



RC3 Regional Consortium Coordinating Council

Member and Mission Landscape Study

May 2014

Chris Terzich

InfraGard Minnesota Members Alliance
Chair

Tom Moran

All Hazards Consortium
Vice Chair

Table of Contents

Executive Summary	1
Study Purpose and Design	1
Findings	1
Next Steps	4
RC3 Member Organization Snapshot.....	5
Introduction and Background	6
Study Methodology.....	6
Study Organization	8
How Members Leverage and Value the RC3.....	9
RC3 Member Organization Composition and Reach.....	11
Partnership Mission Areas.....	16
Critical Infrastructure Security & Resilience Activities	20
Partnership Challenges & Requirements to Grow and Sustain Contribution	24
Member Profiles.....	27
Alaska Partnership for Infrastructure Protection	27
All Hazards Consortium	32
Bay Area Center for Regional Disaster Resilience.....	39
California Resiliency Alliance.....	45
ChicagoFIRST	51
Colorado Emergency Preparedness Partnership.....	59
Great Lakes Hazards Coalition	65
Minnesota InfraGard Members Alliance	70
Missouri Public-Private Partnership	75
New Jersey Business Force/Business Emergency Operations Center Alliance	80
Northeast Disaster Recovery Information X-Change (NEDRIX)	86
Pacific NorthWest Economic Region Center for Regional Disaster Resilience	90
ReadySanDiego Business Alliance.....	96
Safeguard Iowa Partnership	102
SouthEast Emergency Response Network.....	108
U.S. Chamber of Commerce.....	112
Western Cyber Exchange.....	117
Acronym List.....	122
Reference Library	125

Executive Summary

Incidents do not respect jurisdictional or organizational lines, making regional partnerships a key contributor to critical infrastructure security and resilience at the local, regional, and national levels. The recently released *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) recognizes the important role of regional partnerships in partner collaboration, information sharing, education and awareness, and emergency response across sectors and jurisdictions. NIPP 2013 specifically calls out the Regional Consortium Coordinating Council (RC3) as a partner in executing these objectives by leveraging regional collaboration to strengthen critical infrastructure security and resilience.

RC3 member organizations represent a wide range of regions, from metropolitan areas to broad multistate collaborations. The Member Organization Snapshot in the next section provides a summary of factors, including organizational structures, funding sources, primary activities, and sectors of focus. Because of the regions' unique characteristics and the diverse makeup of the stakeholders, each organization identifies and addresses threats and hazards in a variety of ways depending on its level of resources, the scope of its network of partners, and the scale of the potential threat. The RC3 is able to connect these organizations by fostering information sharing, hosting educational opportunities, conducting exercises, identifying best practices, and developing communication and collaboration strategies.

Study Purpose and Design

Through open-source research and interviews with executive directors and leaders of RC3 member organizations (as of October 2013), this *Member and Mission Landscape Study* examined five key areas: the value the RC3 provides its membership, the composition and reach of RC3's member organizations, member organization missions, critical infrastructure security and resilience activities, and member challenges and requirements for continued partnership sustainment. By understanding these critical components of regional partnerships, RC3 and the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) can evaluate the applicability and delivery of tools and services to partnerships.

Findings

The study included a detailed examination of 17 of RC3's member organizations (included in individual member profile appendices). Nine total findings (discussed below) emerged across the five areas of examination.

How Members Leverage and Value the RC3

Finding 1	Members engage in the RC3 to network with regional partnerships, share information through trusted channels, and align actions with national policy.
-----------	--

1.1 RC3 provides opportunities for members to interact, collaborate, and exchange ideas on common security and resilience issues with colleagues both within and outside a region.

1.2 RC3 acts as a trusted clearinghouse of relevant information and training opportunities, including best practices aggregated from multiple sources and training and exercises opportunities for planning, preparedness, response, and recovery.

- 1.3 RC3 helps to convey national-level policies and programs for critical infrastructure security and resilience to members and infuses a regional perspective that enables members to better align their own actions and policies.

Finding 2 RC3 is well placed to provide increased future value to members in the areas of partnership building, information sharing, and national policy.

- 2.1 The RC3 can increase its value to members by expanding partnerships with active organizations and building its reputation as a central source of policy, guidelines, and best practices that actively help regional organizations learn from each other.
- 2.2 RC3 can develop a more formal process to collect, distribute, and socialize highly valued critical infrastructure security and resilience information among regional partnerships and their government partners.
- 2.3 RC3 can act as a national-level coordinator of separate partnerships to enhance critical infrastructure security and resilience efforts in support of NIPP 2013.

RC3 Member Organization Composition and Reach

Finding 3 RC3 member organizations partner with a diverse set of stakeholders through trusted, time-established relationships that are critical to the efficacy of the organizations' activities.

- 3.1 Regional partnerships commonly engage non-traditional and community-level stakeholders that Federal agencies or national organizations may not.
- 3.2 Successful partnerships are based on time-established relationships built over time with consistent action and regular interaction.

Finding 4 RC3 member organizations are able to reach across jurisdictional and sector boundaries.

- 4.1 Each RC3 member organization embraces a network-of-networks approach to partnership building, and many RC3 member organizations are actively involved in helping new partnerships form and evolve.
- 4.2 Many RC3 member organizations are also expanding their reach into additional communities by establishing additional geographic or demographic chapters of their organizations.
- 4.3 RC3 member organizations collaborate with existing formal and informal partnerships to leverage and share knowledge and expertise.

Partnership Mission Areas

Finding 5

Most RC3 member organizations develop from the ground up and adjust their missions and activities to reflect regional and stakeholder needs and lessons learned from experience in events.

- 5.1 Many RC3 member organizations formed following foundational disaster events that exposed regional needs.
- 5.2 Steady, diversified funding sources are crucial for RC3 member organization sustainment and growth.
- 5.3 Emerging issues are integrated into partnership missions and support their evolution and organizational growth.
- 5.4 Leadership buy-in is crucial for operational employees to move boots-on-the-ground initiatives forward.

Finding 6

RC3 member organizations bridge jurisdictional boundaries, either within their organization or by partnering with others, to address region-specific needs while leveraging and tailoring national expertise and policies.

- 6.1 RC3 member organizations have a regional focus and emphasize working across jurisdictions and sectors to solve problems, address interdependencies, and make the region more secure.
- 6.2 RC3 member organizations network with the right set of diverse partners to address regional needs and connect partners that may not otherwise interact.
- 6.3 National expertise and a central approach may be needed for cybersecurity and other expansive topics.

Critical Infrastructure Security and Resilience Activities

Finding 7

RC3 member organizations are well positioned to address cross-sector issues and interdependencies while tackling intractable region-specific challenges in preparedness and response.

- 7.1 Preparedness and response are key priorities for RC3 member organizations, who are engaging the private sector to concentrate resources and address regional challenges.
- 7.2 The structure of RC3 member organizations makes them well-suited to address interdependencies, supply-chain resilience, and other cross-sector focus areas. Partnerships develop based on a common identified threat or need, enabling partners to work across boundaries and identify interdependencies.

Finding 8 RC3 member organizations adjust activities to meet changing missions and partner needs, with a growing focus on joint exercises, cybersecurity, and information sharing.

- 8.1 Regional and national exercises are important critical infrastructure activities for RC3 member organizations.
- 8.2 Cybersecurity has emerged as a top area of concern for RC3 member organizations. Cybersecurity transcends jurisdictional and regional boundaries, and many members are focused on developing practical guidance.
- 8.3 Members increasingly leverage technology solutions and information-sharing platforms to deliver timely information to partners. Some are now also using social media as a force-multiplier to share information and promote activities.

Partnership Challenges and Requirements to Grow and Sustain Contributions

Finding 9 To be sustained or accelerated, RC3 member organizations require sustained funding, increased flexibility in organization, support to address cybersecurity and emerging issues, and a whole community approach.

- 9.1 Dedicated long-term diversified funding is crucial for partnership development, mission and activity sustainability, and training and exercise support.
- 9.2 Partnerships need increased flexibility to organize beyond jurisdictions in ways that make sense to members, connect across existing partnerships, and institutionalize relationships to improve sustainability.
- 9.3 To address cybersecurity and other emerging issues, partnerships need expert input, clear authorities, robust two-way information sharing, and coordinated exercises and training.
- 9.4 Effective regional partnerships take a whole-of-community approach that best leverages private-sector and non-profit resources and knowledge and responds to local needs.

Next Steps

Members widely value the RC3 as a networking mechanism, a clearinghouse of trusted information serving member needs, and a source of information on national-level critical infrastructure security and resilience policies and programs. As RC3 continues to develop and evolve, there are opportunities to provide greater value to members while expanding membership. RC3 leadership and DHS IP can use the insights on member composition, mission, activities, values, and needs to improve how the RC3 partners with regional organizations and with the Federal Government on critical infrastructure security and resilience.

RC3 Member Organization Snapshot

Demographic Snapshot of Participating RC3 Member Organizations

17
Participating RC3
Member Organizations*

*Out of 23 organizations, as of April 2014



Governance Structure of Member Organizations

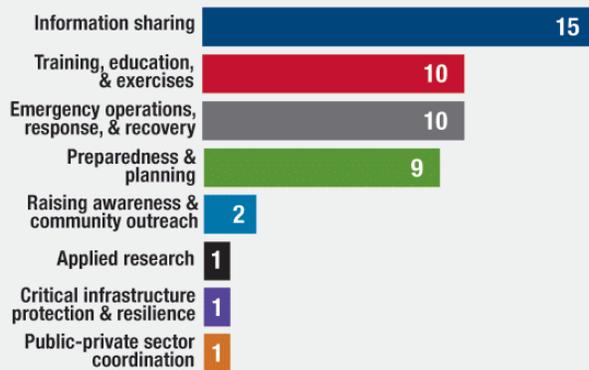


Member Organization Demographics*

Private Sector	Public Sector	Academia	Nonprofits
17	15	6	5

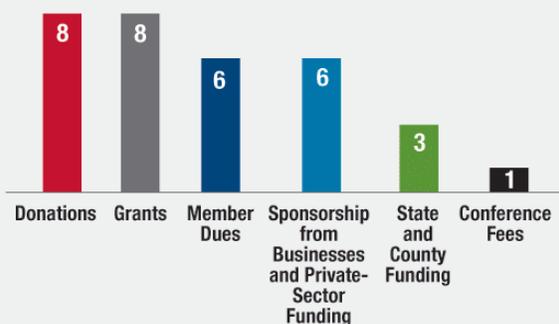
*All 17 member organizations interviewed represent private-sector entities with the majority also representing public-sector stakeholders.

Member Organizations' Primary Activities*



*Total responses from 17 member organizations = 49

Member Organization Funding Sources*



*The 17 member organizations interviewed utilize a mix of 1 to 4 funding sources.

Number of Member Organizations Focusing on Each Sector



Introduction and Background

The Regional Consortium Coordinating Council (RC3) is a national-level partnership council that connects regional organizations focused on critical infrastructure security and regional resilience. It is a key council in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) partnership structure, responsible for leveraging regional coordination to strengthen national security and resilience. With 25 current members across the United States, the RC3 represents organizations that interconnect along common threads of supply chains, hazards, and interdependencies and extends their capabilities by connecting with and drawing upon each others' expertise and resources.

This *RC3 Member and Mission Landscape Study*, made possible by support from the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP), is a companion to the March 2011 *Regional Partnerships: Enabling Regional Critical Infrastructure Resilience*, which highlighted effective characteristics of regional partnerships and detailed their focus areas and needs pertaining to regional resilience. A product of extensive research, interviews, and analysis, the *Landscape Study* is intended to provide RC3 and DHS IP with new insights about RC3 member organizations' composition and their critical infrastructure security and resilience activities and needs. DHS IP and RC3 can use the *Landscape Study* findings to enhance the applicability and delivery of tools and services to individual partnerships.

