can reduce tensions by assuring that every partner's views, ideas, and concerns are fully heard and considered. Regional partnerships provide an incentive for jurisdictions to come together on their own, an activity that is currently impeded by lack of time and resources, and sometimes even mistrust or the perception of impropriety. Tom Moran of the All Hazards Consortium (AHC) discussed the potential benefits realized from informal meetings and events, noting that, "some of the best collaborations have spawned from a casual conversation over a meal."

Regional partnership leaders can provide logistics, including meeting space (physical or virtual), speakers, agenda, and meeting follow-up work (*e.g.*, drafting meeting minutes and soliciting participant feedback). In essence, regional partnerships serve as the "mixing bowl," providing a forum for jurisdictions that do not meet regularly to speak freely and collaborate on regional solutions. The following case study from the AHC provides an example of how a regional

partnership was able to coordinate and engage jurisdictions across State and municipal borders for the purpose of promoting and enhancing regional resilience.

Case Study:

All Hazards Consortium

The All Hazards Consortium (AHC) is a 501c3 non-profit, guided by the regional states of NC, DC, MD, VA, WV, DE, PA, NJ and NY, along with the urban areas of New York City, Newark, NJ, and Philadelphia, PA. Its role is to facilitate multi-state collaboration efforts that result in coordinated planning, investments, research, projects, and the creation of new partnerships and resources for member States and UASIs (urban areas that are part of the Urban Area Security Initiative (UASI) grant program from DHS). The ACH was formed in 2005 out of an identified need to improve collaboration and the conduct of joint resilience-based initiatives among States and regional stakeholders from government, private sector, academia, and non-profit/volunteer organizations.

Over the past five years, the AHC has developed a process to identify multi-State and multi-UASI requirements and facilitate education, collaboration, and funding to bring about solutions that meet regional needs. Regional workshops are an important part of this process and bring regional stakeholders together in a face-to-face environment to meet and discuss critical challenges. These workshops build key relationships across the region that lead to trusted information sharing and ultimately, effective results.

Through these workshops, the AHC acts as a neutral and trusted facilitator by identifying key people and issues in each State and providing a forum at the regional level to discuss challenges and solutions, generate in-kind contributions, coordinate public-private investments, generate projects, and facilitate discussions that can lead to further regional collaboration. This process has produced lasting results that include: seven Regional Workshops/Reports/Studies, Regional Webinars, Resources Raised, Regional Planning/Projects/Policy, Governance Structures, Partnerships, Regional Charters, Regional Agreements, Pilot Projects, Exercises, and Training.

To date, the AHC has hosted several regional workshops to bring its member States together to discuss critical issues and needs within a particular topic area (*e.g.*, Fusion Center, Interoperability, Critical Infrastructure Protection, Geographic Information Systems, Evacuation Planning, Ports and Transportation). Guided and designed by government, these workshops attempt to identify common State needs, requirements, and recommendations. They are sponsored and hosted by a single State or multiple States and are facilitated by the AHC.

The Regional Ports Security Workshop held in October 2009 is an example of a successful AHC workshop. This workshop was produced in partnership with DHS/FEMA, DHS IP, the SLTTGCC, and the RCCC as part of a strategy to increase awareness of the SLTTGCC/RCCC and begin to produce joint critical infrastructure and key resources related projects that all states, UASIs, and critical infrastructure operators can utilize in their efforts that promote resiliency and the NIPP. The workshop participants, which occurred in Hunt Valley, Maryland, brought together Federal, State, local, and private sector stakeholders from across the Mid-Atlantic region, to discuss shared issues related to port security.

The workshop was co-hosted by the State, Local, Tribal and Territorial Government Coordinating Council, Regional Partnerships Working Group; the State of Maryland and its host agencies; and private sector partners. Representatives from DHS and regional port associations played a prominent role in panel discussions and participation. The workshop focused on a variety of topics designed to educate attendees on port security from a regional critical infrastructure perspective and captured a "multi-State snapshot" of key topics to the region's ports (coastal and inland) from several perspectives.

The workshop resulted in the formation of a *Workshop Report* that summarizes key findings and takeaways from the workshop and allows participants to take recommendations for improving port security back to their respective jurisdictions. This report has been distributed nationally and results are already being realized. Due to the workshop and report's success, the AHC is planning to host a follow-on workshop in 2011.

Challenge 1.2: Fostering regional public-private partnerships.

Description of the Challenge
Building effective public-private partnerships continues to be a persistent challenge for many regions. This is due in large part to tension between the private sector and government. A great deal of the tension between government and the private sector stems from the power of government to impose sanctions and regulations on businesses. Historically, the private sector has not seen the need or tangible benefit from partnering with the government. However, the post-September 11 United States has witnessed a strong push for public-private sector coordination, particularly to better protect critical infrastructure assets from vulnerability to terrorist attack. Natural disasters over the past several years (Hurricane Katrina, BP Gulf oil spill) have also demonstrated the need for the public and private sectors to coordinate disaster response efforts. However, getting the private and public sectors to share resources and information during or prior to a disaster remains a critical challenge and one that prevents many public-private partnerships from reaching maturity.

Meeting the Challenge
Regional partnerships can serve as effective mechanisms for creating sustained, public-private partnerships. Regional partnerships utilize unique methods to encourage collaboration between the public and private sector and institutionalize this collaboration at the regional level. These methods involve developing public-private information sharing relationships (see capability 2) and integrating the private sector into regional response and recovery operations (see capability 4). In terms of the former, regional partnerships develop and leverage information sharing technologies and tools that connect the private and public sectors through a bi-directional information sharing relationship. The ease of use and efficacy of these technologies (see case study 2.1) fosters increased interaction and collaboration and builds trust between the public and private sectors.

Regional partnerships also connect private-sector members and infrastructure owners and operators with regional emergency management stakeholders by supporting private-sector liaisons at emergency operations centers (EOCs) (see capability 4). Regional partnerships develop and implement private asset registries to allow private-sector companies to pledge resources to supplement government resources as necessary during an emergency. Lastly, regional partnerships often support the development and operation of Business Operations Centers (BOCs), parallel EOC-type structures stood up during regional emergencies for the purpose of coordinating private-sector response and recovery to a disaster. The close link between BOCs and EOCs provides an additional level of cooperation and strengthens public-private partnerships. The case studies below from the ReadySanDiego Business Alliance and the

Missouri Public-Private Partnership (MOP3) provide prime examples of how regional partnerships have created mechanisms to foster effective public-private collaboration in their regions.

Case Studies:

ReadySanDiego Business Alliance

The ReadySanDiego Business Alliance is a public-private partnership developed to increase coordination, communication, and information sharing during and after disasters between the County of San Diego Office of Emergency Services (OES) and the private sector. During the firestorm of 2007, OES realized the need for a partnership with the private sector when OES staff discovered that there was no coordinated method to request and track private resources or provide the private sector with timely information during the disaster. The Business Alliance currently consists of more than 300 business members representing eight regional business sectors: Public Health and Healthcare, Communication/Media, Services, Production, Service Industries and Supply Chain, Sustenance and Health, Venues/Facilities, and Members-At-Large. Organization based around these sectors allows businesses with similar issues and concerns to address them and prioritize them before presenting them to the larger group. The overarching goal of the Business Alliance is to promote the region's resilience with four sub goals:

- Establish a coalition of businesses that can contribute resources and senior expertise; share best practices for disaster response and recovery efforts; and build a formal supply and communication chain before a crisis occurs, thereby enabling a timely public-private response during times of crisis.
- Participate in ongoing public-private partnership efforts, including additional planning.
- Identify what resources businesses can provide to the community during a disaster.
- Educate Business Alliance members and their employees on how to better prepare for a disaster.

The Business Alliance has also developed a rotating seat for the partnership within the region's Emergency Operations Center in addition to providing its members with Web resources, information sharing tools and emergency planning templates. The Business Alliance also hosts and participates in joint training and exercises with the public and private sectors, and will be hosting a table-top exercise for its members this coming fiscal year. The Business Alliance prides itself on being able to sustain strong public-private sector collaboration through joint initiatives, training, and workshops.

Missouri Public Private Partnership Committee

Created in 2006, the Missouri Public Private Partnership Committee (MOP3) is a coalition of private and public sector leaders directed by Missouri's State government and business leaders. The committee fosters direct involvement of the private sector into Missouri's homeland security issues and emergency management initiatives. The MOP3 promotes the application of best business practices; planning, training, and exercise development; fostering participation in intelligence and information fusion; and it provides a private sector platform to address issues and concerns for homeland security initiatives.

Recent disasters, both in and out of Missouri, demonstrated the need for a stronger, more effective relationship between public emergency responders and the private sector to assist Missouri with its emergency response and homeland security efforts. The MOP3 has four main goals:

1. To engage individual businesses, trade associations, and other non-governmental organizations to foster dialogue with the State on homeland security and emergency management issues.
2. To advise the Office of Homeland Security on the impact of the department's policies, regulations, processes, and actions involving the private sector.
3. To promote public-private partnerships and best practices to improve the State's homeland security preparedness and response capability.
4. To create and foster strategic communications with the private sector to enhance Missouri's homeland security and emergency management initiatives.

The MOP3 has multiple resources available through its partnership. Two of these resources are the Missouri Emergency Resource Registry (MERR) and the Business Emergency Operations Cell (BEOC). The MERR is an asset/resource registry system of private sector companies that pledge to provide goods or services upon declaration of a natural disaster or terrorist threat. The BEOC is a voluntary affiliation of critical infrastructure businesses and associations committed to a public-private partnership with the State Emergency Management Agency. It is focused on helping the State plan and respond to natural and man-made disasters. The MOP3 also hosts and participates in joint training and exercises with the public and private sectors. For example, the MOP3 participated in H1N1, New Madrid Earthquake, and other disaster response-related exercises. Lastly, the MOP3 is a member of the Missouri Alert Network, and uses the following methods of communication to disseminate information to its members: email alerts, MOP3 Web site, text messages, in-person meetings, conferences, and other events.

MOP3 leadership attributes the success of its public-private partnership to the committed and knowledgeable leaders of its business community, who have seen the value and importance of partnering with government to maximize the region's ability to prepare, respond to, and recover quickly from disasters, both man-made and natural.

Challenge 1.3: Creating value for members of a regional partnership.

Description of the Challenge

The strength and ultimate success of regional critical infrastructure partnerships depend on the extent to which stakeholders are engaged and participating on a continual basis. Engagement and participation are driven by the value that each individual member realizes from the partnership. As one interview participant noted, "For a partnership to succeed, there must be a return on

investment of members' time that supports their decision to expend resources on the regional partnership," as well as resources to assist the convener organization. Members devote significant time and resources to regional partnership activities, so they must realize a return on their investment. Resources allocated to partnerships might include personnel, meeting spaces, conference lines, or direct funding. If members are not provided incentives to continue participating in a partnership, they will spend their time and resources elsewhere. Ultimately, member value can take on many forms, but it is often challenging for regional partnership leaders to identify and convey partnership value to their members.