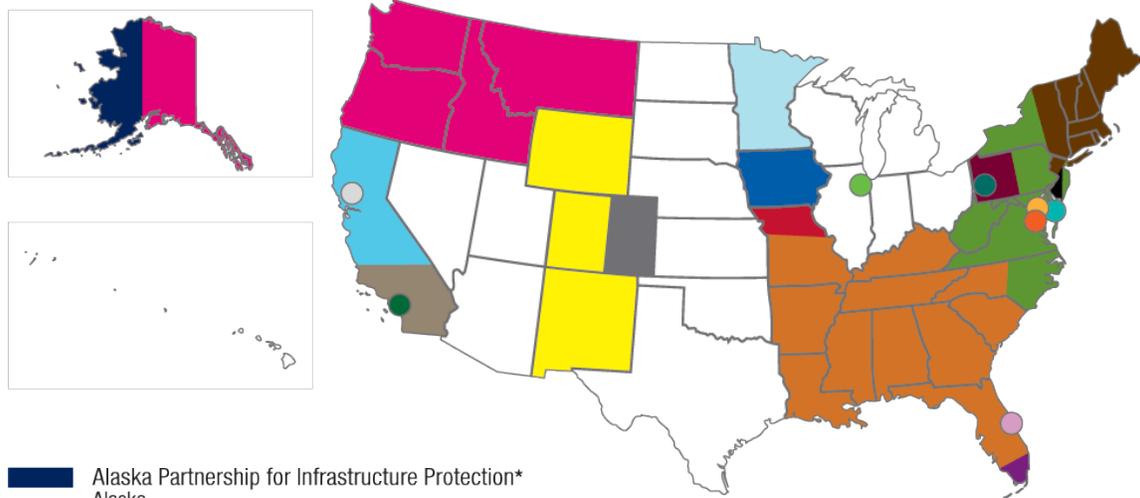
Study Methodology

The *Landscape Study* is based on a series of interviews with the executive directors and leaders of RC3's members, as well as comprehensive open-source research. The study examines 17 partnerships across 40 States and all 10 Federal Emergency Management Agency (FEMA) regions, including 8 representing multistate interests, 7 statewide partnerships, and 3 representing metropolitan areas. Figure 1 depicts the breadth of RC3 member organizations.

Through research and interviews, the study aimed to answer the following questions:

- How do members use and value the RC3?
- What types of organizations comprise the RC3?
- What are the missions of those organizations?
- What critical infrastructure security and resilience activities do they engage in?
- What are members' challenges and requirements for continued growth and success?

Figure 1. National Coverage of RC3 Member Organizations



- Alaska Partnership for Infrastructure Protection*
Alaska
- All Hazards Consortium*
Delaware, Maryland, New Jersey, New York, North Carolina, Pennsylvania, Virginia, West Virginia, and the District of Columbia, along with the UASI areas of New York City; Newark, New Jersey; Philadelphia; and the National Capital Region (NCR)
- California Resiliency Alliance*
California and specific collaboration within the San Francisco Bay Area
- Colorado Emergency Preparedness Partnership*
Colorado
- Minnesota InfraGard*
Minnesota
- Missouri Public-Private Partnership*
Missouri
- New Jersey Business Force/Business Emergency Operations Center Alliance*
Based in New Jersey, focuses on the Philadelphia and New York-New Jersey metropolitan regions
- Northeast Disaster Recovery Information X-Change*
Northeast United States, including Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, and Vermont
- Pacific Northwest Economic Region*
Alaska, Washington, Idaho, Montana, and Oregon and the Canadian provinces and territories of Alberta, British Columbia, Saskatchewan, Yukon, and the Northwest Territories
- Pittsburgh Regional Business Coalition for Homeland Security
Western Pennsylvania
- Safeguard Iowa Partnership*
State of Iowa
- SoCalFIRST
Los Angeles, Orange, Riverside, San Bernardino, Ventura, and Santa Barbara counties
- South Florida Disaster Resiliency Coalition
Broward, Miami-Dade, Monroe, and Palm Beach counties
- Southeast Emergency Response Network*
Southeast United States, including Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Missouri, Mississippi, North Carolina, South Carolina, and Tennessee
- Western Cyber Exchange*
Colorado, New Mexico, and Wyoming
- American Logistics Aid Network
National organization with headquarters in Annapolis, MD
- Bay Area Center for Regional Disaster Resilience*
The San Francisco Bay Area metropolitan area, which includes 12 counties and more than 110 cities
- ChicagoFIRST*
Chicago metropolitan area
- InfraGard Members Alliance
Pittsburgh, Pennsylvania
- National Health-Information Sharing & Analysis Center (NH-ISAC)
Kennedy Space Center, Cape Canaveral, Florida
- Ready San Diego*
San Diego, California-metropolitan area
- The Infrastructure Security Partnership (TISP)
Headquartered in Alexandria, Virginia
- U.S. Chamber of Commerce*
National organization headquartered in Washington, D.C.

*Denotes organizations interviewed as part of the RC3 Member and Mission Landscape Study

Study Organization

Interviews and analysis provided new insights into RC3 member organizations, organized across five key areas that make up the body of the *Landscape Study*:

- **How Member Organizations Leverage and Value the RC3:** Understanding realized and potential value can identify ways the RC3 can help fill the needs of its members.
- **RC3 Member Organization Composition and Reach:** Understanding the composition and key community of stakeholders of RC3 member organizations can bolster engagement by the RC3 and DHS IP on critical infrastructure capabilities, programs, tools, and information.
- **Partnership Mission Areas:** Most regional partnerships develop organically from the ground up and adjust their missions and activities to reflect regional and stakeholder needs and lessons learned from experience in events.
- **Critical Infrastructure Security & Resilience Activities:** Regional critical infrastructure initiatives and best practices, including physical and cyber initiatives, can be leveraged by RC3 member organizations to strengthen regional critical infrastructure efforts and by DHS IP to increase participation in national efforts. A reference library includes links to access guides, plans, toolkits, and initiatives referenced in the *Landscape Study* on the topics of infrastructure resilience and interdependencies, information sharing, emergency operations, exercises, cybersecurity, public health, and surveys.
- **Partnership Challenges & Requirements for Growth and Sustained Contribution:** RC3 member organizations cited several areas where additional assistance is needed to continue or expand their critical infrastructure security and resilience mission and activities.

Member Profiles

Supporting the *Landscape Study* are detailed profiles of each RC3 member organization, presented as appendices to the full report. Each member profile details the following:

- **Organization Snapshot:** Provides a one-page summary that includes the organization's establishment, geographic and sector focus, membership totals and levels, funding type, governance structure, and primary activities.
- **Key Factors of Partnership Success:** Highlights the approaches the organization took to successfully execute its mission. These best practices can help inform the partnership development and maturity of other regional organizations, RC3, and DHS IP.
- **Success Stories:** Summarizes the activities that the organization believes most exemplify its contributions to the critical infrastructure mission.
- **Critical Infrastructure Activities:** Details specific activities led or participated in by the organization in five areas: planning and preparedness, training and exercises, information sharing, emergency response, and partnerships.
- **Organization Background:** Provides more details on the organization's establishment, mission, activities, funding sources, and governance structure.

How Members Leverage and Value the RC3

RC3 member organizations derive value in their council membership primarily from the networking opportunities it provides as an effective vehicle for collaborating with other regional partnerships on common critical infrastructure security and resilience issues. RC3 is also valued as an important source of trusted information relevant to members' interests and for conveying national-level security and resilience policies and programs to members with a regional perspective. Members look forward to RC3 increasing its value by continuing to expand connections between regional partnerships, enhance sharing of highly valued information, and engage the membership to bring national security and resilience policy to action.

Finding 1 Members engage in the RC3 to network with regional partnerships, share information through trusted channels, and align actions with national policy.

Members widely value RC3 membership as a networking mechanism to engage with and learn from other security and resilience partnerships; a clearinghouse of trusted information serving member needs (e.g., threat-specific information or training and exercise opportunity information); and a source of insight on national-level critical infrastructure security and resilience policies and programs.

1.1 RC3 provides opportunities for members to interact, collaborate, and exchange ideas on common security and resilience issues with colleagues both within and outside a region. It serves as a structural support network of partnerships facing similar issues and thus enables members to stay informed and share best practices.

1.2 RC3 acts as a trusted clearinghouse of relevant information and training opportunities, including best practices aggregated from multiple sources and training and exercises opportunities for planning, preparedness, response, and recovery. Members can learn from and leverage proven solutions in other member regions and replicate best practices for specific critical infrastructure-related problems or topics to enhance boots-on-the-ground efforts.

1.3 RC3 helps to convey national-level policies and programs for critical infrastructure security and resilience to members and infuse a regional perspective that enables members to better align their own actions and policies. Providing insight into how national policies (e.g., Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, and NIPP 2013) and programs (e.g., Chemical Facility Anti-Terrorism Standards, InfraGard, and Protective Security Advisor [PSA] programs) specifically relate to regional critical infrastructure partnerships is viewed as a key benefit RC3 brings to its membership. Armed with this added education and awareness, RC3 member organizations are able to tailor their efforts to better serve the critical infrastructure stakeholders in their own regions, aligning with national policy and leveraging national programs for advancing security and resilience.

Finding 2	As a partnership council, RC3 is well placed to provide increased future value to members in the areas of partnership building, information sharing, and national policy.
--------------	---

As the RC3 continues to develop and evolve, members see opportunities to extend value by continuing to build active regional partnerships, enhance information sharing, and enact national-level critical infrastructure security and resilience policy.

2.1 The RC3 can increase its value to members by expanding partnerships with active organizations and building its reputation as a central source of policy, guidelines, and best practices that actively help regional organizations learn from each other. The RC3 can support partnership building by hosting collaborative events (e.g., Webinars, conferences, exercises) to connect existing regional partnerships, and help RC3 member organizations identify active partnerships with which to collaborate on similar issues. Such events can be supported by RC3 member organizations identifying meeting space and logistical assistance.

2.2 RC3 can develop a more formal process to collect, distribute, and socialize highly valued critical infrastructure security and resilience information among regional partnerships and their government partners. High-impact information that members value and could contribute includes:

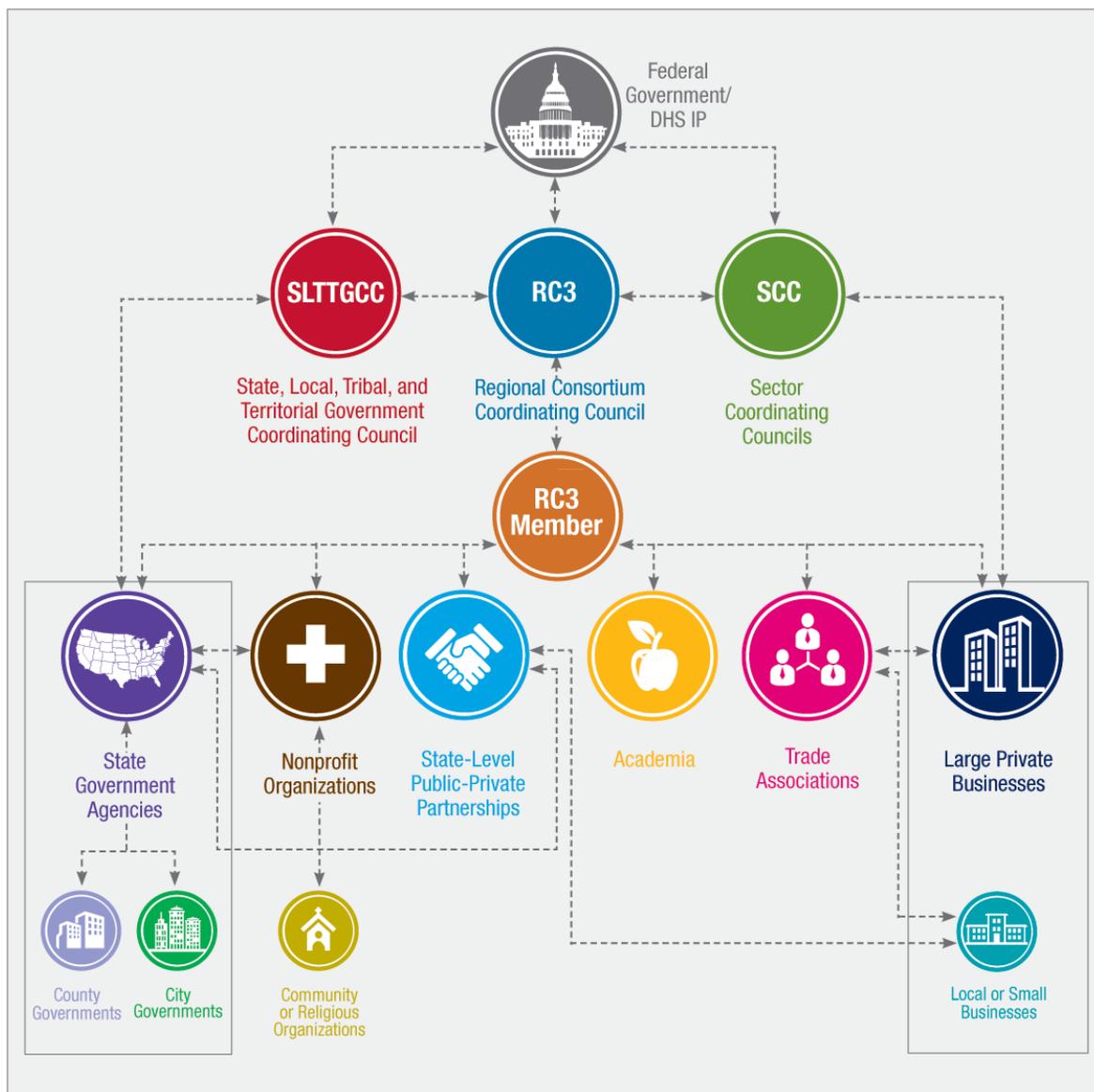
- **Policies, Guidelines, and Best Practices:** Existing critical infrastructure security and resilience planning, preparedness, response, and recovery best practices from regional peers and lessons learned that apply across regions
- **National, State, and Local Asset Registries:** Government and private sector assets and capabilities available for emergency response and recovery
- **Regional Partnerships and Subject Matter Expert Registries:** Existing critical infrastructure security and resilience partnerships and subject matter experts organized by topic or expertise
- **Training and Exercise Opportunities:** Available government and private-sector training and exercises relevant to critical infrastructure security and resilience (especially relating to cybersecurity)

2.3 RC3 can act as a national-level coordinator of separate partnerships to enhance critical infrastructure security and resilience efforts in support of NIPP 2013. In advancing this critical effort, RC3 can help identify and connect existing and new partnerships as well as generate a feedback loop of lessons learned after events so that critical infrastructure security and resilience partners—government and not—can be better prepared for future events.

RC3 Member Organization Composition and Reach

RC3 member organizations represent diverse regions of the Nation, and their work to enhance critical infrastructure security and resilience reflects the distinct characteristics of each region. As a result, members leverage and connect with a varied set of stakeholders—but they each exhibit a valuable capability to connect existing partnerships and expand or build new partnerships to address emerging security and resilience threats and issues. Figure 2 shows how an RC3 member organization may link existing partnerships and diverse stakeholders at the regional and community level, and effectively extend the delivery of Federal policies and programs throughout its partnerships. In addition, RC3 is able to connect its members to the partnership structure established under the 2009 NIPP and reaffirmed in NIPP 2013, which created a mechanism for public-private collaboration. In this way, RC3 member organizations often serve collectively as a highly connected network of networks.

Figure 2. RC3 Member Organizations Act as a Network of Networks



Each region, State, community, and sector has its own distinct set of security and resilience stakeholders, challenges, resources, and capabilities; RC3 member organizations do not partner with a uniform mix of stakeholders. However, they engage stakeholders and interact in common ways.

3.1 Regional partnerships commonly engage non-traditional and community-level stakeholders that Federal agencies or national organizations may not. RC3 member organizations extend beyond the typical government and infrastructure owner/operator base and reach partners largely different from those of national partnerships. Examples include emergency management professionals, small- and medium-sized businesses, non-profits, community groups, Voluntary Organizations Active in Disasters (VOADs), educational institutions, and other local or regional private-sector leaders. As these partners are immediately involved in local response and recovery efforts for incidents, regional organizations collaborate with them to enhance regional resilience.

Member Highlights. In the Northeast, the All Hazards Consortium (AHC) represents a network of more than 15,000 people including representatives from nine State governments, 5 major urban areas, 22 Federal agencies, 78 private-sector entities, and 16 institutions of higher education. The organization also works with 27 nonprofit entities that provide subject matter expertise.

The Bay Area Center for Regional Disaster Resilience (CRDR) utilizes an open membership structure that allows participants from other partnerships to work with the organization on initiatives. Their focus is on facilitating disaster resilience among the various partnerships within the Bay Area, which enables the partnership to draw many participants for various initiatives. Through its “whole community” participants, Bay Area CRDR connects individuals and organizations that may not otherwise communicate. It allows for a larger discussion and a larger pool of expertise and experience to draw from to enhance the security of the Bay Area.

3.2 Trust built over time is the foundation for successful partnerships. Partnerships are based on time-established relationships built on consistent action and regular interaction. RC3 member organizations continuously cultivate stakeholder relationships through joint planning and preparedness activities; training and exercises; public-private collaboration during incidents and emergencies; and sharing best practices.

Partnerships operate most effectively when they have built sustainable relationships and a positive reputation with key partners—elements built over time with consistent action, including between incidents. There is no substitute for time and experience in building partnerships and trust. Day-to-day contact between operational partners is important to partnership sustainment and enables employees at lower levels to implement initiatives more quickly, rather than requiring more formal executive interaction and approval before work can begin.

A key to partnership success is building long-term relationships with innovative leaders and champions in each organization. By providing a forum for the go-getters to successfully make headway on important issues, organizations build a reputation that attracts other motivated leaders and develop relationships with innovative thinkers who continue their partnerships even after they change jobs or careers.

Member Highlights. The Pacific NorthWest Economic Region (PNWER) launched its CRDR following the September 11th attacks as a way to raise awareness about interdependency issues. The center was created more than a decade after member jurisdictions established PNWER by statute (1991) to addresses common issues and interests of the region. The CRDR builds on PNWER’s legacy of working with States, municipalities, private-sector entities, and other regions to build security and resilience. However, the CRDR is focused on a specific aspect of resilience: interdependencies and cascading failures.

ChicagoFIRST credits consistent contact with key partners to build trusted relationships and successfully implement complex multipartner, multiyear efforts, such as its credentialing program, the Business Recovery Access Program.

3.3 Successful partnerships share lessons learned and seek insight from others. Many successful partnerships are able to facilitate information sharing with similar partnerships nationwide. There is a clear desire among RC3 member organizations to share lessons learned and adapt them to needs and issues within an organization’s geographic focus. Rather than a one-size-fits-all approach, the RC3 allows each region to take the best ideas from other regions and adapt them to their own individual needs and issues.

Finding 4 RC3 member organizations are able to reach across jurisdictional and sector boundaries.

RC3 member organizations expand and interconnect not merely along geographic lines but along common threads of supply chains, hazards, and interdependencies. Because RC3 member organizations are not predicated on sector or jurisdictional boundaries, they are able to extend their capabilities and influence by connecting with one another—drawing and building upon others’ expertise and resources. This ability makes them nimble and adaptable to emerging threats and issues. RC3 member organizations collaborate through RC3 on joint projects and shared major issues, such as cybersecurity exercises, border issues, and access credentialing. The activities of RC3 member organizations regarding partnerships generally follow three themes:

4.1 Each regional partnership embraces a network-of-networks approach to partnership building, and many RC3 member organizations are actively involved in helping new partnerships form and evolve in their regions and in other areas of the Nation. Seasoned, established partnerships assist newer organizations by providing best practices and mentoring for stakeholder engagement, mission development, and information sharing.

Member Highlights. Through the Great Lakes Regional Maritime Commerce, Resiliency, and Security Initiative, the Great Lakes Hazards Coalition (GLHC) supports the *Beyond the Border* initiative, an effort sponsored by the U.S. Coast Guard and

Transport Canada for the purpose of bilateral partnering for maritime economic commerce, resilience, and security. The effort will establish new partnerships, create information-sharing conduits, engage stakeholders in response and recovery, and promote resilience for maritime commerce and security. Activities include strengthening maritime public-private communities; hosting bi-national regional meetings, Webinars, and exercises; and producing reports.

ChicagoFIRST was able to develop successful working relationships with city, State, and Federal agencies through day-to-day interactions and conversations. The organization's 27 member firms—which include banks, exchanges, brokerages, securities and future firms, and insurance companies—developed regulatory relationships with city, State, and Federal agencies, such as the Illinois Department of Financial and Professional Regulation and the Securities and Exchange Commission. But ChicagoFIRST is able to make connections outside the regulatory process focused on planning, preparedness, and response to ensure that its member firms, the city, and State are all more resilient. Based on its success, ChicagoFIRST was held up as a model partnership organization, and two dozen other “FIRSTs” have formed across the country. In 2005, ChicagoFIRST formed *RPCfirst* to foster collaboration between the organizations. Through annual meetings, the coalitions share best practices and make additional connections.

As part of the Bay Area Public-Private Partnership Initiative, the California Resiliency Alliance (CRA) is working with the private sector in San Mateo County, Santa Clara County, and the cities of San Jose and Oakland to facilitate pre-disaster planning and partnerships through private-sector committees and Emergency Operation Center (EOC) volunteers. The goal of the initiative is to support disaster response and build more sustainable relationships, communications, and coordination between the private sector and local emergency management agencies.

4.2 RC3 member organizations may establish additional chapters to expand reach in additional communities. Many RC3 member organizations are expanding their influence into the varying communities and jurisdictions of their regions by establishing additional geographic or demographic chapters of their organizations. These new chapters are created to bring public and private stakeholders together from specific rural or urban areas with unique characteristics, as well as specific industries or other economic drivers critical to the region or community.

Member Highlights. The ReadySanDiego Business Alliance is in the process of delineating chapters based on sub-regions within the county. For example, ReadyCarlsbad is a current regional chapter, representing the northern portion of San Diego County. In Alaska, the cities of Anchorage and Juneau are developing chapters of the Alaska Partnership for Infrastructure Protection (APIP) to facilitate location-specific critical infrastructure security and resilience partnerships for Alaska's largest cities.

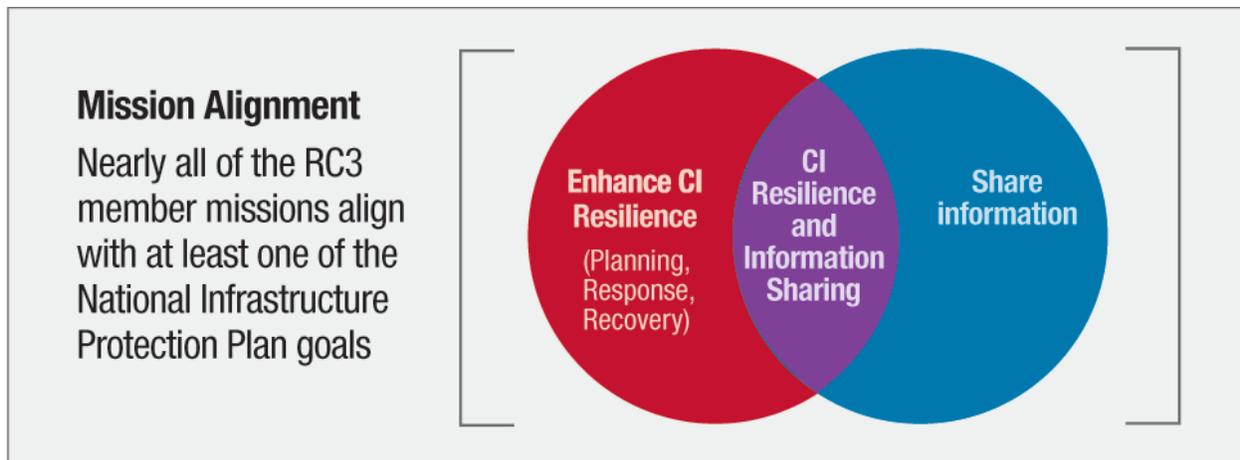
4.3 RC3 member organizations collaborate with existing formal and informal partnerships to leverage and share knowledge and expertise. Each partnership exhibits varying expertise, capabilities, and stakeholders that are leveraged to share information and best practices; host, conduct, and coordinate training and exercises; develop stakeholder relationships; and sponsor conferences and other events. The following examples of collaboration mechanisms were cited as particularly beneficial to RC3 member organization operations:

- Colorado Emergency Preparedness Partnership (CEPP) collaborates with trade associations and similar organizations to hold joint training opportunities to share lessons learned.
- Some RC3 member organizations have strong relationships with the DHS PSAs and actively participate in the NIPP partnership structure (e.g., Sector Coordinating Councils, Government Coordinating Councils, or the State, Local, Tribal, and Territorial Government Coordinating Council).
- Federal Bureau of Investigation (FBI) programs (e.g., offered through InfraGard and Joint Terrorism Task Forces) are leveraged for information sharing and cybersecurity training.
- Urban Area Security Initiative (UASI) partnerships are an example of existing regional collaborative bodies that RC3 member organizations leverage to share knowledge and expertise.