Meeting the Challenge

The challenge of creating partnership value to keep members engaged has become more acute given the recent economic downturn. However, regional partnerships provide a tangible benefit for stakeholders by first acting as a "force multiplier" for stakeholder concerns. Members can raise issues or questions that the partnership can then present or address in a unified manner. For example, if a few critical infrastructure owners or operators in the partnership are finding it difficult to implement a new State regulation at their facilities, their petition to the State for a revision of the regulation holds more merit coming from a partnership representing the critical infrastructure of the entire region.

As discussed previously, partnerships provide a neutral and trusted forum through which regional stakeholders can develop solutions to specific concerns. Partnerships can also leverage the knowledge of their leadership and members to foster direct access to real-time, cutting edge threat or disaster information and develop mutually beneficial relationships with other regional stakeholders through increased networking opportunities. All partnership organizations interviewed for this study deliver value to their members in some unique way. The case studies included throughout this report describe this value as it relates to the work they undertake to support capabilities that enhance regional resilience. While any organization interviewed could have been highlighted here to illustrate how partnerships create value for members, PNWER is highlighted due to the well documented and unique value it provides to its members through the Blue Cascades exercise series.

Regional Partnerships: Enabling Regional Critical Infrastructure Resilience

Case Study:

Pacific NorthWest Economic Region

In 1991, after recognizing their common issues and interests and the importance of regional collaboration, the States of Washington, Oregon, Idaho, Montana, and Alaska in the US, and the provinces of British Columbia and Alberta in Canada, established the Pacific NorthWest Economic Region (PNWER). The partnership later expanded to include Canada's Yukon Territory and Northwest Territories, as well as Saskatchewan province. In 1994, the partnership expanded to include the private sector, non-profit and NGO organizations. PNWER established a parallel private sector council that mirrors the organization's legislative delegate council, and private sector representatives were integrated into the working groups.

PNWER is a unique approach to engaging a large number of stakeholders with common interests dispersed across multiple jurisdictions and an international border. It is the only statutory, non-partisan, non-profit, bi-national, public/private partnership in North America. PNWER serves as a bi-national, regional advocate for the US Pacific Northwest and Western Canada, which is home to several important industries and several major infrastructure projects. It provides the public and private sectors a cross-border forum for unfiltered dialogue that capitalizes upon the synergies between business leaders and elected officials who work to advance the region's global competitiveness.

PNWER's Blue Cascades: Critical Infrastructure Interdependencies Regional Exercise Series raise awareness of infrastructure interdependencies and associated vulnerabilities, impacts, and preparedness gaps, and identify potential solutions to make needed improvements (more information on the Blue Cascades Exercise series can be found in Capability 3). Action Plans developed after the exercises specify the discrete activities identified during the exercise that are needed to understand infrastructure interdependencies and improve disaster resilience. These activities, and the associated actions initiated or completed since they were identified, demonstrate a concrete value to the individual participants and the region as a whole of their participation in the partnership.

V. Capability 2

Regional stakeholders share information and intelligence through an information sharing network.

Capability Description
Establishing a robust information sharing network available to regional stakeholders is a critical component of regional resilience. Such a network should work to provide regional stakeholders with current, accurate, actionable, and region-specific information and intelligence regarding a wide-range of all-hazards threats and incidents. Representatives from critical emergency functions (*e.g.*, Fire, EMS, and Public Health) as well as law enforcement, critical infrastructure owners and operators, and government representatives must actively engage in regional information sharing activities in order to conduct threat-based planning, respond appropriately to emergencies, and maintain situational awareness during man-made or natural disasters.

Specifically, a regional information sharing network should:

- Employ an accepted process for sharing relevant threat and disaster information among stakeholders while protecting that information.
- Establish clearly defined and institutionalized information sharing roles, rules, and responsibilities among stakeholders.
- Leverage the latest information sharing technologies to improve stakeholder access to, and dissemination of, information and intelligence.
- Include bi-directional, horizontal, and vertical information sharing relationships.

Interview participants noted that critical infrastructure owners and operators should play a central role within this network and must work with other regional stakeholders to build and maintain clear, two-way channels of communication across critical infrastructure sectors. Specifically, critical infrastructure owners and operators must be aware of current threats to their assets, which will allow them to develop emergency response and business continuity plans tailored to specific threat scenarios as well as exercise those plans. Critical infrastructure owners and operators must also be aware of the institutionalized information sharing mechanisms that exist, or should exist, regionally to facilitate the process of reporting and receiving information and intelligence.

Fusion centers are an integral part of regional information sharing by serving as a clearinghouse of information for local stakeholders. Many fusion centers across the country have incorporated critical infrastructure liaisons (in addition to public health, fire, campus security, and emergency management representatives) into their information and intelligence functions. Fusion centers are often co-located with State and local emergency operations centers (EOCs), connecting the intelligence and emergency management disciplines on a physical and strategic level to allow for informed decision making and carefully executed operations in the event of a regional emergency. Principally, fusion centers provide a single point of connection for the regional information sharing network; a central hub from which regional stakeholders can receive and

report information to others in the network. However, fusion centers serve in this capacity only if their leaders have a clear understanding of stakeholder requirements and ensure that stakeholders, particularly critical infrastructure owners and operators, are appropriately trained in formal information sharing processes and protocols.

The following key challenges exist toward developing sustained regional information sharing relationships among stakeholders:

- Overcoming stakeholder mistrust.
- Involving small- to mid-sized critical infrastructure stakeholders in the regional information sharing network.
- Developing information requirements and setting expectations of regional stakeholders.

Each challenge is described in detail below along with ways that regional partnerships have addressed these challenges. Following each section is a case study highlighting how an individual partnership overcame each challenge.

Challenge 2.1: Overcoming stakeholder mistrust.

Description of the Challenge
Regional stakeholders operate in very distinct and often separate corporate and organizational cultures. A natural mistrust within information sharing relationships stems from that fact that many stakeholders are unaware of other stakeholders' operations, often due to few connections being made between them on the individual level. This mistrust is compounded by fears that if stakeholders share information about threats, suspicious activities, or incidents, the information will not be adequately protected (from media or competitor misuse). This inhibits stakeholder participation in open and transparent information sharing relationships and may likewise prevent any efforts to institutionalizing such relationships.

Meeting the Challenge
Regional partnerships can foster a culture of collaboration and trust that enables information sharing among stakeholders. First, regional partnerships host seminars, informational meetings, and educational workshops (see Capability 1). These events allow stakeholders to meet, either physically or virtually (through WebEx or similar technology), and simply "get to know" one another. Interview participants emphasized the inherent value of these meetings in their ability to help regional stakeholders determine "who" is in their regional information sharing network and how they can benefit from sharing information with these individuals. Establishing these trusted relationships is a critical first step toward building a lasting information sharing network.

Regional partnerships can also support the development of formal, institutionalized information sharing relationships among stakeholders. Once trust is instilled among regional stakeholders, they are more likely to develop institutionalized information sharing agreements and procedures that serve to clarify and sustain protocols for sharing information. Interview participants stressed the importance of these formal information sharing agreements, as they outline clear procedures

for when, how, and with whom, they can share information. Further, these agreements can endure beyond staff transitions. Chris Terzich of Minnesota InfraGard noted that, "Institutionalizing information sharing relationships is valuable, but overcomplicating them could be detrimental. Formal relationships do not necessarily mean complex relationships." Ultimately, regional partnerships help ensure that information sharing relationships among stakeholders operate on basic principles of trust, mutual information needs, and clear communication channels. The following case study examines how the California Resilience Alliance (CRA) was able to instill trust in the information sharing relationships of its members through the establishment of a formal Memorandum of Understanding.

Case Study:

California Resiliency Alliance: Memorandum of Understanding

Due to a series of recent natural disasters in the State, the California Resiliency Alliance (CRA) decided it wanted to improve information-sharing relationships between its member businesses and the State of California. To accomplish this, CRA, in partnership with the State of California, developed a Memorandum of Understanding (MOU) for its organization, the California Governor's Office of Emergency Services, and CRA's affiliated partnerships in the State.

The MOU outlines formal information-sharing protocols to be used during emergencies. Further, the MOU establishes guidelines for the safeguarding of that information consistent with applicable laws. The MOU includes a Purpose Section stating the reason behind its creation: "Businesses play a significant role in protecting their employees and community during disasters (and) also play a vital role in working with government to facilitate and provide emergency response and recovery from all types of disasters." The MOU is therefore intended to fully integrate CRA and its partners across the State into the State's Standardized Emergency Management System, allowing them to better share critical information and resources during emergencies.

The MOU also describes the main roles and responsibilities for all parties involved in the agreement and how CRA will use the Response Information Management System (RIMS) "for mutual notification of emergency conditions that may affect the business or States assets." RIMS is a computer based system that provides essential emergency response information, such as standardized event or incident reports, incident damage estimates, and other types of real-time disaster information. The MOU also discusses the protection of critical information shared between the State, CRA, and its partners and outlines associated costs, rights and liabilities, and terms of the MOU. Ultimately, the MOU allows CRA to share and receive information with the State and other regional partnerships in a transparent and efficient manner. The MOU creates an information sharing process by which the methods, rules, and context for information sharing is clear and understood by all parties involved, which helps to build trust and confidence in the information sharing relationship and ensure that it endures beyond any transitions in staff.

Challenge 2.2: Involving small- to mid-sized critical infrastructure stakeholders in the regional information sharing network.

Description of the Challenge
Involving small- or mid-sized critical infrastructure stakeholders in the regional information sharing network can be difficult for a number of reasons. First, owners and operators of small- and mid-sized critical infrastructure may not recognize the value of participating in information sharing processes, whereas bigger assets might be mandated to share information or might receive more attention from law enforcement, government, or emergency response agencies (entities that traditionally provide information to critical infrastructure). Participants noted that this issue arises with critical infrastructure assets that do not fit into the 18 Federal sectors but are still considered regionally critical. Participants also noted that this challenge is compounded by the fact that many small- to mid-sized critical infrastructure owners and operators function under the assumption that if vital information (*e.g.*, an alert, warning) needed to be passed on to them, it would reach them in some manner (a law enforcement or emergency response agency simply calling businesses, for example).

Second, disseminating information (either real-time or preparedness/threat focused) to small- and mid-sized critical infrastructure can be difficult, as clear and established channels or mechanisms for sharing information might not exist. Law enforcement, government, or emergency response agencies might not have the relationships or contacts necessary within these small- or mid-sized businesses that would enable them to share critical information.