Partnership Mission Areas

The core of any RC3 member organization is its mission. It guides programming decisions, activities, and operations. RC3 member organizations have diverse missions and structures that reflect region-specific partner needs. Despite their diversity, RC3 member organizations share several common themes when it comes to their missions and what drives them in their efforts to improve regional resilience. As exhibited in Figure 3, RC3 member organizations' missions align with national goals to improve critical infrastructure (CI) resilience and information sharing.

Figure 3. RC3 Member Organization Mission Alignment



Note: Based on interviews with 17 RC3 member organizations. Mission areas may align with more than one category.

Finding 5

Most RC3 member organizations develop from the ground up and adjust their missions and activities to reflect regional and stakeholder needs and lessons learned from experience in events.

In most cases, RC3 member organizations were formed as a result of an event that had significant consequences for the region. The event prompted leaders in public and private organizations to connect with one another and address recognized gaps in the community's response and the need for increased coordination to improve security and resilience in the future. These leaders go on to form partnerships that aim to build resilience through information sharing, planning, and training and exercises to better prepare stakeholders, partners, and community ahead of the next event.

When the next event occurs, preparedness planning is put to the test during the response phase. During the recovery, stakeholders (including critical infrastructure owners and operators) identify successes and gaps in their preparedness or response, and take action to fill these gaps—often by growing partnerships with new stakeholders, revising response plans, and launching new training and information-sharing initiatives. In this way, RC3 member organizations continually grow their respective partnerships both by increasing membership and by increasing formal and informal partnerships that improve coordination for planning, response, or recovery. As public- and private-sector members gain experience with the partnership, see it in action, and understand the important role it plays in community security and resilience, the partnership expands, gains prominence, and becomes a crucial part of emergency preparedness and response.

The cyclical process helps RC3 member organizations gain footholds in the communities they serve and improve regional resilience. See Figure 4 for a visual of this process.

RC3 member organizations share a number of common themes regarding their establishment, sustainment, and growth, as discussed below.

5.1 Many RC3 member organizations formed following foundational disaster events that exposed regional needs. Many were established specifically to address needs identified during the crisis and have evolved over time.

- Local events triggered the formation of several regional partnerships. Following the 2003 Northeast Blackout, public- and private-sector representatives in the Great Lakes region recognized the need to coordinate preparedness and response. Furthermore, some organizations are established in recognition of a potential threat. Leaders within the Bay Area community requested a nonprofit forum to address the natural and manmade threats in the region, resulting in the Bay Area CRDR.
- The September 11th attacks were also a turning point for security and resilience in the United States. In the aftermath, DHS was formed to coordinate a comprehensive national security strategy, while stakeholders at the regional level were also forming new organizations and partnerships. ChicagoFIRST was established by 14 major financial institutions in the Chicago-land area to address credentialing, evacuation planning, and private-sector seats at the city's EOC—all identified as issues during the September 11th attacks.

5.2 Steady, diversified funding sources are crucial for RC3 member organization sustainment and growth. Several RC3 member organizations cited money from the Homeland Security Grant Program as a sustaining part of their funding mix. Organizations that cannot sustain their funding mixes are exploring other business models, such as seeking nonprofit status, which allows organizations to access both public and private funding streams.

Member Highlight. For the Safeguard Iowa Partnership (SIP), its nonprofit status has provided flexibility in programming and allows the partnership to sustain operations without relying on unpredictable or restricted public funding. Other organizations, such as ChicagoFIRST, use member dues to fund full-time staff. Some organizations rely on in-kind donations to support training or exercises.

5.3 Emerging issues are integrated into partnership missions and support their evolution. Although events triggered the establishment of many organizations, their missions evolve and build over time to address emerging issues identified in subsequent events and support organizational growth.

Member Highlight. PNWER started its CRDR following the September 11th terrorist attacks to bring first responders up to speed on interdependency issues. Over the years, its mission has evolved, and in 2013, the CRDR mission was noted as providing a nexus between the public and private sectors to build trust and share information.

5.4 Leadership buy-in is crucial for operational employees to move initiatives forward.

Many RC3 member organizations are boots-on-the-ground organizations that uniquely tackle intractable issues and work persistently to resolve them in their regions. This requires buy-in from a combination of senior leadership, public-private executives, and motivated and connected operational employees to move projects forward. Trusted relationships are critical to successful regional partnerships and require support from decision makers. For example, the Bay Area CRDR was successfully formed by the request of State and local government leadership in the region.

Finding 6

RC3 member organizations bridge jurisdictional boundaries, either within their organizations or by partnering with others, to address region-specific needs while leveraging and tailoring national expertise and policies.

The characteristics that make up a region—its population’s size and demographics, major industries, government structures, geographic landscape, and infrastructure—are what make that region distinct. Solutions or policies that improve resilience in one region may not work in another because they do not take into account the reality that particular region faces. RC3 member organizations are uniquely qualified to apply national policies, programs, and expertise in a way that works best for individual regions. The relevant strategies are summarized below.

6.1 Bridging jurisdictional and sector boundaries is a unique capability of regional partnerships. RC3 member organizations have a regional focus and emphasize working across jurisdictions and sectors to solve problems, address interdependencies, and make regions more secure. Regional partnerships focused on common problems have been successful in reaching across jurisdictional lines and enabling entities to work together.

Member Highlight. APIP defines its mission based on supply lines, which means its geographic focus ranges from Alaska and the Pacific Northwest through the Yukon and Northwest Canadian Territories. APIP partners with major multinational corporations, regional business associations, local businesses, volunteer organizations, State agencies, local municipalities, and Federal Government agencies to maintain operations amid threats and disasters. By focusing on the supply chain, efforts transcend typical geographic and jurisdictional boundaries.

6.2 RC3 member organizations network with the right set of diverse partners to address regional needs. RC3 member organizations provide value to stakeholders through their ability to connect partners that would not otherwise interact outside of previously established relationships. They also structure their activities to meet their missions based on what works best and delivers the most actionable products to its partners. Some members structure activities by specific sectors, States, threats, or issues and are flexible enough to change as needed.

Member Highlight. AHC has not changed its central mission, but it has adjusted the way it approaches its mission based on experience. When the organization was founded in 2005, it focused on communications interoperability and coordinating emergency planning and asset procurement between States. Over time, AHC decided more private-sector coordination was needed. With this in mind, it launched the Integrated Planning Initiative in 2011 to identify top critical infrastructure security and resilience issues by sector. In this way, AHC changed the way it carried out its mission from a State-by-

State vendor-sponsored initiative to a sector-by-sector focus and State-sponsored activities.

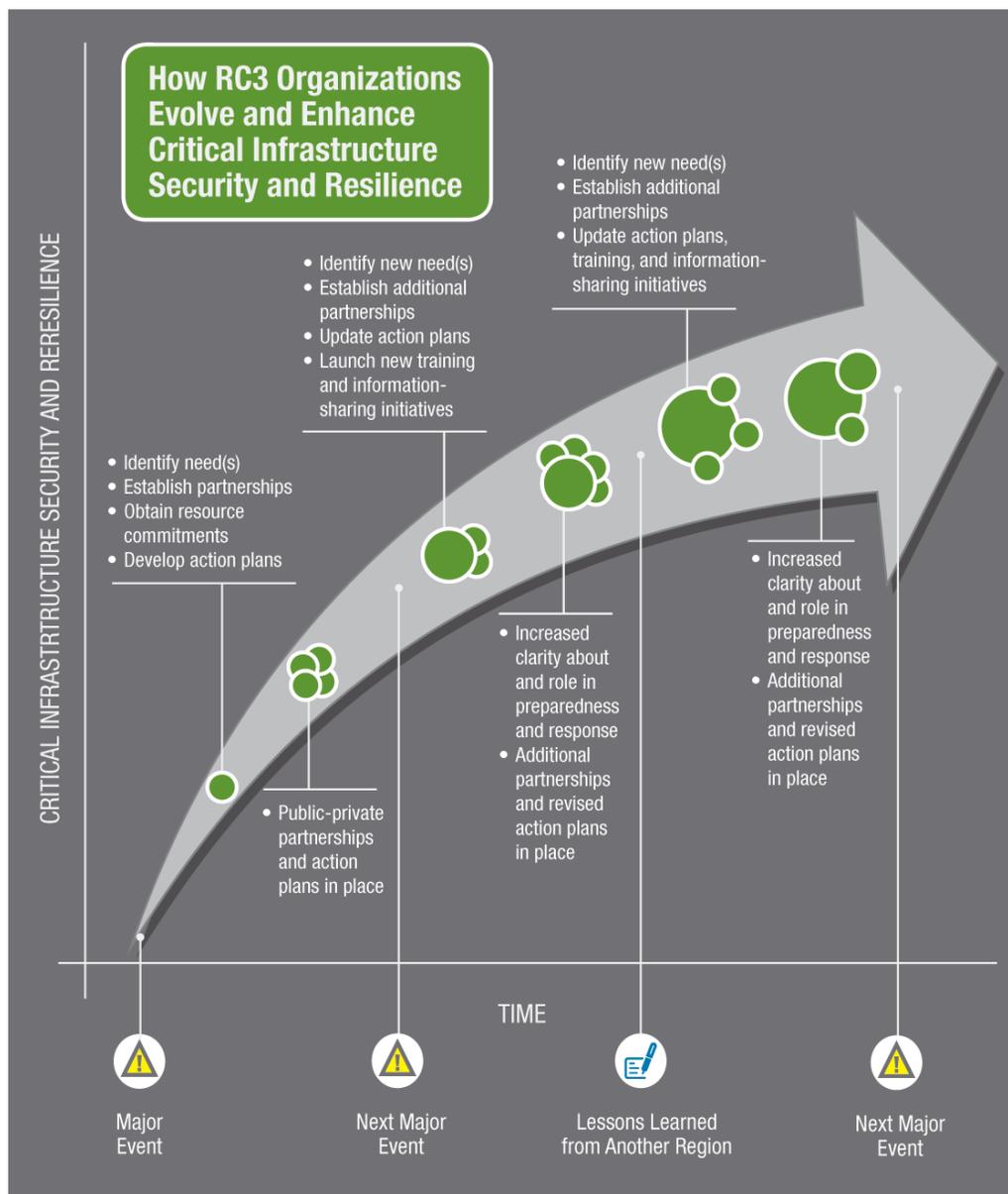
6.3 National expertise and a central approach may be needed for cybersecurity and other expansive topics. Cyber events may have significant local consequences to critical infrastructure, but threats exist at a national or international level and typically require wide coordination. Some organizations are working to address expansive topic areas, but a central national focus may allow regional organizations to be more active in addressing these topics at the regional level.

- RC3 member organizations not involved in specific cybersecurity activities generally leave the technical aspects of cybersecurity to other groups who have the expertise, such as InfraGard and the United States Computer Emergency Readiness Team.
- RC3 member organizations that are focused on cybersecurity aim to increase awareness through operational and pragmatic methods, such as training and education on potential cyber attacks. For example, the Western Cyber Exchange (WCX) uses exercises to raise awareness about the potential region-wide effects of a cyber attack. This helps build support and drive action at the local level.

Critical Infrastructure Security & Resilience Activities

RC3 member organizations pursue a variety of critical infrastructure security and resilience activities with a common goal: delivering high-quality tools, information, training, processes, or programs that markedly improve the way stakeholders are able to prepare and respond to the next threat. For many members, this creates a reinforcing cycle in which the organization gains a reputation for delivering results, which attracts greater participation and resources and enables the organization to grow and continue delivering more value. As the partnership grows, it extends its reach further in the region and creates the potential to widen its effect on regional security and resilience (see Figure 4). RC3 member organizations best deliver value by focusing on partner needs and evolving activities as needs change over time.

Figure 4. How RC3 Member Organizations Evolve



RC3 member organization activities reflect their missions and stakeholder needs, which often include preparedness and response requiring a multi-sector effort at the regional level. RC3 member organizations are well adapted to address cross-sector issues, such as interdependencies and cybersecurity.

7.1 Preparedness and response are key priorities for RC3 member organizations, who are engaging the private sector to concentrate resources and address regional challenges. Across RC3 membership, partnerships are using workshops to uncover lessons learned, mentoring small businesses, and integrating the private sector into Federal and regional planning processes. Nearly all RC3 member organizations are engaged in emergency response activities through asset registry development, alert dissemination, private sector integration into operations centers, and sector information sharing.

Member Highlights. Minnesota InfraGard started the Public-Private Coordination Action Team (P2CAT) in 2007 to formalize a structure and process for information sharing and response coordination between critical infrastructure owners and operators and the public sector. P2CAT reaches out to private-sector members to determine resource availability to fill a need during an emergency. For example, during one flood event P2CAT was able to locate and transport a 20-ton generator. The organization also arranged the movement of animals from a veterinary clinic threatened by flooding, as well as coordinated with companies to provide items for victims of a bridge collapse and the crews working to rebuild it.

Following an EF-5 tornado that hit Joplin, Missouri, in May 2011, the State's Business Emergency Operations Center (BEOC) was activated and, with the Missouri Public-Private Partnership, coordinated private-sector resources and contributions, including working with more than 25 companies and neighboring States to deliver first responder equipment and medical supplies.

7.2 The structure of regional partnerships makes them well suited to address interdependencies, supply chain resilience, and other cross-sector focus areas. RC3 member organizations have been established and grown based on a common identified threat or need among partners. The result is a partnership structure that enables partners to work across jurisdictional boundaries, identify potential interdependencies, and collectively work to broadly reduce risk for all partners. Many RC3 member organizations also use participant-driven working groups or other processes to enable stakeholders to drive organization activities based on high-priority needs.

Member Highlights. APIP, New Jersey Business Force, and AHC all identify supply chain resilience as a priority for their regions. PNWER's CRDR is working with the Puget Sound Regional Catastrophic Planning Team and influential private-sector partners on a project to develop a supply chain resilience public-private sector working group able to provide input and advice on regional supply chain resilience.

The ReadySanDiego Business Alliance uses a bottom-up priority-identification approach that encourages partners to determine what capabilities they need from the County of San Diego to improve their preparedness, rather than having the county dictate needs.

Finding 8 RC3 member organizations adjust activities to meet changing missions and partner needs, with a growing focus on joint exercises, cybersecurity, and information sharing.

As the partnerships have evolved, member activities have adjusted to address changes in mission or emerging needs. The following summarizes key shifts common among multiple members.

8.1 Regional and national exercises are important critical infrastructure activities for RC3 member organizations. Training, planning, and awareness efforts have advanced over the past few years to include an increased focus on joint exercises. RC3 members participate in regional exercises, such as the Great Lakes Hazards Coalition’s 2013 regional tabletop exercise that focused on an improvised nuclear device scenario and involved more than 125 public and private sector participants. The DHS National Level Exercise (NLE) is popular with regional partnerships because it offers an opportunity to contribute a regional perspective to the testing of the Nation’s incident management system.

Member Highlights. RC3 member organizations regularly host training and exercises. In 2013, AHC hosted its first annual Catastrophic Exercise (CATEX) to test catastrophic planning efforts and projects under the Regional Catastrophic Planning Grant Program (RCPGP). The Northeast Disaster Recovery Information X-Change (NEDRIX) conducts at least one timely and topical simulation exercise annually, such as active shooter in the workplace (2013) and integration of cybersecurity, physical security, and business operations (2012).

8.2 Cybersecurity has emerged as a top area of concern for RC3 member organizations. Cybersecurity is a broad issue that transcends jurisdictional and regional boundaries, and the level of focus partnerships place on cybersecurity ranges from leveraging other partnerships and Federal resources to explicit mission dedication.

Several organizations have started to work with private- and public-sector partners to raise awareness about cybersecurity and the potential effect a cyber attack could have on their regions.

Member Highlights. WCX partnered with FEMA, the State of Colorado, the Colorado Emergency Preparedness Partnership, and Colorado Technical University to hold a community emergency preparedness cyber exercise to raise awareness for emergency management personnel about the potential widespread impact of a cyber attack. Many RC3 member organizations said their cybersecurity focus is on developing practical guidance for their members on preventing and responding to an attack.

Through its national network of partners, including 3 million U.S. businesses, the U.S. Chamber of Commerce coordinates outreach to business owners and operators as well as incorporated participants from regional, State, and local government security officials. The organization also stresses the potential consequences of a cyber attack on

businesses, and it calls upon business leaders to better integrate cybersecurity into their organizations' enterprise risk management, emergency or disaster management, business continuity, and cost-benefit decision-making programs.

8.3 Members increasingly leverage technology solutions and information-sharing platforms to deliver timely information to partners. When organizations first formed, many were concentrated on addressing foundational challenges, such as overcoming stakeholder mistrust and developing information requirements. Organizations now embrace information technology systems and tools to advance information-sharing capabilities. In supporting information-sharing efforts, a majority of the organizations work with their State or local fusion center to create information-sharing avenues and collaborate on issues such as examining cybersecurity issues, receiving fusion center bulletins, sharing information for situational awareness, maintaining a private sector liaison to the fusion center, and supporting the development of a critical infrastructure component at the fusion center. In addition, members are leveraging Federal resources—such as the Homeland Security Information Network (HSIN), InfraGard, and FEMA's daily Situation Briefings—in order to disseminate high-quality information and to build information-sharing platforms and are now using social media as a force-multiplier to share information and promote partnership activities.

Member Highlight. NEDRIX public- and private-sector partners are able to access NEDRIX Notify, an automated alert notification tool, to coordinate communication and disseminate real-time information on severe weather, cyber threats, terrorist attacks, and evacuation updates. The tool also allows individual owners and operators to submit information on impacts to operations.

For many RC3 member organizations, having a seat at the State or local emergency operations center facilitates real-time information sharing between the public and private sectors, including how incidents are affecting critical infrastructure owners and operations, the availability of private-sector resources to assist in response, and actionable information that businesses need to make decisions.

Partnership Challenges & Requirements to Grow and Sustain Contribution

RC3 member organizations identified current organization challenges and needs that, if met, could sustain or accelerate partnership activities and broaden their reach. RC3 and DHS IP can address these common requirements to further leverage member contributions to national critical infrastructure security and resilience.

Finding 9

To be sustained or accelerated, RC3 member organizations require sustained funding, increased flexibility in organization, support to address cybersecurity and emerging issues, and a whole community approach.

Each regional partnership has challenges and requirements unique to its mission, stakeholders, and activities. However, common core needs and challenges emerged across the network of RC3 member organizations.

9.1 Dedicated long-term diversified funding is crucial for partnership development, mission and activity sustainability, and training and exercise support. Funding is the most commonly cited need and is indispensable to each organization's ability to create real value for its members in a way that reinforces continued participation to advance effectiveness over time.

- **Sustainment:** Without express long-term funding, even the most effective partnerships may dissolve. Changing life cycles of funding are a challenge to sustaining partnerships. Implications of reduced or eliminated funding and how partnerships have reacted and/or adapted would be valuable best practices to share.
- **Broader Community Value:** Member activities that promote preparedness have positive long-term effects that extend beyond a business into its community and region. Members face difficulty measuring or articulating this shared value and translating it into shared costs.
- **Training and Exercises:** Training workshops and exercises that engage broad participation are widely regarded as one of the most effective tools for mission achievement—but only if they are high-quality and carefully planned, which requires considerable funding.
- **Federal Program Coordination:** By examining and engaging in existing regional programs or capabilities that show promise, DHS IP can avoid developing new programs that may be redundant or have considerable startup costs.

9.2 Partnerships need increased flexibility to organize beyond jurisdictions in ways that make sense to members, connect across existing partnerships, and institutionalize relationships to improve sustainability.

- **Flexibility:** Regional partnerships need the flexibility to evolve, combine, or reconfigure—even if temporarily—along common hazards or supply chains rather than only along geographical boundaries. New organizations or limited partnership engagements could emerge that cut across the existing network of regional partnerships based on a cross-regional common need. Members can build off of current engagements to deliver new value.

- **Federal Support:** DHS IP can continue to support specific projects to identify effective critical infrastructure partnerships, link partnerships, and enable sharing of best practices in a coordinated way. DHS IP could also support personnel to directly build, sustain, or manage regional partnerships.
- **Institutionalizing Relationships:** Informal relationships are not strong enough to ensure critical interaction if a large disaster occurs. Formal relationships and processes must be put into place.

9.3 To address cybersecurity and other emerging issues, partnerships need expert input, clear authorities, robust two-way information sharing, and coordinated exercises and training.

- **Cybersecurity:** Cybersecurity is an incredibly complex issue that does not conform to regional boundaries but is still a top area of concern for RC3 member organizations. Partnerships need expert input on the potential physical, social, and economic consequences of cyber attacks, as well as how to plan for cyber events that could generate significant consequences to regional critical infrastructures.
- **Unclear Authorities:** Cybersecurity and other complex issues create confusion over which stakeholders have authority during emergency events, and how to take proactive measures when impacts and responsibilities are unclear.
- **Information Sharing:** Regional partnerships need accurate, timely, and relevant information to be most effective. DHS can improve information-sharing efforts in the following ways:
 - *Bidirectional information sharing.* Fusion centers and DHS (e.g., IP and the Office of Intelligence and Analysis) should continue to engage in and improve bidirectional information sharing with the private sector.
 - *HSIN improvements.* A mobile version of HSIN would improve usability in emergency incidents, and encouraging daily use would ensure partners can reliably access and leverage HSIN in an emergency.
 - *Information-sharing platform development.* An interactive online information-sharing platform that allows partnerships to share success stories, best practices, and resilience activities would enable information sharing that members value most.
- **Coordinated Exercises:** Large-scale coordinated exercises are vital to improving preparedness. These efforts, such as NLE and other regional exercises, should garner wider support at all levels and encourage stronger engagement from State, local, tribal, and territorial (SLTT) and private-sector security and resilience stakeholders.

9.4 Effective regional partnerships take a whole-of-community approach that best leverages private-sector and non-profit resources and knowledge and responds to local needs.

- **Whole-of-Community Approach:** Public-private partnerships are not exclusive to government and businesses. Nonprofit organizations, academic and research institutions, VOADs, and faith-based organizations remain vital partners. They can mobilize non-traditional resources, extend activities to the local level, and enable

personal and community resilience that supports infrastructure and regional resilience. Members need continued support to engage these partners.

- **Private-Sector Solutions:** Private-sector owners and operators have exclusive insight into infrastructure operations and may have more advanced understanding of threats and hazards than public-sector stakeholders. Regional leaders can expand the private-sector role in planning and risk assessment to encourage cross-sector and adaptable solutions to complex issues.
- **National Registry for Response Activity Support:** A national database of private emergency response resources (e.g., trucks, trailers, generators, and volunteers) would improve response activities, particularly in cross-jurisdictional events or when a State is unable to access resources in its jurisdiction.
- **Local-Level Support:** Increased Federal support for local-level business continuity development leads to better support for local critical infrastructure needs, improved communication of national priorities, and an enhanced whole-of-community approach.
- **National Guidance on Strategic Planning:** Regional organizations continue to value national-level guidance for businesses and SLTT governments to create and improve preparedness and continuity strategies, goals, and objectives.

Member Profiles

Alaska Partnership for Infrastructure Protection		ready.alaska.gov/apip
<p>The Alaska Partnership for Infrastructure Protection (APIP) is focused on improving interoperability and coordination between the public and private sectors to protect critical infrastructure. APIP is one of the primary providers of critical infrastructure security and resilience information in the State. It conducts its information sharing through monthly meetings, the Homeland Security Information Network (HSIN) platform, and a seat at the State Emergency Operations Center (SEOC).</p>		
Geographic Focus	Members	
 <p>State of Alaska</p>	<p>200+ members</p> <p>Private Sector</p> <ul style="list-style-type: none"> Major multinational corporations Regional business associations State- and local- level businesses Volunteer organizations <p>Public Sector</p> <ul style="list-style-type: none"> State departments and agencies Representatives from Federal agencies Municipalities 	
Sector(s) of Focus		
		
Commercial Facilities	Communications	Emergency Services
		
Energy	Food & Agriculture	Healthcare & Public Health
		
Information Technology	Transportation	Water
Establishment		
2005	The Alaska Division of Homeland Security and Emergency Management (DHSEM) consolidated several public-private task forces working on infrastructure protection to form APIP.	
Funding	Governance	Primary Activities
<ul style="list-style-type: none"> Member donations 	<ul style="list-style-type: none"> One public and one private sector co-chair 	<ul style="list-style-type: none"> Information sharing Training and exercises Planning and preparedness

Keys Factors of Partnership Success

- Staffing a seat at the SEOC allows APIP to provide timely, actionable information to private-sector partners and assist in emergency response efforts.
- APIP leverages Federal resources to improve the cybersecurity awareness of its members by regularly collaborating with multiple Federal Bureau of Investigation (FBI) information-sharing organizations to receive information on cybersecurity threats. It also participates in United States Computer Emergency Readiness Team (US-CERT) training to increase cybersecurity awareness.
- Through regular meetings with members and partners, APIP identifies partners’ needs and future training opportunities.