Meeting the Challenge
Regional partnerships can help engage small- and mid-sized critical infrastructure owners and operators in the information sharing process by first simply involving them in the partnership environment. When asked how they engage small- to mid-sized assets in information sharing, interview participants stressed the importance of inviting and obtaining participation from these assets for partnership meetings, events, and seminars. This is often accomplished through leveraging the contacts of current members or partnering with local chambers of commerce or economic recovery organizations, which already have relationships with these businesses. Partnership events then introduce small- or mid-sized critical infrastructure stakeholders to other regional stakeholders and create interactions that build trust and mutual awareness of stakeholder roles and responsibilities. Participants note that if small- and mid-sized businesses realize what types of information other stakeholders can provide (and *vice versa*), entering into an information sharing arrangement might be seen as more beneficial.

Regional partnerships can also be active in sharing information with small and mid-sized businesses through the use of real-time information sharing technologies. These technologies include Web sites, email alerts, phone chains, secure text messages, and other types of information dissemination tools. Stakeholders often have to register with regional partnerships to receive this information, which might include real time disaster alerts specific to a particular critical infrastructure sector, threat alerts, or preparedness information (during non-emergency times). This information sharing option is attractive for many critical infrastructure owners and operators, especially smaller businesses, as it requires minimal effort and resources on their end.

Information is pushed directly to owners and operators without the regional partnership requesting anything in return. However, many of these information sharing tools make available clear channels through which critical infrastructure can provide information back to the partnership, which will then distribute the information to the appropriate entity (*e.g.*, law enforcement, government, emergency response agency.). Ultimately, government and emergency management agencies can benefit from such information sharing systems, as it provides them with a means of pushing and receiving real-time information to and from these small- and mid-sized businesses, which previously may have been difficult to reach. The following case study examines how the NorthEast Disaster Recovery Information X-change (NEDRIX) developed an alert notification tool to enhance information sharing with small and mid-sized critical infrastructure.

Case Study:

NorthEast Disaster Recovery Information X-change: NEDRIX Notify

The NorthEast Disaster Recovery Information X-change (NEDRIX) wished to improve its ability to disseminate real-time threat and disaster information to owners of critical infrastructure in the region and also provide a means for bi-directional communication between critical infrastructure owners and other regional stakeholders. As a result, NEDRIX partnered with an information technology firm to create the NEDRIX Notify information sharing system, which provides real-time emergency alert information to its members and partners across Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, and Vermont. The goal of the system is to, "supply reliable information for use during an emergency" and ensure that the information sharing process is bi-directional.

NEDRIX Notify acts as an automated alert notification tool and provides NEDRIX with the ability to coordinate communications and disseminate real-time incident assessment information to a broad group of regional stakeholders. Government representatives can use NEDRIX Notify to disseminate information to critical infrastructure and other regional stakeholders regarding a wide range of critical situations, including severe weather, cyber threats, terrorist attacks, and evacuations updates. Those that receive information from NEDRIX Notify can in turn provide information (anonymously if preferred) regarding individual business operations or cross-sector impacts. The system delivers alert notifications to subscribed members via voice and text messages sent to email addresses, pagers, or mobile and landline telephones. Members can choose which device through which they wish to receive alert notifications, and these preferences, along with their member information, are stored in a protected database used exclusively for NEDRIX member communications. The messages are sent repeatedly until delivered and confirmed by recipients to ensure information is not missed and reaches its intended party. During non-emergency periods, NEDRIX Notify is used to distribute general member information regarding training opportunities or upcoming meetings and exercises. NEDRIX Notify currently services 2,000 individuals across the northeast region of the U.S.

Similar alert notification systems have been developed by other regional partnerships, including the Pittsburgh Regional Business Coalition for Homeland Security's Business Emergency Communications Network and the California Resiliency Alliance (CRA), which utilizes Twitter in addition to email and text alerts to distribute real-time incident updates and status reports to its members.

Challenge 2.3: Developing information requirements and setting expectations of regional stakeholders.

Description of the Challenge
Interview participants noted that developing clear information needs and requirements is a critical step when forming information sharing relationships or networks. However, critical infrastructure owners and operators often do not spend time developing these requirements or communicating requirements to those stakeholders with which they share information. This may result in critical infrastructure owners and operators having unrealistic perspectives or expectations as to how the information sharing process operates. Owners and operators might expect to receive a certain type of information during emergencies or even non-emergency periods, without actually clarifying their needs or requirements to the information provider.

Further, if information sharing expectations are not met, critical infrastructure owners and operators might think that their information sharing relationships are "one way" (*i.e.*, they provide other regional stakeholders with information, but do not receive information of value in return or are unable to see how the information they provided is consumed). Interview participants described how this issue often arises in relation to fusion centers, an entity to which critical infrastructure owners and operators often provide critical information, such as suspicious activity reports, incidents reports, or other types of real-time emergency information. Participants highlighted that critical infrastructure owners and operators often believe that information they provide to their fusion center "enters into a black hole," where there is no follow-up, no return information provided from the fusion center (or information is not useful), and no updates on cases opened or actions taken based on information provided.

Meeting the Challenge
Regional partnerships can help critical infrastructure owners and operators better understand their individual information requirements and needs and help them develop realistic expectations for the types of information they can expect to receive and from whom they can expect to receive it. Regional partnerships can host meetings or workshops where critical infrastructure stakeholders can meet as a group, individually, or with other regional stakeholders, to discuss their information needs (see the New Jersey Business Force (NJBF) example below). As Hank Straub from NJBF noted, "The more you know, the more you will realize what you don't know" and can build targeted information sharing relationships that will provide the most useful types of information.

Regional partnerships can also facilitate connections between regional critical infrastructure and State and local fusion centers. For critical infrastructure owners and operators specifically, these connections can result in the development of formal information sharing mechanisms where regular two-way information exchanges can occur between the fusion center and critical infrastructure stakeholders. One mechanism for achieving this involves positioning a critical infrastructure liaison on-site at the fusion center to serve as a single point of contact for the critical infrastructure stakeholder community. Another mechanism involves training critical infrastructure owners and operators on how to recognize and report suspicious activity or other types of information to law enforcement personnel associated with the fusion center, and *vice versa*. The first case study below examines how InfraGard Los Angeles developed a program to

train its critical infrastructure members to recognize and report suspicious activity to their area fusion center. The second case study highlights how the NJBF Business Emergency Operations Center (BEOC) was able to help critical infrastructure owners and operators identify their information needs and requirements.

Case Studies:

InfraGard Los Angeles: Infrastructure Liaison Officer Program

InfraGard Los Angeles recognized that critical infrastructure owners and operators could benefit from having a stronger relationship with their area fusion center, the Los Angeles Joint Regional Intelligence Center (JRIC). Specifically, LA InfraGard saw the success of the fusion center's Terrorism Liaison Officer (TLO) program, which involved training law enforcement, fire, and EMS personnel on how to recognize, document, and share suspicious activity that may be related to terrorism or other crime. As a result, LA InfraGard developed the Infrastructure Liaison Officer (ILO) training program, modeled on the JRIC TLO program, to provide critical infrastructure owners and operators with training on how to recognize and share information on suspicious activity they might witness at or near their critical assets with the JRIC.

The LA InfraGard ILO course lasts for 8 hours and is taught by the primary instructor used for the TLO program. An ILO can be any representative from a critical infrastructure asset in the region who has been appointed by their company as the primary contact with their local law, fire, and EMS TLO and InfraGard personnel at the JRIC. The mission of the ILO is to serve as a trained conduit of information between the private sector and their local public sector partners, for the protection of their company and community, in the defense of our critical infrastructure.

Any InfraGard background cleared member of the national critical infrastructure private sector may attend the ILO training course as well as any TLO member from any city, county, State, tribal government, or special district who assesses, analyzes, or implements critical infrastructure or the National Infrastructure Protection Plan (NIPP) concepts within the private or public sector.

The ILO training course is funded through a DHS Urban Area Security Initiative grant, and, to date, InfraGard LA has delivered 4 ILO sessions and trained over 200 individuals.

John Wentworth of LA InfraGard noted that "The ILO program ensures that critical infrastructure can share important information with the JRIC, and that this information sharing process is useful to both parties." Ultimately, the ILO program enhances the information sharing relationship between InfraGard members and the JRIC and provides trusted single points of contact through which JRIC analysts can receive and share critical information from and with critical infrastructure in the region.

New Jersey Business Emergency Operations Center: Information Requirements Development

The New Jersey Business Emergency Operations Center compiled a categorical list of critical infrastructure information requirements tied directly to continuity of operations and restoration of the supply/value chain during emergencies and disasters. The New Jersey Business Force (NJBF) hosted a series of meetings and seminars with critical infrastructure partners aimed at gathering and organizing these information requirements. Hank Straub of NJBF noted that, "the private sector cannot expect government agencies to know what elements of information are essential to specific operational plans or the priority of each. Once a general consensus is reached on the efficacy of these requirements, then the business community should pursue every avenue to make government counterparts cognizant of their importance and significance."

This process is ongoing and will be used to help inform and develop key information sharing relationships among critical infrastructure, government representatives, and emergency response entities. A few examples of the types of information requirements determined thus far are as follows:

- Changes in the Homeland Security Alert System.
- Initial activation and subsequent changes in the operational status/staffing of State emergency operations/fusion centers.
- Area evacuation notifications.
- Prioritization of the restoration of critical utilities/lifeline sectors, like water, natural gas, and electricity.
- Permit and regulatory waiver application procedures and issuance of same (primarily affects transportation and transportation infrastructure).
- Shipments and allocation of gasoline and diesel fuel during emergencies and national/regional shortages.
- Debris clearance prioritization and status.
- Credentialing.
- Transportation system closures.
- Border closings and blockades imposed by executive decree.
- Strategic National Stockpile distribution and activation of Points of Distribution.
- Mandatory quarantines during health emergencies or infectious disease outbreaks among animals (Foot and Mouth Disease).
- Employee absentee tracking and reporting.
- Building lock-downs.
- Operating radio frequencies.
- Rules of Engagement for deployed military during States of emergency or martial law.
- Specific provisions affecting the Private Sector within Emergency Declarations or States of Emergency.
- Expectations held toward the Private Sector including role as resource provider.
- Suspicious activity reporting procedures.

VI. Capability 3

Regional stakeholders assess critical infrastructure risks and identify interdependencies.

Capability Description:
A recurrent theme throughout the interviews with regional partnerships was the importance of conducting critical infrastructure risk assessments and identifying interdependencies. These assessments help critical infrastructure owners and operators and other regional stakeholders identify gaps, prioritize issues, implement targeted solutions, and inform the development of business continuity and emergency response plans tailored to specific threat scenarios. As Timothy Gablehouse of Denver InfraGard noted, "Critical infrastructure resilience is a blend of understanding risks and capacities to mitigate risks." Collectively, these activities can enhance the resilience of a region from disruption.

Risk assessments must account for the threats and vulnerabilities, as well as associated consequences of failure or disruption to the critical infrastructure asset and its essential functions. Further, assessments should not only consider physical assets (building structures, entryways, foundations) but also personnel, information technology systems, and the efficacy of emergency preparedness plans. Other important aspects of a successful regional risk assessment program include:

- Full participation in cross-sector, multi-jurisdictional assessments that test the resilience of the regional critical infrastructure network across a wide range of scenarios.
- Assessing capacity to respond to targeted threats and situations of regional significance.
- Assessments focused on regional issues, locations, and networks.
- Including participants that will play a critical role in any regional emergency, including critical infrastructure owners and operators; State, local, and Federal government representatives; first responders; law enforcement personnel; and community leaders.
- Test or assess skills, practices, and knowledge learned during training and education activities to ensure stakeholders retain knowledge.

It is essential that critical infrastructure owners and operators understand the impact that disruptions will have on their own critical infrastructure network, as well as the impact those disruptions will have on the region as a whole. Risk assessments of individual assets and systems can be assembled into a broader picture of a region's risk landscape and interdependencies. These broader views can support emergency planning, preparedness, response, and short- and long-term recovery efforts. David Shimberg of the Contingency Planning Associate of the Carolinas highlighted the interconnected and interdependent nature of regional critical infrastructure networks and stressed that if a business falters others in the region dependent on its goods or services could be dramatically affected. Other interview participants stressed the importance of conducting critical infrastructure interdependency analyses and supply chain vulnerability assessments aimed at educating owners and operators on the impact their assets — or loss of their assets — have on the region, and how other assets in the region support their

individual business operations. These assessments can pinpoint single points of failure and work to build redundancies into the regional critical infrastructure network.

Once critical infrastructure owners and operators understand that the continuity of their operations depends in large part on the continuity of the regional critical infrastructure network, they will be more likely to focus on building specific capabilities to assist the region in all-hazards response efforts. Sue Mencer of the Colorado Emergency Preparedness Partnership (CEPP) noted, "The very best planning by an individual company is for naught if the community around that business cannot function after a disaster."

Regional partnership organizations interviewed for this study face several common challenges to conducting risk assessments and identifying interdependencies. These challenges are:

- Assisting small- to mid-size businesses that lack resources with risk assessments;
- Establishing a common understanding of regional risk; and
- Creating value for members of regional partnerships.

These challenges are explored below and examples of how regional partnerships have helped critical infrastructure owners and operators assess risk, work with other regional stakeholders to create a common understanding of the regional risk landscape, and identify critical interdependencies and supply chain vulnerabilities to promote the resilience of the regional network.

Challenge 3.1: Assisting resource-constrained small- to mid-size businesses with risk assessments.

Description of the Challenge
For many critical infrastructure owners and operators, risk assessments — in particular business risk assessments — are a regular part of their day-to-day operations. However, some small- and medium-sized owners and operators, whose operations, if disrupted, would result in significant regional consequences, do not have the resources, staff, or time necessary to conduct assessments or participate in regional catastrophic planning. This challenge is compounded by the fact that Federal support for such risk assessments of critical infrastructure often extends only to the most high-risk assets and systems. In addition, there are few established programs for assessing the risks of regionally significant assets that may not be considered nationally significant.

Meeting the Challenge
Regional partnerships can support critical infrastructure owners and operators in assessing risks to their critical assets. This can be accomplished by connecting owners and operators to available resources at the State or Federal level outside the region, providing training to critical infrastructure owners and operators on how to conduct thorough self-evaluations, or analyzing region-wide vulnerability gaps and making targeted recommendations to individual critical infrastructure assets.

Regional partnerships may also be able to directly support site visits by risk assessment professionals. For example, Pennsylvania Region 13 Counter Terrorism Task Force has supported critical infrastructure owners and operators that need risk assessments and are more comfortable with a local entity providing the assistance.

Case Study:

Pennsylvania Region 13 Counter Terrorism Task Force: Critical Infrastructure Risk Assessments

The Pennsylvania Region 13 Counter Terrorism Task Force has mobilized several of its members trained in risk assessment methods to conduct free risk assessments, "red team" company information systems, and provide initial "out-briefs" to critical infrastructure owners and operators that include options for consideration to mitigate vulnerabilities uncovered during site visits. The Task Force had envisioned creating Area Risk Evaluation Survey (ARES) Teams for many years, but the program was created when learning site assessment tactics and organizational approaches from the National Guard during their G20 infrastructure surveys. The program, which is modeled after the LAPD Project Archangel, has conducted fifteen assessments to date, with the intended targets being smaller critical infrastructure owners and operators that have regionally significant critical infrastructure facilities, but are not necessarily identified at a national level.

Each specific jurisdiction within the Region 13 body has a member specifically trained in the principles and approach of site assessments, 14 total individuals. In addition to the specific jurisdictions, the City of Pittsburgh Emergency Management Agency Staff has all been trained on the principles and approach of site assessments. These individuals then assist in educating other public safety personnel from their jurisdiction to add discipline specific expertise to their ARES Team. The site assessments serve a threefold benefit to the community:

- Providing the opportunity for public and private sector security personnel to work together. Developing personal relationships and familiarity with their facility adds a level of confidence during a crisis.
- Providing first responders with first-hand experience and understanding of the unique surroundings and aspects of a facility located in their jurisdiction. The information identified from the site assessments is deemed protective critical infrastructure information (PCII) and then stored in the automated critical asset management system (ACAMS) in the event of a crisis.
- Allowing the facility managers with a focus on personnel, engineering, and cyber issues an opportunity to discuss the intricacies of their facility and their areas of concern, and have an honest evaluation of their facility to consider measures that can make it more secure.

Because of the healthy information sharing environment and involvement of city and county officials, this program has had strong interest by critical infrastructure owner and operators. The Pennsylvania Region 13 Counter Terrorism Task Force views this as a unique effort and continues to stress the importance of these "face-to-face relationships when working with regional critical infrastructure owners and operators.

Challenge 3.2: Establishing a common understanding of regional risk.

Description of the Challenge
Regional stakeholders often face the challenge of understanding how the risks to individual assets, systems, or sectors fit into the broader regional risk picture. In many cases, stakeholders do not consider the role and importance of critical infrastructure owners and operators in the regional network and how the continuity of certain critical infrastructure assets directly affects the continuity of other critical assets in the network. This challenge stems from the fact that many critical infrastructure owners and operators do not have strong relationships with homeland security and emergency management representatives in their region or with other critical infrastructure owners and operators outside their immediate sectors. Without these relationships in place, it is difficult to engage critical infrastructure owners and operators in cross-sector interdependency exercises or supply chain vulnerability assessments.
Developing a clear and common understanding among regional stakeholders of the specific risks to a region is a challenging and time consuming task, especially in large, complex urban areas. Understanding regional risks enables stakeholders to mitigate potential consequences in the event there are disruptions in the critical infrastructure network.

Meeting the Challenge
Many of those interviewed for this study stressed the important role that regional partnerships can play in establishing a common understanding of regional risk by facilitating efforts to conduct individual and regional risk assessments. Partnerships can bring together critical infrastructure owners and operators on a regular basis and encourage integrated planning with an eye toward not just protecting individual assets, but also the resilience of the regional critical infrastructure network. To accomplish this, regional partnerships can host seminars and workshops with critical infrastructure owners and operators and other regional partners. These seminars would educate attendees on effective risk assessment practices and also uncover dependencies, interdependencies, and potential cascading effects of the regional network. These meetings can also identify any critical infrastructure capabilities that may be available to respond to regional emergencies. Further, these events serve as an opportunity for regional partnerships to arrange speakers, such as subject-matter experts from private industry, law enforcement, and government. Together with their regional partners, speakers can share information regarding emerging threats, cutting-edge technologies used to improve systems security, recent legislation or regulatory standards effecting critical infrastructure operations, effective emergency preparedness measures, or information on upcoming critical infrastructure-related exercises or events.

Regional partnerships may also serve as a vehicle to mobilize resources or tools that are beyond the capability or mandate of regional stakeholders. For example, there are Federal programs, such as the Regional Resiliency Assessment Program (RRAP) that assist regions with identifying their critical assets and risks associated with the operation of those assets (see below case study). The case study below demonstrated how a regional partnership was able to leverage the RRAP to improve stakeholder understanding of their regional risk landscape.

Case Study:

ChicagoFIRST: Regional Resiliency Assessment Program Implementation

In 2008, a ChicagoFIRST member brought to the organization's attention several questions regarding the physical security of the area immediately surrounding its facilities. ChicagoFIRST relayed these questions to DHS' Chicago Protective Security Advisor. As a result of this, downtown Chicago became the first urban area evaluated under the then relatively new Regional Resiliency Assessment Program (RRAP).

The RRAP is an assessment of critical infrastructure 'clusters', regions, and systems that includes both the physical security concerns of individual critical infrastructure, as well as the interdependencies among critical infrastructure sectors in the region. The intent is to reduce the Nation's vulnerability to all-hazard threats by coordinating efforts to enhance critical infrastructure resiliency and security across geographic regions.

In 2009, 24 buildings in downtown Chicago were evaluated, including commercial facilities, finance, power, telecommunications, and water plants. DHS established a security score for the assessment footprint and developed a baseline score for covered facilities and sectors that was shared with participants. DHS also helped facilities analyze the costs and benefits of possible methods of enhancing their security profile. In 2010, ChicagoFIRST supported a RRAP Tabletop Exercise that focused largely on information sharing issues between the public and private sectors, as well as between infrastructures within the private sector. An after-action report (AAR) revealed gaps in the critical infrastructure information sharing network. As a result, the AAR recommended that the newly-formed Chicago Critical Infrastructure Resilience Task Force (Task Force), which is co-chaired by the City of Chicago's Office of Emergency Management & Communications and ChicagoFIRST address these issues and implement corrective actions. The Task Force is considering the following corrective actions:

- Improving information sharing between buildings and critical tenants.
- Streamlined processes in which the public sector handles and shares suspicious activity information.
- Improving cross-sector communications during a crisis.
- Establishing and populating a database of building and tenant information that the public sector may use during an emergency.

In the coming year, the Task Force is looking to further address issues surrounding interdependencies and recovery operations that arose from the Table-Top Exercise (TTX). ChicagoFIRST and the Task Force will work with DHS on a follow-on TTX that will consider interdependency and recovery issues.