Snapshots of Recent Success

- APIP members hosted and ran a scenario-based exercise in which all electronic financial transactions in Alaska were unavailable due to a disaster. The hypothetical cash-only economy highlighted important interdependencies and led to the State increasing the amount of physical money in circulation and developing contingencies for critical financial information technology systems.
- A disastrous flood of Galena, Alaska in June 2013 required a total evacuation. APIP facilitated rapid restoration of communications for first responders through the SEOC- and private- sector contacts. The SEOC obtained freezers for each household to preserve food, and APIP coordinated the use of a Coast Guard C-17 cargo plane to move goods and people to and from the disaster area.
- APIP successfully facilitated the rapid response to restore rail service through a critical transport artery after a C-17 crash shut down the railroad. Through APIP’s partnership, the response effort was able to quickly remove debris and establish an additional rail line around the site, while allowing the incident investigation to continue. APIP facilitated coordination and cooperation among multiple entities, including the private owner of the rail line, the military facility through which the railroad passes, and Federal and State railroad agencies.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Continuity Planning: APIP assists member organizations with continuity and response planning, including the following: <ul style="list-style-type: none"> – Plan development – Mitigation of conflicts between plans – Integration of plans for cohesion • Understanding Vulnerabilities: Portions of regular APIP meetings are dedicated to advancing member organizations’ understanding of their vulnerabilities and, as a result, developing appropriate continuity and response plans.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Identifying Training Needs: APIP identifies training needs through its meetings and engagements and members decide which organizations could address those needs. Members volunteer their organizations to host and lead new training—in-person and/or remote, Web-based—as APIP sees fit.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Training Topics: Recent training and exercise topics include the following: Methods and capabilities for critical infrastructure resilience, interdependencies, and cybersecurity Information sharing and information management <ul style="list-style-type: none"> – Continuity and response planning – Cybersecurity awareness – Resource management
Information Sharing	<ul style="list-style-type: none"> • APIP Role: Sharing critical infrastructure security and resilience information in Alaska occurs primarily through APIP, which focuses more on the sharing of information than information analysis. • Mechanisms: APIP leverages a variety of methods to share information, including in-person meetings, video teleconferencing, email bulletins, its HSIN-APIP portal, and the SEOC. <ul style="list-style-type: none"> – Monthly in-person, full-day meetings are held from September through May. Members present and discuss current critical infrastructure topics, participate in exercises, and develop strategies for enhancing APIP partnerships. These meetings also include two hours of training (See “Training and Exercises”). – HSIN-APIP is used as a central resource for sharing and updating information during an emergency event. Steady-state information, For Official Use Only information, and analysis relevant to security and resilience are also disseminated via HSIN-APIP in the form of email bulletins and open-source reports. – The SEOC has a position designated for the participation of an APIP member to increase the member’s and APIP’s overall situational awareness. Following activation, email messages sent out by the SEOC also go to APIP members to give members an immediate awareness of the emergency and the details. • Intelligence Information: The Alaska Information and Analysis Center Critical Infrastructure and Key Resources (CIKR) Liaison leverages the center’s intelligence community channels to share relevant threat-information with APIP and DHSEM. • Cybersecurity Information: APIP collaborates on a regular basis with multiple FBI information-sharing groups—including the Joint Terrorism Task Force (JTTF), the Joint Information Sharing Group, and InfraGard—focusing primarily on cybersecurity threats.
Emergency Response	<ul style="list-style-type: none"> • Real-time Information: APIP serves as the central hub of information sharing during an incident to rapidly determine owner and operator needs and the capabilities available through APIP’s membership/relationships to address those needs. APIP leverages the equipment, facilities, and services of its member organizations to facilitate and increase the efficiency of emergency response. For more information see “Snapshots of Recent Success.” • SEOC Seat: An APIP representative is included in the SEOC when activated (See “Information Sharing”).

Critical Infrastructure Activities

Partnerships	<ul style="list-style-type: none"> • FBI: APIP regularly collaborates with InfraGard, the Joint Information Sharing Group, and JTTF regarding cybersecurity information sharing. • State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC): The APIP public sector chair also participates in the SLTTGCC as part of the NIPP 2013 partnership structure.
--------------	---

Organization Background

Establishment, Governance, and Funding

Establishment	The Alaska DHSEM consolidated several public-private task forces working on infrastructure protection to form APIP
Governance	All members are at equal level in the 100-percent, volunteer organization, with two co-chairs—one public sector (DHSEM) and one private sector—leading outreach and coordination efforts to build the partnership.
Funding	APIP operates entirely on the support of its member organizations. Members leverage their organizations’ missions and goals to advance activities in support of APIP.
Members	<ul style="list-style-type: none"> • Private Sector members include major multinational corporations (e.g., AT&T, BP, and ExxonMobil), regional business associations (e.g., hospital and other health provider associations), and State- and local-level businesses (e.g., barge, banking, and communications companies). • SLTT Government: members include major departments and agencies (e.g., DHSEM, the Alaska Department of Transportation and Public Facilities, the Alaska Department of Health and Social Services, and the Alaska Railroad Corporation) as well as local municipalities (e.g., the city of Anchorage, the port of Anchorage, and Anchorage International Airport). • Federal Government members include the U.S. Department of Defense, Federal Emergency Management Agency (FEMA), and FBI. • Volunteer organization members include the American Red Cross and local-level volunteer organizations.

Mission and Objectives

Mission	Improve collaboration and interoperability between the public and private sectors.
Vision	To maintain the continuity of a prosperous Alaska, amid the threat or occurrence of disaster.
Critical Infrastructure Security and	<ul style="list-style-type: none"> • Presenting and recommending critical-infrastructure-relevant information and outreach to all members. • Increasing APIP membership statewide among both public- and private-sector

Organization Background

<p>Resilience Related Objectives</p>	<p>stakeholders.</p> <ul style="list-style-type: none"> • Hosting and providing high-quality training and exercises for members on methods and capabilities for critical infrastructure security and resilience, interdependencies, and cybersecurity. • Encouraging information sharing and management by critical infrastructure stakeholders, including the use and management of the HSIN-APIP portal. • Providing a planning environment for the management of interconnected critical infrastructure supply chains.
<p>Working Groups</p>	<p>State-sponsored Task Forces: Members participate in a variety of State and local partnerships, including State-sponsored Task Forces for catastrophic planning and response. The Task Forces bring together public and private disaster planning and response partners to examine critical needs among sectors or disciplines and develop appropriate preparedness and response plans. APIP members bring information from the Task Forces back to APIP to be shared among its membership. Current active Task Forces include the following:</p> <ul style="list-style-type: none"> • Energy • Healthcare and Public Health • Shelter (an additional priority sector for Alaska due to the particular sheltering needs of the State and its harsh climate) • Transportation • Communications • Search and Rescue • Mass Care • Law Enforcement and Civil Order
<p>Local Chapters</p>	<p>The cities of Anchorage and Juneau are developing APIP chapters to facilitate location-specific critical infrastructure security and resilience partnerships for Alaska’s largest cities.</p>
<p>Points of Contact</p>	
<p>Chair (Public)</p>	<p>Bryan Wuestenberg, DHSEM, Emergency Management Specialist III/CIKR Planner</p>
<p>Partnerships and Programs Leveraged</p>	
<p>Federal Programs</p>	<ul style="list-style-type: none"> • DHS Protective Security Advisor (PSA): APIP members collaborate with the Alaska PSA on vulnerability assessments. • FBI JTTF: See “Information Sharing” and “Partnerships.” • FEMA: APIP uses FEMA preparedness training modules to increase critical infrastructure awareness and resilience. • InfraGard: See “Information Sharing” and “Partnerships.” • Regional Resiliency Assessment Program (RRAP): A recent State-level RRAP was completed for the Energy and Transportation Sectors; it was very well received because it highlighted interdependencies. • US-CERT: APIP uses US-CERT training to increase cybersecurity awareness.

All Hazards Consortium (AHC) is a 501(c)(3) organization focused on helping States and the private sector collaborate on multistate emergency management and disaster recovery/business continuity issues. A broad network of more than 15,000 people in government, the private sector, and several regional working groups delve into specific areas such as multistate power/supply restoration, regional rail security, and communications interoperability. The AHC's Integrated Planning Initiative aims to have the private sector be included in State and local government planning and preparedness projects and vice versa. During the crisis that followed Superstorm Sandy, AHC facilitated an information/data exchange process between the private sector and government that focused on expediting power restoration via fleet movements, support for public safety efforts using social media trends, and real-time situational awareness of private sector resources including the open/closed status of thousands of food, fuel, hotel and pharmacy locations. The data sets of information from the private sector allowed for better coordination and response across the region.

Geographic Focus	Members
 <p>Delaware, Maryland, New Jersey, New York, North Carolina, Pennsylvania, Virginia, West Virginia, and the District of Columbia, along with the UASI areas of New York City; Newark, New Jersey; Philadelphia; Baltimore; and the National Capital Region</p>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; border-radius: 50%; width: 60px; height: 60px; display: flex; align-items: center; justify-content: center; margin-right: 10px;"> 15,000 </div> <div style="text-align: left;"> <p>person network →</p> <p>Partners include representatives from:</p> <ul style="list-style-type: none"> • 9 State governments • 5 major urban areas • 22 Federal agencies • 78 private-sector entities • 16 higher education institutions <p>Subject Matter Experts from:</p> <ul style="list-style-type: none"> • 27 nonprofit entities </div> </div>

Sector(s) of Focus

								
Chemical	Commercial Facilities	Communications	Energy	Financial Services	Healthcare & Public Health	Information Technology	Transportation	Water

Establishment

2005

The AHC was founded to help States collaborate across a wide regional footprint with private sector critical infrastructure owners and operators on multistate issues relative to emergency management, disaster recovery, and business continuity.

Funding	Governance	Primary Activities
<ul style="list-style-type: none"> • State and local government grants • Private-sector funding 	<ul style="list-style-type: none"> • Board of Directors • Regional Working Groups • Executive Director • Executive Director 	<ul style="list-style-type: none"> • Catastrophic event preparedness planning • Critical infrastructure protection and resilience • Public safety communications • Secure information sharing • Business continuity

Keys Factors of Partnership Success

- Several regional working groups focus on specific issues facing the region and guide the organization's activities. The working groups are led and managed directly by the public and private stakeholders giving them control over goals, priorities, outcomes, and direction.
- Trusted relationships are indispensable to the success of major activities that require regional public- and private-sector support. AHC's broad network of more than 15,000 people including State governments, Federal agencies, private-sector entities, higher-education institutions, and nonprofits.
- AHC's Integrated Planning Initiative aims to include the private sector in local emergency planning and preparedness efforts and vice versa.

Snapshots of Recent Success

- Following Superstorm Sandy, AHC combined the collective information available from its private-sector stakeholders to identify and monitor power outages in the region (including food, fuel, pharmacy, hotel, ATM, and communication locations). Sharing this large data set, along with information regarding utility fleet movement through toll stations and other choke points (including requirements, waivers, and operational routes/locations), allowed for better coordination of response. States in the region relied heavily on the AHC for this private sector information.
- Many of the AHC's successes have come as a result of its 2011 Integrated Planning Initiative focused on private-sector involvement in emergency preparedness and response.
- The AHC has been very successful at building and maintaining relationships with leaders who are able to innovate. These relationships have been very important to advancing critical infrastructure security and resilience initiatives. A mark of AHC's success in this regard is its retention of stakeholders even after they have changed jobs or careers.
- The first annual Catastrophic Exercise (CATEX) held in October 2013 was funded by the National Capital Region (NCR) Urban Areas Security Initiative (UASI) and the FEMA Regional Catastrophic Preparedness Grant Program (RCPGP). This exercise project focused on the NCR and tested catastrophic preparedness plans and projects as well as expediting power restoration via regional coordinated fleet movement. Subsequent exercises will focus adding food and fuel sectors to be held in Philadelphia in 2014 and New Jersey/New York City in 2015.