Challenge 3.3: Overcoming the complex challenge of identifying and mitigating regional critical infrastructure interdependencies.

Description of the Challenge

It is critically important that regional stakeholders identify and understand the interdependencies and supply chain vulnerabilities among and between their assets and systems. This can be a very complex undertaking that expands in scope and complexity as the geographic scope of the region

and the number of critical infrastructure assets and systems that support a region's way of life and economy increases. Adding to the complexity of this task is often the critical importance of small and often unknown goods or services provided by smaller critical infrastructure owners and operators whose importance to regional resilience is disproportionate with their size.

Infrastructure owners and operators often believe that their internal business continuity planning and preparedness exercises are sufficient to prepare them for regional disruptions. This belief may place them at a distinct disadvantage when a regionally significant disruption deprives them or another critical infrastructure asset of an essential good or service.

Identifying and addressing critical infrastructure interdependencies remains one of the most challenging problems facing regional planners. The logistical challenge of assembling the right stakeholders to identify interdependencies can be significant. Critical infrastructure owners and operators may not even have a firm understanding of their own critical functions, how others depend on them, and the products or services on which they depend. It can be a manageable task at an asset level, but becomes increasingly more difficult as the scope and complexity of the region's critical infrastructure increases and serves a larger geographic area and population. Understanding interdependencies at a regional level is significantly more complex due to the number of potential owners and operators, impact of other stakeholders, and the difficulty identifying primary and causal relationships.

Meeting the Challenge

Cross-sector, multi-jurisdictional, and even cross-regional exercises — along with after-action reports and other follow-on activities — can be vitally important to addressing specific threats that outline real concerns of critical infrastructure owners and operators.

Regional partnerships can help address complexities associated with dependency analysis and supply chain vulnerabilities by conducting or facilitating regional cross-sector exercises. These exercises allow critical infrastructure owners and operators to focus on revealing interdependencies and supply chain vulnerabilities and testing preparedness and business continuity measures in place at their sites of operation. Matt Morrison of PNWER suggested that an exercise focused on regional critical information networks, "allows you to better understand the nuances" of critical infrastructure networks. Identifying and understanding the nuances can be significant in making a region resilient, and PNWER has conducted a series of exercises focused on regional issues that are important to local stakeholders. The Alaska Partnership for Infrastructure Protection (APIP) has also conducted exercises that focus on Alaska's unique geographic location and supply chain vulnerabilities.

In addition to the case studies below, Minnesota InfraGard recently worked together with the SafeGuard Iowa Partnership and DHS in September 2010 to develop and conduct a five-State critical infrastructure exercise entitled "Northern Lights." The exercise scope spanned the States of Minnesota, Iowa, North Dakota, South Dakota, and Nebraska and the exercise scenario specifically targeted regionally critical assets.

Case Studies:

Pacific NorthWest Economic Region: Blue Cascades Exercises

PNWER's Blue Cascades exercises are an outgrowth of an effort to help the region determine which assets must be protected and how to enhance recovery and mitigate the effects of disruptions from terrorist attacks or natural disasters. Each Blue Cascades exercise was designed by PNWER, co-sponsored by regional partners, including the Canadian Federal government, and reflects regional critical infrastructure concerns.

The first Blue Cascades exercise in June 2002 centered on raising awareness of interconnections among the region's critical infrastructures and resulting vulnerabilities associated with largely physical attacks and disruptions. The four additional Blue Cascades exercises held since have focused on cyber disruptions; response, recovery and restoration after a subduction zone earthquake; response and recovery from an influenza pandemic; and post disaster supply-chain resilience, specifically the resumption of food, fuel, and water supplies, after a catastrophic earthquake,.

The Blue Cascades exercises pursue the following common objectives:

- Raise awareness of infrastructure interdependency issues.
- Identify ways to make infrastructure providers aware of the extent and duration of disruptions.
- Identify and focus attention on the most important vulnerabilities that result from infrastructure interdependencies.
- Promote a mutual understanding of infrastructure service restoration priorities, challenges, and time lines, given the nature and scope of the region's infrastructure interdependencies.
- Identify and highlight roles, responsibilities, and authorities (local, county, State, Federal) for responding to and recovering from infrastructure disruptions.
- Determine ways to foster a more effective interface and information sharing among public and private-sector service providers and local, county, State/province, and Federal officials in developing and implementing infrastructure protection, mitigation, response, and recovery options.
- Identify preparedness shortfalls.
- Identify cross-border challenges to U.S. and Canadian abilities to cooperatively prepare for and deal with attacks and disruptions that impact the Pacific Northwest.
- Develop a detailed Action Plan to implement and track improvements.

Matt Morrison of PNWER commented that through the Blue Cascades exercises his organization is able to help critical infrastructure (CI) owners and operators reveal interdependencies, which is "a service that the private sector often cannot readily find in government." Further, these exercises help build trust and sustain information sharing relationships among CI stakeholders and government. Exercise participants are involved in the post exercise "action-planning session," where they categorize which projects are short-, medium-, and long-term, and produce a Regional Action Plan. PNWER will use the resulting Plan to help obtain funding for targeted regional initiatives focused on reducing vulnerabilities or challenges revealed during the exercises.

Alaska Partnership for Infrastructure Protection: Supply Chain Vulnerability Assessments

Since March 2009, APIP has conducted three exercises to identify supply chain vulnerabilities. These exercises and events focused on determining the interdependencies between and among sectors, the potential for cascading or escalating failures of critical infrastructure assets, immediate workarounds, and systemic improvements to eliminate or mitigate the effects of future events. Supply chain issues are critically important to the State of Alaska, given its geographic isolation and the importance of reliable supply chain security to its economy and way of life.

The first exercise was based on a scenario that shut down all automated transactions for exercise participants. Internet and phone transaction ability was lost and infrastructure owners and operators were forced to work in a cash-only environment that created a need for increased phone communications with customers, increased security measures, issues surrounding the purchase of fuel for service vehicles on roadways, and challenges managing out of town personnel.

The second exercise tested the communications capabilities of APIP members and required members to develop "work arounds" for resolving business impairments and loss of data systems. APIP members learned the importance of developing redundant communications methods for both satellite and priority landline systems as well as the need to train employees on how to communicate with customers face to face during the loss of internet and telephone capabilities.

The third exercise, entitled "Alaska Shield," provided APIP members with a virtual platform to test organizational response plans and procedures within a complicated earthquake scenario. During the exercise, members experienced loss of communications and power, fuel shortages, and challenges communicating with remote personnel. As a result of the exercise, APIP members realized a need to better understand the State and Federal response and recovery process, which will now be a focus of APIP in the coming year. To this end, APIP has scheduled briefs for APIP members to be delivered by each applicable emergency support function (ESF) representative from the Alaska Shield exercise, to create a great awareness of CI response and recover issues.

VII. Capability 4

Critical infrastructure owners and operators are integrated into regional emergency response and recovery planning and operations.

Capability Description:
An effective response to any regional emergency requires joint participation from, and coordination between, the public-sector and the critical infrastructure stakeholder community. These two groups must work to develop regional mechanisms that will allow them to gather and share information, analyze problems, propose solutions, acquire and stage resources, and make joint decisions during the response and recovery phases of man-made or natural disasters.

Often, the public sector does not have the resources necessary to adequately respond to and recover from emergencies that have a regional impact. Critical infrastructure owners and operators have access to and can contribute critical supplies and equipment, subject matter expertise and personnel, and on-the-ground situational awareness in times of crisis to support the public-sector response. A region is more resilient if its critical infrastructure owners and operators understand their role. Further, private-sector contributions during the response and recovery phases of significant regional events can significantly speed restoration of critical infrastructure operations. This requires owners and operators and public-sector representatives to plan, train, and regularly exercise alongside together. In a resilient region critical infrastructure owners and operators are integrated into the region's recovery planning and are prepared to support not just their recovery but also those of the broader critical infrastructure network and the region at large.

In the immediate aftermath of any disruption, the top priority of critical infrastructure owners and operators is to return to normal operations and provide their critical goods and services. Planning in many regions is focused on preventing terrorist attacks and protecting critical infrastructure assets, but not much effort is dedicated to short-, medium-, and long-term recovery, as it is often thought of as the responsibility of other stakeholders. Kelly Barcic of the Pittsburgh Regional Business Coalition for Homeland Security (PRBCHS) noted that while many businesses have detailed business continuity plans in place to address immediate disruptions in their operations, "they do not deliberately plan for regional recovery." Recovery planning is a task that presents unique challenges to regional stakeholders. Finding the time and resources to make a distinct effort to develop a recovery strategy and associated plans can be difficult in regions where emergency planners and critical infrastructure owners and operators have limited time and resources to do so. However, critical infrastructure owners and operators can assist with the identification and assessment of damages to the critical infrastructure network and regional supply chains, the prioritization of business recovery needs, and the provision of resources for use in individual and disaster assistance efforts.

Regional stakeholders must consider the following potential challenges when attempting to fully integrate critical infrastructure owners and operators into regional response and recovery operations.

Challenge 4.1: Establishing a mechanism where public and private-sector representatives can effectively collaborate during an emergency.

Description of the Challenge
Many small- and mid-sized critical infrastructure owners and operators manage with limited resources and personnel and conduct business continuity planning that focuses on the maintenance of their critical functions. Convincing public and private-sector stakeholders of the utility of establishing emergency collaboration mechanisms can be a significant challenge equal to or greater than creating the mechanisms themselves. Many stakeholders do not recognize the need or utility of coordinating their emergency response and recovery efforts with other businesses, let alone public entities. Likewise, government may not see the utility in establishing a collaborative space for the critical infrastructure community to make joint decisions during a response and may not believe that having a representative of the critical infrastructure community imbedded in their operations is necessary. Even if the concept of private-sector participation is accepted in a region, getting critical infrastructure owners and operators to participate in training and exercising for emergency response activation, roles, responsibilities, and response functions can be seen as time consuming, burdensome, and unnecessary.

Meeting the Challenge
Many interview participants suggested that regional partnerships can leverage their network to establish mechanisms where critical infrastructure owners and operators and government representatives can collaborate. Regional partnerships can work with the public sector to create a physical or virtual space where critical infrastructure owners and operators, trade associations representatives, chambers of commerce, and other members of the business community can meet before and during the response and recovery phases of a crisis to communicate needs, develop joint priorities, and make decisions using shared capabilities.