Critical Infrastructure Activities

Planning and Preparedness	<ul style="list-style-type: none">• Integrated Planning Initiative: Launched in 2011, the initiative aims to focus stakeholders on integrating the private sector into State and local planning and preparedness projects, and vice versa. The AHC compiles a running list of regional projects that are funded by States or UASIs. Partners include DHS (including the Federal Emergency Management Agency [FEMA]); State and local governments; and private-sector companies from the Communications, Energy, Financial Services, Food and Agriculture, Healthcare and Public Health, Information Technology, Transportation, and Water Sectors.• RCPGP: AHC facilitates RCPGP workshops and meetings of States that participate in the program, which was developed by FEMA to focus on low-probability, high-impact events. The RCPGP is intended to support coordination of regional all-hazard planning for catastrophic events, including the development of
----------------------------------	--

Critical Infrastructure Activities

	<p>integrated planning communities, plans, protocols, and procedures to manage a catastrophic event.</p> <ul style="list-style-type: none"> • Regional Integrated Planning Working Groups: AHC facilitates several integrated working groups that promote disaster response planning and business continuity planning and solution development. • Regional Workshops: Since 2005, the AHC has hosted nine regional workshops that identified issues, gaps, and recommendations on topics such as catastrophic planning, fusion centers, transportation, geospatial information systems, critical infrastructure security and resilience, ports security, and evacuation planning. • Multi-State Fleet Response Working Group Workshop Report: In January 2013, the AHC partnered with DHS (including the Office of Infrastructure Protection and FEMA), the Commonwealth of Pennsylvania, the State of New Jersey, and several stakeholders of the private sector to assess lessons learned from Superstorm Sandy and identify opportunities for improving movement of fleets in response to emergency events. As part of the workshop, the U.S. Department of Energy held an Energy Roundtable on the effects of the storm on the Energy Sector, focusing on fuel availability. Following the workshop, information was captured in a final report, <i>The Multi-State Fleet Response Working Group Workshop Report: Rapid Critical Infrastructure Restoration Through Joint Integrated Planning For the Movement of Private Sector Resources in Response to Hurricane Sandy</i>. (www.fleetresponse.org)
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Webinars: The AHC hosts regular educational Webinars to raise awareness of operational needs and identify opportunities to leverage resources and investments to expedite business recovery and raise overall community resilience. Last year Webinars focused on the power sector, the aftermath of Superstorm Sandy, the cascading effects of electric power outages, and the cybersecurity threat-landscape. Recorded Webinars are available to stakeholders who are unable to attend the original sessions. • CATEX: AHC UASI jurisdictions test their catastrophic planning efforts and projects through the CATEX as part of the RCPGP. The first annual CATEX exercise, held in October 2013 and funded by the NCR UASI RCPGP exercise project, focused on the NCR. Subsequent exercises will focus on Philadelphia in 2014 and New Jersey/New York City in 2015. • Federal Training Coordination: The AHC keeps its stakeholders informed on up-to-date training opportunities offered by the Federal Government (e.g., FEMA preparedness and continuity training).
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Website: The AHC maintains a Website for information-sharing purposes. Stakeholders also share information with each other directly via email, teleconference, and Webinars. • Regional Situational Awareness Workshop: In August 2012, the AHC, the DHS Science and Technology Directorate (S&T), the New Jersey Office of Homeland Security and Preparedness, and MITRE Corporation hosted a regional workshop

Critical Infrastructure Activities

	<p>focused on situational awareness and information sharing between the public and private sectors during natural and manmade disasters. The results of this workshop enhanced the response to Superstorm Sandy. (See “Snapshots of Recent Success”)</p> <ul style="list-style-type: none"> • Delaware River Infrastructure Protection Project (DRIPP): The AHC facilitated the development of the DRIPP in 2011 to provide situational awareness for government first responders and private-sector critical infrastructure owner and operators situated along the Delaware River. The project’s focus is to provide a regional, interoperable communications network that will allow stakeholders to share vital information on a real-time basis for threat-detection, intelligence analysis, and incident-response management. Key stakeholders in the project include Delaware, New Jersey, and Pennsylvania State and local government officials; the U.S. Coast Guard; and Delaware River owners and operators. • Protecting Sensitive Information: The Personal Identity Verification Interoperable / First Responder Authentication Credential (PIV-I FRAC) Technology Working Group is promoting the use of PIV-I credentialing for the secure transfer of information between critical infrastructure stakeholders. • Verified Identity Based Information Sharing Pilot Project: This project will secure and share sensitive private sector information to support expedited power and critical infrastructure restoration efforts using a federally approved personal identity verification process and promote education of the PIV-I standard. • Electric Sector Fleet Movement Coordination Initiative: The AHC’s Multi-State Fleet Response Working Group developed a multi-State process in 2013 aimed at expediting power restoration efforts on the East Coast. Still under refinement, this process has yielded tangible, measurable success in the Electric Sector by coordinating multiple States with private sector fleets to reduce chokepoints and delays for fleets coming from around the country and Canada to respond to hazards and storms.
Emergency Response	<ul style="list-style-type: none"> • Incident Information Sharing: The AHC serves as an information-sharing hub with private sector for large-scale events in the Mid-Atlantic and Northeast regions. <ul style="list-style-type: none"> – Stakeholders leverage the AHC’s real-time data set of operational fuel, power, and communication locations to enhance incident response. – The Multi-State Fleet Response Working Group facilitates the movement of response fleets across State lines by leveraging its private- sector contacts to prioritize routes, enhance situational awareness, and coordinate regulations. • Fusion and Emergency Operation Centers (EOCs): State fusion centers and EOCs leverage the AHC as a liaison to private-sector critical infrastructure owners and operators for situational awareness. • Federal Response Efforts: The AHC supports Federal response efforts by sharing private-sector data and status information along with supporting the coordination and communication between Federal and private-sector stakeholders.
Partnerships	<ul style="list-style-type: none"> • Trade Associations: The AHC works closely with a number of trade associations (e.g., American Petroleum Institute, Edison Electric Institute, and Fuels Merchants

Critical Infrastructure Activities

	<p>Association) to raise public-sector awareness of potential opportunities for integration with the private sector.</p> <ul style="list-style-type: none"> • Nonprofit Organizations: The AHC draws upon a network of partner associations (e.g., National Governors Association, National Capital Region Planning Group, and Business Executives for National Security) for subject matter expertise. • Pacific NorthWest Economic Region (PNWER): AHC participates in an annual strategic planning session with PNWER to focus on high-level economic issues relative to regional security and resilience. • Regional Catastrophic Planning Team (RCPT) of New York, New Jersey, Connecticut, and Pennsylvania: In the spring of 2013, RCPT hosted three Webinars as part of its ongoing effort to improve the resilience of critical infrastructure in the region. This national discussion series titled “The Cascading Impacts of Electric Power Outages,” featured panel discussions by industry experts and explored regional and cross-sector resilience strategies. The AHC co-hosted the second Webinar, which focused on Federal, State, and local government priorities and expectations from industry during emergency events. Future projects are under development.
Cybersecurity	<ul style="list-style-type: none"> • Planning: The AHC recently introduced cybersecurity into its integrated planning practices and initiatives, focusing on the potential consequences of and operational responses to cyber attacks. Recognizing that cybersecurity is a very broad topic, the AHC’s goal is to develop practical guidance for its stakeholders on preparing and planning for cyber events.

Organization Background

Establishment, Governance, and Funding

Establishment	<p>The AHC was founded in 2005 to help States collaborate across a wide regional footprint on multistate issues relative to emergency management and disaster recovery. AHC States determined that effective disaster preparation, response, and recovery require a coordinated, pre-planned effort that combines private and public resources.</p>
Stakeholders	<ul style="list-style-type: none"> • Stakeholder Total and Types: AHC partners include representatives from nine State governments, 22 Federal agencies, 78 private-sector entities, and 16 institutions of higher education. Through these partners and the 27 nonprofit entities that provide subject matter expertise, the AHC represents a network of more than 15,000 people. Levels of membership include: <ul style="list-style-type: none"> – Government: Qualified State, local, tribal, and territorial (SLTT) and Federal Government employees. – Corporate: Private sector owners and operators of critical infrastructure in the lifeline sectors, such as Energy, Transportation, Communications,

Organization Background

	<p>Food, Water, Retail, and Medical.</p> <ul style="list-style-type: none"> – Other: Solution or technology providers, risk-management organizations, consultants, and manufacturers, research organizations, higher education, as well as organizations that support and promote the efforts of all members in the areas of AHC interests.
Governance	AHC leadership includes a Board of Directors, a Regional Executive Advisory Group, and the Executive Director. All are supported by the AHC Program Management Office staff and volunteers.
Funding	<ul style="list-style-type: none"> • Funding Sources: Capital support for the AHC comes from multiple sources, including State/UASI grants and private-sector funding support for specific efforts and working groups. Federal support is provided by Federal contractors assigned to work with the AHC on specific issues or events. <ul style="list-style-type: none"> – SLTT governments (which are not asked to pay dues) contribute grant funding related to preparedness, homeland security, and emergency management projects and initiatives involving the private sector and multi-State coordination. – Private-sector organizations provide funds in support of working groups and related activities, products, and services offered by the AHC or its working groups.

Mission and Objectives

Mission	<ul style="list-style-type: none"> • To support the efforts of organizations and individuals (public or private) in the Mid-Atlantic and Northeast regions to improve their ability to handle emergencies at the regional, multistate level. • AHC’s overall mission has not changed since its inception. Its conceptual focus, however, has changed over time. What began as a State-by-State focus with vendor-sponsored activities and initiatives changed in 2011 to a sector-by-sector focus with State-sponsored activities and initiatives.
Working Groups	<ul style="list-style-type: none"> • Working Groups: The AHC’s work is accomplished primarily through the activities of its Regional Working Groups. AHC working groups are led and managed directly by the stakeholders, giving the stakeholders control over goals, priorities, outcomes, and direction. Each working group may form subcommittees focused on the specific needs of its stakeholders. These groups currently include: <ul style="list-style-type: none"> – Multi-State Fleet Response Working Group: Focused on expediting power and supply chain restoration efforts via fleet movement across State lines. – PIV-I FRAC Technology Working Group: Focused on exploring the use of PIV-I credentials as a standard for facilitating rapid response access and secure information sharing. – Multi-State Communications Interoperability Working Group: Focused on communications and broadband issues for public safety. – East Coast Corridor Coalition: Focused on broader East Coast issues

Organization Background

	<p>effecting government and the private sector, such as Superstorm Sandy.</p> <ul style="list-style-type: none"> – Regional Rail Security Working Group: Focused on enhancing information sharing between the rail sector; State and local governments; and other lifeline sectors, including electricity, communications, fuel, water, and food. – RCPT Working Group: Focused on multiple projects designed to enhance catastrophic event planning among member States. – Regional Executive Advisory Working Group: Participates in a variety of activities as a governance body, including exercises, training, planning, and program development by leveraging its networks and contacts in support of regional initiatives.
<h3>Points of Contact</h3>	
Personnel	Tom Moran, Executive Director
Board of Directors	Board of Directors include representatives from State emergency management agencies; private corporations, such as a utility and telecommunications company; and universities. The majority represent the public sector.
<h3>Partnerships and Programs Leveraged</h3>	
Federal Programs	<ul style="list-style-type: none"> • U.S. Department of Energy: In January 2013, the U.S. Department of Energy worked with the AHC to conduct public/private panel sessions looking at post-Hurricane Sandy issues related to electricity and fuel issues and produce a report. • FEMA RCPGP: AHC facilitates RCPGP workshops and meetings of States that participate in the program, which was developed by FEMA to focus on low-probability, high-impact events (See “Planning and Preparedness”). • DHS IP: In December 2011, DHS IP worked with the AHC to establish a private sector group to enhance power restoration efforts. This group evolved in the Multi-State Fleet Response Working Group that now provides a proven, multi-State, trusted, legally approved framework that uses integrated planning, training, education, exercises, and joint public/private solution development that help get “businesses back to business” faster, which helps government expedite community and economic resilience. • DHS S&T: In August 2012, AHC, DHS S&T, the New Jersey Office of Homeland Security and Preparedness, and MITRE Corporation hosted a regional workshop focused on situational awareness and information sharing between the public and private sectors during natural and manmade disasters. The results of this workshop enhanced the response to Superstorm Sandy (See “Information Sharing” and “Snapshots of Recent Success”). • UASI: UASI funding was used for the first CATEX in October 2013, along with several other initiatives that support multi-State coordination and private sector integration.