One mechanism is the creation of a BOC that runs parallel to the local EOC. The BOC can work in conjunction with and serve as the direct critical infrastructure link into the EOC during an emergency. Many State and local EOCs have a designated seat reserved for a critical infrastructure (or "private sector") representative who acts as a liaison between the BOC and EOC and provides a single point of contact for BOC communications. This individual can facilitate increased two-way communications between government and the critical infrastructure network by providing government agencies with real-time information on critical infrastructure disruptions while at the same time ensuring the latest disaster information reaches critical infrastructure owners and operators. BOC representatives and volunteers must receive proper training (*e.g.*, National Incident Management System training) prior to any activation, and roles, procedures, and relationships between and among infrastructure owners and operators and government agencies should be institutionalized and frequently exercised. Additionally, BOCs can serve as a real-time alert and warning center capable of disseminating alert messages (via text, email, phone, or other forms of communication) to the regional business community that will inform disaster decision making.

BOCs can be effective as either physical or virtual spaces. Operating virtually can alleviate concerns about staffing and the relocation of personnel to a BOC site during an emergency. This is especially critical when seeking engagement and BOC support from small to mid-sized critical

infrastructure businesses that have few resources to devote to the response effort. Further, regional partnerships can assist stakeholders in locating and securing a BOC venue and acquiring necessary BOC equipment and supplies. For example, many companies, especially those with large critical infrastructure assets, have developed extensive internal emergency management capabilities that include cutting edge communications tools and equipment, emergency management-trained personnel, and the ability to ramp up operations for large scale disasters. These centers provide a location where employees in charge of emergency management can communicate with their workforce and make important business continuity decisions. One interview participant described how a major company in their region allowed government agencies to utilize its EOC, as the facility possessed capabilities above and beyond that of the local EOC. The participant added that some companies have superior logistics capabilities which the government can "tap into" to make sure critical supplies are available to the public.

The case studies below highlight how regional partnerships in Chicago and New Jersey have successfully facilitated the development of mechanisms to connect critical infrastructure owners and operators with public-sector officials during emergencies. In addition to these case studies, the California Resiliency Alliance (CRA) supported the development of a BOC that is focused on collaboration between utilities companies and government during emergencies as well as the Washington State Emergency Management Division Public Private Partnership, which supports a similar virtual EOC system to the ChicagoFIRST example highlighted below.

Case Studies:

ChicagoFIRST: 24/7 Virtual Emergency Operations Center

ChicagoFIRST created the 24/7 Virtual Emergency Operations Center (EOC) to provide ChicagoFIRST staff with the ability to update members regularly with information that does not merit the "push" of email or emergency notifications, or more information must be provided than can be included in an alert. During emergencies, ChicagoFIRST serves as a critical liaison between its members, public officials, and first responder agencies in order to inform and assist each member's own response and recovery operations. A private, password-protected, members-only section of the ChicagoFIRST website is regularly updated during events and emergencies and serves as a secure source from which the membership can "pull" information as needed for use in determining their own response measures or to update their leadership and staff.

ChicagoFIRST has access to and may staff the City of Chicago and the State of Illinois Emergency Operations Centers to monitor emergency events. For smaller, day-to-day emergencies and special events ChicagoFIRST has determined that a physical presence in these EOCs is often unnecessary. In those instances ChicagoFIRST activates its Virtual EOC and communicates and coordinates virtually with local, State, and Federal officials as well as with its business membership. This around-the-clock information stream allows ChicagoFIRST staff to monitor emergency events to determine whether an event is escalating or de-escalating, whether further monitoring or additional information is needed, or whether the dissemination of membership alert notifications are warranted.

The Virtual EOC has proved useful for ChicagoFIRST during several events and emergencies, including several major immigration marches in the downtown area, 2008 Election Night, major sports championship rallies, and routine, but significant events, such as the annual Taste of Chicago.

New Jersey Business Force: Business Emergency Operations Center

In 2007, the New Jersey Business Force (NJBF) discussed how the private sector could support the public sector during the response and recovery phases of a catastrophic event that would encourage business sustainability and continuity during emergencies using a business to business (B2B) model. NJBF members determined that the private sector (writ large) cannot rely on the public sector for at least 72 to 96 hours after a catastrophic event and wished to develop a capability to permit B2B communication and allow critical infrastructure stakeholders to develop a Common Operating Picture and shared situational awareness during times of crisis.

In the fall of 2007, NJBF began developing the Business Emergency Operations Center (BEOC) as a way to promote B2B communications and interaction with local, county, State, the FEMA Region, and the Federal government. NJBF partners were able to negotiate a Cooperative Research and Development Agreement with the Armament Research and Development Engineering Center (ARDEC) at Picatinny Arsenal to use their Emergency Operations Center test bed facility, which became the physical BEOC site for participation in National Level Exercises 2008 and 2009.

The BEOC is staffed by pre-identified, pre-trained, and pre-equipped individuals from the business community, who have been appointed by their organizations to participate in BEOC drills and emergency operations. BEOC members participate in monthly planning sessions, ongoing training, and periodic exercises. The BEOC possesses a volunteer registry capability developed through a Memorandum of Understanding signed between BEOC managers and The World Cares Center in New York City, a non-profit organization specializing in the training, management, and effective use of spontaneous volunteers to assist in emergency operations.

The BEOC provided support to the Colorado Emergency Preparedness Partnership (CEPP) during the planning and operations phase of the 2008 Democratic National Convention. Individuals from ARDEC, the New Jersey Institute of Technology, and the NJBF staffed the BEOC in support of the Denver business community for an entire week, twelve hours each day, providing them with critical preparedness measures and situational awareness of Convention events. To facilitate BEOC assistance, CEPP provided the NJBF with access to its member portal. Additionally, the Southeast Emergency Response Network (SEERN) provided the BEOC and CEPP with on-the-ground situational awareness of protestor movements and actions that might threaten businesses and citizens. SEERN is also representing and reporting back to the BEOC on all NLE 2011 planning efforts underway involving the private sector.

Challenge 4.2: Understanding and leveraging available private-sector resources for use during and following emergencies.

Description of the Challenge

The private sector may be able to provide critical resources during an emergency, including electrical power, communications capabilities, engineering/construction assistance, equipment maintenance, lodging, food services and sanitation, site security, medical services, mortuary services, water and ice, and transportation vehicles. However, it is difficult for emergency managers and responders to leverage these resources if critical infrastructure owners and operators do not have a clear and easy way to "plug-in" to the disaster supply chain. Interview participants stressed that there is simply not enough time to identify these types of private-sector resources on an *ad hoc* basis during an emergency and that there must be a mechanism or process to do so prior to an emergency. Such a mechanism would allow businesses to pre-pledge or spontaneously contribute supplies and personnel to the disaster response and recovery effort while adequately safeguarding those supplies.

Further, critical infrastructure owners and operators often perceive cooperation with public safety agencies as risky, due to concerns about the protection of proprietary information, the misuse of donated equipment and goods, and public disclosure requirements. They may be reluctant to share resources with government agencies due to questions surrounding liability, cost (initial or otherwise), duration of resource use, and cost reimbursed. All of these factors speak to the need of establishing processes to identify potentially useful private-sector resources before a disruptive event and ensuring the right public-sector representatives have that information at their fingertips.

Meeting the Challenge

As a way to understand what supplies, equipment, and people are available to assist regional responders, regional partnerships can develop and expand stakeholder participation in critical infrastructure emergency resource registries. These registries log emergency supply information, equipment, subject-matter expert contacts, and volunteers that businesses choose to pre-pledge or pre-designate for use during regional disasters. Regional partnerships can leverage their connections in the business community and reach out to local chambers of commerce and other trade associations to inform businesses of the existence of the registry, discuss the regional and community benefits obtained from pledging assets, and address any legal or regulatory concerns from the business community about government use of critical infrastructure assets in regional emergencies. According to Kelly Barcic of PRBCHS, "private asset registries maximize speed and utility, and minimize redundancy" when identifying and providing resources needed to respond to emergencies.

Regional partnerships can also work with government agencies and critical infrastructure stakeholders to develop joint agreements that cover inventorying, requesting, allocating, utilizing, and returning critical infrastructure resources. These agreements should include certain qualifications that must be met in order for resource sharing to occur, such as prior depletion of public-sector resources or expected impact of the incident on the critical infrastructure asset's area of concern. Regional partnerships can also host public-private training exercises that include the testing of resource sharing plans and address any issues associated with liability and reimbursement.

Business or Emergency Operations Centers should have access to asset registry databases to allow government agencies to improve their staging of resources near disaster-prone areas in a region, prior to or immediately following an event. The acquisition and placement of these assets into the field can be coordinated through the joint BOC-EOC relationship.

The case studies below from the Safeguard Iowa Partnership and PRBCHS are examples of how regional partnerships have created mechanisms that have enabled the public and private sector to work more effectively during emergencies. Several other regional partnerships have developed resource registries that have been tailored to the unique needs of their region, including the CRA Disaster Asset Registry and CONNECT Colorado, which is a project of CEPP and the Denver InfraGard Member's Alliance.

Case Studies:

Safeguard Iowa Partnership: Business Resource Registry

The Safeguard Iowa Partnership (SIP) Business Resource Registry is a secure Web-based catalog of private-sector resources that businesses may agree to make available to emergency management officials, on either a voluntary or paid basis, in the event of a natural or manmade disaster. The resource registry allows businesses to "help maintain continuity of community and insure a viable and secure future for the Iowa region." The Business Resource Registry essentially functions as a confidential "Yellow Page" listing of private sector resources within the State of Iowa. Private sector resource owners can register any type of resources that could be utilized for disaster response or recovery within the State of Iowa. Resources that have been registered with SIP will be used to assist public emergency responders when government resources are depleted or unavailable for disaster relief within the State of Iowa.

There is no limit to the number of resources that each private sector owner can register with SIP, and registering resources is completely voluntary. Certain indemnification and protection is available and applicable to all participants. Resources can be provided as donations or charitable contributions, or provided on a pre-defined fee structure. Resource information contained in the Business Resource

Registry Database is only accessible by State Emergency Response Officials or their designees for emergency preparedness and response purposes. SIP has developed a user manual with policies and procedures for authorized users of the registry, including county emergency management, businesses and State emergency management officials. SIP has also developed training materials and educational offerings to increase awareness and use of the registry. Currently, SIP is piloting the Business Resource Registry in the Cedar Rapids-Iowa City SIP Chapter and plans to significantly expand SIP partner participation in the Business Resource Registry in the coming year.

Pittsburgh Regional Business Coalition for Homeland Security: Private Assets for Regional Responders System

In 2005, the Pittsburgh Regional Business Coalition for Homeland Security (PRBCHS) worked with the Region 13 Task Force to develop the Private Assets for Regional Responders System (PARR) program, which allows emergency managers to view specific assets that private companies may have available for use during emergencies. Businesses use a Web-based system called the "Knowledge Center" to register equipment, facilities, supplies, and personnel that they may have available for use during an incident or event. The system provides Region 13 emergency managers with a list of available assets that private companies can contribute as well as an easy way to request these resources during emergencies. As of September 2009, 11 companies have pledged assets on the PARR system.

The system was used heavily during "the big snowstorm." The PRBCHS attributes the success of the PARR system in large part due to its ability to keep registry information private until a disaster happens, so companies do not know your capabilities. This ensures that companies feel comfortable pledging goods in a trusted and secure manner.

Challenge 4.3: Establishing a process to credential critical infrastructure owners and operators before a disruption.

Description of the Challenge
Delays or hold-ups in credentialing of critical infrastructure owners and operators during or post-disaster will inhibit many private industry subject-matter experts or volunteers from entering a disaster area to provide support to emergency responders. Likewise, damaged critical infrastructure assets may often require outside assistance in resuming operations (*e.g.* hiring a plumber or electrician), but may encounter difficulties in properly credentialing these individuals who must enter the field of operations in order to perform their services. The timely provision of many emergency services during a disaster often requires critical infrastructure personnel to accompany emergency responders into the field of operations. These individuals may require physical access to buildings, network access, human resource asset accountability, incident command and control capabilities, and integration into the National Incident Management System.

Meeting the Challenge
Partnerships can work to reduce roadblocks historically associated with credentialing of critical infrastructure owners and operators. Many participants noted that it is important that regional jurisdictions institute some form of access credentialing for representatives of critical infrastructure owners and operators, either in the form of "Smart Cards" or simple contact lists. Regional partnerships can help develop a database of these individuals and their credentials that can be easily accessed by government agencies across multiple jurisdictions, and assist in the implementation of Smart Cards (or similar type mechanisms) that can be interoperable across regional jurisdictions. This will ensure that expertise of critical infrastructure personnel can be leveraged regionally to support recovery operations following a disaster. The case study below describes how a regional partnership, ChicagoFIRST, addressed the issue of credentialing in their region.

Case Study:

ChicagoFIRST: Credentialing System Development

ChicagoFIRST recognized that critical personnel from both the public and private sectors routinely experienced difficulty performing essential duties during and following an emergency due to delays in credentialing. To address this issue, ChicagoFIRST has been collaborating with the State of Illinois and the City of Chicago for the past few years to institute both access credentialing systems and the protocols that govern their use and applicability. With the encouragement of ChicagoFIRST, the State of Illinois implemented a smartcard system modeled after the DHS First Responder Partnership Initiative, which serves as a model for other regions to enhance cooperation and efficiency between their State and local first responders and their Federal counterparts. As of October 2010, ChicagoFIRST has been piloting the Illinois credentialing system for their private sector network in addition to a more traditional credentialing system for the City of Chicago. ChicagoFIRST's longer term goal is to ensure that the credentialing systems are interoperable across regions, States, and multi-State areas, so that multiple cards need not be carried. Additionally, ChicagoFIRST will continue to advocate the following regarding credentialing:

- All State and local jurisdictions should institute some form of access credentialing for critical infrastructure owners and operators. Such systems may prove useful during the response to and recovery from emergencies, as well as when access must be restricted for other reasons.
- Credentialing systems need not be identical; rather, they should be tailored to the jurisdiction. In some cases, an elaborate smart card approach would be appropriate while in others simple contact information sheets could suffice.
- Access cards themselves are secondary to the protocols that govern their use by and applicability to the private sector.
- The public sector must own the credentialing system and incorporate it into its emergency response plans. The private sector cannot simply produce cards and seek to use them, because local responders will not recognize them.

VIII. Capability 5

Regional stakeholders participate in education and training.

Capability Description:
Critical infrastructure protection and resilience is a dynamic study; there are continually evolving methods and tools used to manage all-hazards risk to infrastructure. For a region to achieve maximum resilience, the stakeholders in the region need to maintain awareness of effective tools and cutting-edge methods as well as any legislation and regulations that might impact their operations. Formal training and education opportunities provide this level of awareness and sustain regional stakeholder engagement, while empowering them to take ownership over their role as an integral part of the regional critical infrastructure network. Establishing formal training and education programs across regionally significant focus areas also allows stakeholders to gauge other stakeholders' parallel grasp of issues, knowing that they have completed similar training and education. This deepens the level of collaboration between regional stakeholders and allows them to address issues and challenges from an educated perspective.

Examples of training opportunities might include: steps for building a robust business continuity plan; how to operate emerging technologies; training in emergency management topics (such as understanding the National Incident Management System or the Target Capabilities List); courses on how to conduct vulnerability self-assessments of critical infrastructure assets; or understanding interdependencies with other critical infrastructure assets in the region (see capability 3). Educational opportunities might include briefings to stakeholders regarding emerging regional threats; how to recognize signs of terrorism; the role of government during a disaster; the details of new Federal or State regulations, policies, or laws affecting critical infrastructure stakeholder operations; or best practices on how to share information effectively. Training and education provides critical infrastructure owners and operators with an awareness of the current regional threat culture and allows them to plan accordingly to mitigate those threats. Further, training and education builds a common lexicon of emergency preparedness, response and recovery language that can improve the quality of communications between regional stakeholders. As Tom Moran of the AHC commented, "Education tears down walls faster than mandates" by allowing regional stakeholders to fully grasp issues of regional significance and apply that knowledge to improve the way they protect their critical infrastructure assets.

However, the following key challenges exist toward developing sustained regional stakeholder engagement in training and education:

- Ensuring subject matter is relevant to stakeholder needs.
- Leveraging public-sector resources to help support or make available training and education opportunities.
- Engaging small- and mid-sized critical infrastructure owners and operators in training and education.

Each challenge is described in detail below along with ways that regional partnerships have addressed these challenges. Following each challenge section is a case study highlighting how an individual partnership overcame each challenge.

Challenge 5.1: Ensuring subject matter is relevant to stakeholder needs.

Description of the Challenge
Training and education opportunities must not only provide new knowledge to regional stakeholders but must also be relevant to stakeholder needs and the unique needs of the region. Without relevant subject matter, stakeholder participation in regional training and education opportunities will wane and cease to demonstrate utility. Regional stakeholders, particularly critical infrastructure owners and operators, need to be able to take knowledge and skills learned from training and education courses and apply them to their own business operations in a way that enhances their operations and enables them to understand and operate within the regional network. However, pinpointing stakeholder training and education needs and keeping abreast of the latest developments in emergency preparedness and response is a challenging endeavor, especially for regions with limited resources.

Meeting the Challenge
Regional partnerships can help ensure that the subject matter of training and education opportunities remains relevant to stakeholder needs through several different methods. First, regional partnership leaders can periodically survey stakeholder needs, including information requirements, requests for systems access, emergency response capability gaps, or current threat awareness. From this survey, partnership leaders can work to develop or make available training and education courses tailored to these stakeholder needs. This ensures that subject matter will be relevant and applicable to stakeholder operations.

However, regional partnership leaders may not be aware of the most effective types of available training and education that can best meet stakeholder needs. To overcome this, regional partnerships often partner with academic institutions to leverage the knowledge and skills of subject-matter experts who are conducting ongoing research and analysis of homeland security and emergency management topics. Colleges, universities, think tanks, and other non-profit organizations across the country possess a wealth of expertise and knowledge of current homeland security practices, including risk management, disaster response and recovery, counterterrorism, and business continuity. Regional partnerships can tap into these institutions for training and education needs. In many cases, these subject matter experts can serve as instructors for regional stakeholder training and education courses.

Case Study:

The Southeast Region Research Initiative: Partnering with Academia to Provide Training

The Southeast Region Research Initiative (SERRI) has partnered with several academic institutions in developing and providing training and education opportunities for critical infrastructure owners and operators across the southeastern region of the U.S. The first such opportunity was established in 2008 and is offered through Mississippi State University. The initiative educates critical infrastructure stakeholders in areas of cyber security awareness, food safety, emotional resilience for young children, digital forensics, and surveillance and response to biological threats.

SERRI has also teamed with Western Carolina University in conducting facilitated workshops and focus group meetings aimed at training community members, public agencies, non-governmental organizations, faith-based organizations, and the private sector in North and South Carolina in emergency preparedness and response. Lastly, SERRI has worked with the University of Southern Mississippi to develop training tools for use at the university's National Center for Spectator Sports Safety and Security, which trains first responders at sports stadiums in Improvised Explosive Device and other multi-hazards awareness training.

The success of these training courses and relevance of course subject matter is directly attributed to SERRI's ability to leverage partnerships with academic institutions across the southeastern U.S. to provide cutting edge training and education to its members. Member feedback has been very positive regarding the efficacy of these courses, and SERRI intends to expand both the number and type of training and education courses offered as well as those partnership members benefitting from it.

Challenge 5.2: Leveraging public-sector resources to help support or make available training and education opportunities.

Description of the Challenge

Public-sector employees, including emergency responders, law enforcement, public health, and military must often complete training and education courses designed to improve their ability to do their day-to-day jobs. Government agencies and other public-sector organizations often have robust training departments or relationships with subject-matter experts to teach these courses to their employees. Regional stakeholders, particularly critical infrastructure owners and operators, could benefit from having access to the training and education opportunities, especially in areas of emergency management, contingency planning, counter terrorism awareness, and other types of workplace safety courses. However, the public sector may not have the appropriate resources or relationships to extend these training and education opportunities to all regional stakeholders.

Meeting the Challenge

Regional partnerships can partner with stakeholders from government in order to leverage training and education opportunities for their members. Some regional partnerships are led by members of State or local emergency management or homeland security agencies and can provide a clear avenue into government-sponsored training and education opportunities.

Government agencies often have access to technologies that regional stakeholders wish training in, such as WebEOC or the Homeland Security Information Network (HSIN).

Also, public-sector agencies may be able to provide venue space and logistics (*e.g.*, parking, food, member invites) for stakeholder training and education. This is especially critical for regional partnerships that operate on an all-volunteer basis and lack the appropriate funding and meeting space to host these education and training courses for their members. The first case study below illustrates how a regional partnership, ArizonaFIRST, was able to leverage its relationship with State emergency management agency to secure critical training for its members. The second case study provides an example of how a regional partnership leveraged its local Citizen Corps chapter to provide critical training for its members.

Case Studies:

ArizonaFIRST: Partnering with the State of Arizona to Provide Training

Since the partnership's launch in 2008, ArizonaFIRST has made a concerted effort to develop and maintain a strong relationship with its State Division of Emergency Management (DEM). This relationship is further enhanced by the creation of a private sector liaison position within the State DEM, tasked with coordinating with key private industry leaders on issues of emergency management and homeland security. Through this relationship, ArizonaFIRST leaders recognized that the State DEM had several key training courses available to its employees in areas of emergency management and homeland security that could benefit ArizonaFIRST members, particularly those in the private sector. As a result, ArizonaFIRST collaborated with the DEM private sector liaison to make available DEM training and education courses to ArizonaFIRST members. DEM often hosts these courses at its facilities and provides instructors to teach the courses, which cover several different emergency management areas. Further, the DEM private sector liaison completed a "train the trainer" course in the Incident Command System (ICS) and is now teaching courses in ICS to ArizonaFIRST members from the private sector who may deploy to the State Business Emergency Communications Center during emergencies.

Due to the strong relationship ArizonaFIRST has fostered between its organization and the public sector, ArizonaFIRST members receive invitations to other public sector trainings offered or sponsored by DHS, the Federal Bureau of Investigation (FBI), InfraGard, and other State emergency management groups.

For example, ArizonaFIRST members from the private sector participated in the Joint Security Symposium, a one-day event sponsored by Arizona DHS and the FBI focused on providing training and education in regional security matters. ArizonaFIRST also participated in the Phoenix Emergency Management All-Hazards All-Stakeholder Summit, a half-day event that included both public and private sector participants, working together to address issues of emergency preparedness, response, and recovery. Lastly, ArizonaFIRST sponsors two one-day seminars each year and invited its public sector partners to attend those events and enlisted their participation as presenters. Jan Williams of ArizonaFIRST attributes the success of their partnership with DEM and other agencies to members' active efforts to maintain close ties with the public sector, which involve regular monthly meetings and casual coffee "get-togethers."

Contingency Planning Association of the Carolinas: Community Emergency Response Team Training

The Contingency Planning Association of the Carolinas (CPAC) recognized that many of its members, particularly small- and mid-sized businesses, lacked sufficient knowledge of emergency and preparedness and disaster response and did not have the tools necessary to be able to respond to incidents at or around their businesses or communities. To accomplish this, CPAC partnered with the North Carolina Citizen Corps to sponsor Business Community Emergency Response Team (CERT) training. The CERT program educates individuals about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. CERT members can then assist others in their community or workplace following an event when professional responders may not immediately be available to help. CERT is run by Citizen Corps and receives funding through DHS.

In March of 2008, CPAC worked with Citizen Corps to host the CERT training for 31 CPAC members, representing 18 businesses and organizations. The training not only focused on educating individuals on specific emergency response techniques, but also aims to train these individuals on how to train others, in essence a "train the trainer" program. The training covered how to conduct emergency triage, rapidly categorize treatment needs of survivors, perform emergency treatments for bleeding or breathing victims, and educate participants on disaster psychology responses, Incident Command principles, CERT team organization, and basic search and rescue operations.

During the training, CPAC made it clear to participants that the CERT training is not intended to train them as professional fire fighters, medical responders, or search and rescue personnel, but rather it is designed to prepare individuals to supplement the efforts of professional responders during no-notice emergencies. CPAC plans to conduct similar type training in the future and offers information and registration for the training through their Web site: http://www.cpaccarolinas.org/.

Challenge 5.3: Engaging small- and mid-sized critical infrastructure owners and operators in training and education.

Description of the Challenge

As mentioned in previous capabilities, engaging small- and mid-sized critical infrastructure owners and operators in regionally focused activities can be problematic, especially when attempting to gain their participation in training and education. This is due in large part to owner and operator perception that they do not have the necessary time, resources, or staff to devote to training and education. Also, many smaller companies might not have designated business continuity personnel or directors of security to send to these opportunities, further compounding the challenge.

Meeting the Challenge

Regional partnerships have taken many different approaches to gaining small- and mid-sized critical infrastructure owner and operator participation in training and education, all with varied success. Several interview participants stressed the idea that even though many of these businesses operate on limited resources, firms will make resources available for training and education if they see that their participation can help preserve and protect their "bottom line," particularly during disasters that might cause disruptions to their operations or the regional

critical infrastructure network. Therefore, regional partnerships must in effect "pitch" training and education opportunities to these businesses and demonstrate their value. However, this requires a great deal of partnership resources, since (depending on the size of one's region) there may be several critical small- to mid-sized businesses in a region, and they may be geographically spread apart.

To meet this challenge, some regional partnerships have engaged State and local chambers of commerce and other economic development organizations, rather than the critical infrastructure businesses themselves. Some regional partnerships have begun to conduct "train the trainer" programs aimed at educating members of these State and local chambers on how to conduct critical emergency management, business continuity, and workplace safety training for those small- and mid-sized businesses who are intimately connected with these chambers and economic organizations. Below is a case study examining how one regional partnership, the Washington State Emergency Management Division public-private partnership, conducted such a training program for local chambers of commerce in their State.

Case study:

Washington Emergency Management Division: 'Train the Trainer' Business Continuity Training Program

In 2009, leaders from the Washington Emergency Management Division (EMD) public-private partnership recognized that small- and mid-sized businesses across the State lacked sufficient training in effective business continuity planning, and that there were business continuity resources that could help these businesses. However, the partnership also recognized the inherent difficulties involved in reaching out to these businesses, who make 70 percent of the State's revenue, due to lack of partnership resources and direct connection with business leaders. To address this issue, Washington State EMD partnered with the Washington State Department of Commerce, the Association of Washington Businesses (the State chamber of commerce), and Pierce College to develop a business continuity "train the trainer" program for local chambers of commerce. The aim of the program is to empower representatives from area chambers of commerce with the knowledge and skills needed to conduct effective business continuity training for those businesses registered and involved in their organizations.

Washington EMD partnered with Pierce College's Center for Excellence in Homeland Security, which has several business continuity experts and resources, to develop the curriculum for the "train the trainer" program. Washington EMD utilized their partnership with the Association of Washington Businesses, which is the State chamber of commerce representing 6,800 businesses, to reach out to local chambers and economic development organizations across the State to gain their participation. With those elements in place, the "train the trainer" program was officially launched in October 2010 and is being taught by subject matter experts from Pierce College and other area colleges with similar homeland security and emergency management programs. The training lasts a single day (7-8 hours) and the curriculum focuses heavily on preparedness, mitigation, planning, risk assessment methodology, and how businesses can mitigate and transfer risk. A portion of the training also focuses on building an effective business continuity plan and additional critical steps that business should take following a disaster.

While the program is still in its infancy, Washington EMD leaders are already seeing value in its implementation. Wendy Freitag of Washington EMD noted that, "There are several benefits to approaching the issue of training small businesses through this type of program." She continued to note that the program requires few partnership resources to maintain, and the curriculum is "top-notch," due to its development by business continuity experts. In addition, small businesses are willing to participate, because the training is being offered by organizations with which they are already connected on a regular basis, and the program can reach many businesses through partnerships with State and local chambers of commerce.

Appendix A:

Compendium of Regional Partnerships

The following *Compendium of Regional Partnerships* provides information about active regional partnerships in the United States. The *Compendium* provides the following information: name of partnership, region of focus, date founded, type of regional partnership (operational, educational, and/or networking), representative contact information (phone, email, partnership Web site), and a description of the partnership mission including a list of key partnership activities and initiatives. The *Compendium* is intended to facilitate increased interaction among regional stakeholders who might wish to learn more about a particular partnership initiative or focus area or simply wish to build stronger ties within the regional partnership network. This Compendium is not comprehensive and does not include every regional partnership in the country; rather, it includes all of the partnership organizations interviewed for this study.

(See Attached Excel File: "Regional Partnership Compendium.xls")

Appendix B:

Acronyms

AAR	After-Action Report
ACAMS	Automated Critical Asset Management System
ARDEC	Armament Research and Development Engineering Center
AHC	All Hazards Consortium
APIP	Alaska Partnership for Infrastructure Protection
B2B	Business to Business
BECON	Business Emergency Communications Network
BEOC	Business Emergency Operations Center
BOC	Business Operations Center
CEPP	Colorado Emergency Preparedness Partnership
CERT	Community Emergency Response Team
CI	Critical Infrastructure
CPAC	Contingency Planning Association of the Carolinas
CRA	California Resilience Alliance
CRADAR	California Resilience Alliance Disaster Asset Registry
DEM	Arizona State Division of Emergency Management
DHS	Department of Homeland Security
EMD	Washington State Emergency Management Division
EMS	Emergency Medical Services
EOC	Emergency Operations Center
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
HSIN	Homeland Security Information Network
HSPD-7	Homeland Security Presidential Directive 7
ICS	Incident Command System
ILO	Infrastructure Liaison Officer
IP	DHS Office of Infrastructure Protection
JRIC	Joint Regional Intelligence Center
MERR	Missouri Emergency Resources Registry
MOP3	Missouri Public-Private Partnership

MOU	Memorandum of Understanding
NEDRIX	NorthEast Disaster Recovery Information X-change
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NJ BEOC	New Jersey Business Emergency Operations Center
NJBF	New Jersey Business Force
NLE 2011	National Level Exercise 2011
OES	County of San Diego Office of Emergency Services
PARR	Private Assets for Regional Responders System
PCII	Protected Critical Infrastructure Information
PNWER	Pacific Northwest Economic Region
PODS	Points of Distribution
PRBCHS	Pittsburgh Regional Business Coalition for Homeland Security
PSA	Protective Security Advisor
QHSR	Quadrennial Homeland Security Review
RCCC	Regional Consortium Coordinating Council
RIMS	Response Information Management System
ROE	Rules of Engagement
RRAP	Regional Resiliency Assessment Program
SEERN	Southeast Emergency Response Network
SEOC	State of Illinois Emergency Operations Center
SERRI	Southeast Region Research Initiative
SIP	Safeguard Iowa Partnership
SLTTGCC	State, Local, Tribal and Territorial Government Coordinating Council
SNS	Strategic National Stockpile
TLO	Terrorism Liaison Officer
TTX	Table-Top Exercise
UASI	Urban Area Security Initiative

Appendix C:

Regional Consortium Coordinating Council Leadership

RCCC Chair

- Brian Tishuk, Executive Director, ChicagoFIRST

RCC Vice-Chair

- Tom Moran, All Hazards Consortium

RCCC Executive Council

- Ann Beauchesne, Vice President, National Security and Emergency Preparedness Department, US Chamber of Commerce
- Jami Haberl, Executive Director, Safeguard Iowa Partnership
- Ian Hay, President, South East Emergency Response Network (SEERN)
- John Madden, Director, Alaska Division of Homeland Security and Emergency Management
- Matt Morrison, Executive Director, Pacific NorthWest Economic Region (PNWER)
- Christopher Terzich, President, Minnesota InfraGard
- Dr. Robin White, South East Regional Research Initiative (SERRI)