Bay Area Center for Regional Disaster Resilience (Bay Area CRDR) was established after leaders in the region requested a forum focused on uniting disaster resilience efforts across the Bay Area. The nonprofit's open membership allows it to remain a voluntary organization that draw participants from other partnerships for varying initiatives. Through exercises, workshops, and forums, Bay Area CRDR brings together stakeholders to share best practices, improve awareness on key critical infrastructure security and resilience issues, and discuss lessons learned from incidents.

Geographic Focus



San Francisco Bay Area

Members

Bay Area CRDR has adopted an open membership of "whole community" participants

Participants

- Public
- Private
- Nonprofits

Sector(s) of Focus



Dams



Energy



Healthcare & Public Health



Information Technology



Transportation



Water

Establishment

2011

The Bay Area CRDR was established to enable organizations and associations to collectively move toward sustainable regional and community resilience

Funding

- Donations
- Grants
- Project funds

Governance

- Board of Directors
- Executive Director

Primary Activities

- Information sharing
- Training and exercises
- Planning

Keys Factors of Partnership Success

- An open participation model helps facilitate partnerships. The Bay Area CRDR has adopted an open membership of “whole community” participants interested in building a resilient Bay Area. The focus is on facilitating disaster resilience among the various partnerships within the Bay Area, not on building up the Bay Area CRDR’s own membership. This enables the partnership to remain a voluntary organization and draw many participants from other partnerships for varying initiatives. By having open membership, Bay Area CRDR is able to attract participants from other partnerships for various initiatives.
- Leaders in the region established the organization to address a recognized need in the region, based on the natural and manmade threats challenging the region’s resilience.

Snapshots of Recent Success

- In 2012, the Bay Area CRDR partnered with the California Emergency Management Agency (now the California Office of Emergency Services [Cal OES]) to hold a first-of-its-kind meeting to engage public, private, and nonprofit stakeholders in planning leading up to the Golden Guardian 2013 State functional exercise. As a result, there are more engaged and diverse stakeholders interested in participating in the annual exercise.
- In March 2013, more than 200 stakeholders participated in a Bay Area CRDR-hosted event that examined the impacts and preparedness gaps from Superstorm Sandy and the implications for Bay Area disaster resilience.
- As part of a Bay Area Community Health Resilience Forum in February 2014, the Bay Area CRDR brought together “whole community” stakeholders from across the region, Healthcare and Public Health Sector organizations, and key Federal agency partners to raise awareness on regional resilience capabilities and challenges.

Critical Infrastructure Activities

Planning and Preparedness

- **Disaster Resilience Action Plan Initiative:** The Bay Area CRDR partnered with the Association of Bay Area Governments and regional stakeholders, such as the California Resiliency Alliance (CRA), to develop a San Francisco Bay Area Disaster Resilience Action Plan Initiative focused on recovery and long-term restoration. The plan was developed using input from three stakeholder-driven workshops, a survey, and interviews with major regional resilience stakeholders and elected officials.
 - The workshops included a Disaster Resilience Initiative Kickoff Workshop, an Infrastructure Interdependencies Workshop I – Utilities and Transportation Systems, and an Infrastructure Interdependencies Workshop II – Essential Goods and Service Providers.
 - The initiative culminated with four targeted policy papers (Governance, Housing, Infrastructure, and Economy and Business) and an action plan to guide future work in the region to build resilience to major disasters.
- **Bay Area Community Health Resilience Forum:** In February 2014, the Bay Area CRDR brought together “whole community” stakeholders from across the region

Critical Infrastructure Activities

	<p>with Healthcare and Public Health Sector organizations and key Federal agency partners to raise awareness on regional resilience capabilities and challenges.</p> <ul style="list-style-type: none"> • Superstorm Sandy Lessons Learned Workshop: In March 2013, the Bay Area CRDR hosted an event attended by more than 200 stakeholders to examine the effects and preparedness gaps from Superstorm Sandy and the implications for Bay Area disaster resilience. • Community Health Resilience Initiative: In partnership with the U.S. Department of Homeland Security (DHS) Office of Health Affairs and a national stakeholder group of practitioners, the Bay Area CRDR is helping to develop a community health resilience planning template and toolkit of stakeholder-validated best practices, tools, and technologies. The goal of the initiative is to enhance the national resilience for the health effects of all hazards. • Roundtable on Climate Change Effects to Bay Area Energy Assets and Interdependent Infrastructure: The roundtable, sponsored by the Bay Area CRDR and hosted by the East Bay Municipal District focused on coordinating flood mapping and assessment activities in the Bay Area. Federal, State, and local government representatives and the private-sector participants discussed a path forward to collaboratively address rising sea levels and coastal storm surge threats and consequences. • The Infrastructure Security Partnership (TISP): The Bay Area CRDR Executive Director led a Critical Infrastructure and Regional Resilience Task Force of close to 100 practitioners and experts to develop guidelines for regional resilience planning for TISP. The resulting <i>Regional Disaster Resilience Guide Second Edition</i> is currently in use by organizations across the Nation.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Regional Exercises: By developing and facilitating exercises for local agencies and other stakeholder organizations, and supporting established exercises run by both the government and the private sector, the Bay Area CRDR is able to limit redundancies of effort and helps to ensure optimal participation of public, private, and nonprofit partners for regional events. • Energy and Other Lifelines Infrastructure Interdependencies Tabletop Exercise: The Bay Area CRDR with the Alameda County Emergency Managers Association developed and conducted an infrastructure interdependencies tabletop exercise with Pacific Gas and Electric (PG&E), Verizon, and East Bay Municipal Utility District that examined restoration issues with localities after a prolonged power outage event. • Emergency Fuel Tabletop Exercise: The Bay Area CRDR helped San Jose Water Company—along with oil distributors and other key stakeholders—explore post-disaster fuel distribution challenges. • Stakeholder Golden Guardian 2013 Exercise Objectives Meeting: In 2012, the Bay Area CRDR partnered Cal OES to hold a first-of-its-kind meeting to engage public, private, and nonprofit stakeholders in planning leading up to the Golden Guardian 2013 State functional exercise. This has resulted in having more engaged and diverse stakeholders interested in participating in the annual exercise.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • National Guard Exercises: The Bay Area CRDR provided expertise and assistance with stakeholder outreach and engagement in developing the California National Guard’s Exercise in August 2013, which focused on a major Bay Area earthquake scenario.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Bay Area Common Operating Picture (BayCOP) Development: The Bay Area CRDR is collaborating with the Golden Gate Safety Network, the CRA, Carnegie Mellon University’s Disaster Management Initiative, regional utilities, State and local governments, and technical experts to develop a situational awareness tool to support regional response and recovery. • BayCOP Development Workshop: The Bay Area CRDR spearheaded a workshop that brought together both practitioners and experts to hear about BayCOP capabilities and discuss stakeholder situational awareness requirements.
<p>Partnerships</p>	<ul style="list-style-type: none"> • Bay Area Resilience Coalition: The Bay Area CRDR is leading an effort to identify and contact more than 800 diverse organizations focused on preparedness and resilience with the goal of developing an informal but powerful coalition of stakeholders across the Bay Area that have the goal of enhancing the region’s security and resilience. • Critical Infrastructure/Key Resources (CIKR) Bay Area Emergency and Security Information Collaborative (BAESIC): The Bay Area CRDR partnered with San Jose Water Company to create and facilitate a regional lifelines coordination group with water systems, PG&E and other energy companies, and communications providers, to address ways to improve post-event restoration coordination and decisionmaking as well as address other security and resilience issues of mutual concern. • Business Continuity Partnerships: The Bay Area CRDR partners with several regional partnerships focused on business continuity, including the Bay Area Association of Contingency Planners, the Business Recovery Managers Association, the CRA, Carnegie Mellon University’s Disaster Management Initiative, the Association of Bay Area Governments, and chapters of the Building Owners and Managers Association. • Mutual Aid Regional Advisory Committee: The Bay Area CRDR chairs quarterly Cal OES meetings with county and major city representatives, which help Cal OES serve as a conduit for the regional and local perspectives and provide a physical presence for Cal OES functions at the local level in all phases of emergency management. • Disaster Resilience Action Plan Initiative: The Bay Area CRDR partnered with the Association of Bay Area Governments and regional stakeholders, such as the CRA, to develop a San Francisco Bay Area Disaster Resilience Action Plan Initiative focused on recovery and long-term restoration. See “Planning and Preparedness” for more information. • TISP: The Bay Area CRDR Executive Director led a Critical Infrastructure and Regional Resilience Task Force of close to 100 practitioners and experts to develop

Critical Infrastructure Activities

guidelines for regional resilience planning for TISP. The resulting *Regional Disaster Resilience Guide Second Edition* is currently in use by organizations across the Nation.

Organization Background

Establishment, Governance, and Funding

Establishment	A number of leaders in the Bay Area requested that the current Executive Director begin a regional chapter focused on uniting disaster resilience efforts across the region in response to natural and manmade threats and numerous county and local governments with varying governance structures. The Bay Area CRDR was established in April 2011 to enable organizations and associations to collectively move toward sustainable regional and community resilience.
Governance	The Bay Area CRDR is governed by a small Board of Directors with collective experience in business, Federal and State government, healthcare, academia, weapons of mass destruction, nonprofits, and engineering.
Funding	The 501(c)(3) nonprofit organization relies on donations, grants, and project funds to fund two full-time staff members and additional staff for specific projects. For operations, the Bay Area CRDR relies heavily on volunteers and contributions from stakeholders for developing and hosting events—including donating venues—and refreshments.

Mission and Objectives

Mission	To partner with public, private, and nonprofit organizations for the charitable and educational purposes of raising awareness and empowering cross-sector, cross-discipline, and multijurisdictional collaborative action to address all-hazards disasters; health, safety, economic, environmental, and societal consequences; and preparedness gaps and improvement measures.
Goals	Enable organizations and associations with an interest in all-hazards preparedness to collectively move toward sustainable regional and community resilience.
Key Activities	<ul style="list-style-type: none"> • Provides education and training to enable understanding of vulnerabilities and the associated infrastructure interdependencies and consequences of natural and manmade events and disasters. • Builds and fosters regional collaboration and trusted information sharing among diverse organizations and interests. • Works with stakeholders to develop and implement comprehensive, dynamic regional resilience action strategies of priority policy and operational solutions. • Serves as an impartial forum for government, industry, and nonprofit leaders through workshops, exercises, and roundtables to accomplish the following:

Organization Background

- Facilitate multijurisdictional, cross-sector, and cross-discipline cooperation.
- Enable dialogue among practitioners and experts on how to accelerate collective stakeholder progress toward sustainable regional disaster resilience.
- Provides guidance and informational resources to practitioners, experts, and policy makers to help them examine and identify pressing regional and community resilience needs.

Points of Contact

Personnel

Dr. Paula Scalingi, Executive Director
Gerald Kiernan, PhD, Deputy Executive Director and Chief Scientist

Partnerships and Programs Leveraged

Federal Programs

- **Bay Area Urban Areas Security Initiative (UASI):** The partnership leveraged an UASI grant for a specific project on infrastructure resilience.
- **DHS Office of Health Affairs (OHA):** As part of its Community Health Resilience Initiative, Bay Area CRDR partnered with DHS OHA and a national stakeholder group of practitioners to develop a community health resilience planning template and supporting toolkit of stakeholder-validated best practices, tools, and technologies. See “Planning and Preparedness” for more information.

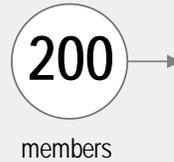
California Resiliency Alliance (CRA) was started in 2005 as a way to connect business and government to improve resilience in the region. One of the biggest ways it accomplishes involving the private sector in preparedness and response through its asset registry, seat at the State Emergency Operations Center (EOC), and its facilitation of private- sector representation at local EOCs.

Geographic Focus



State of California with specific collaboration within the San Francisco Bay Area

Members



Members

- State, county, and city government officials
- Private-sector entities
- Nonprofits

Sector(s) of Focus

CRA focuses on community resilience rather than specific sectors.

Establishment

2005

CRA was started as the Bay Area Business Executives for National Security (BENS) in 2005 to bridge a divide between business and government. The CRA became a stand-alone organization in 2010.

Funding

- Sponsorship from businesses and foundations

Governance

- No information provided

Primary Activities

- Information sharing
- Emergency operations
- Partner education and exercises

Keys Factors of Partnership Success

- CRA provides private-sector members with timely, actionable information during an event because it is an active member in disaster response through its seat at the EOC.
- CRA and its membership demonstrate a strong track record in private-sector integration during incidents. This has been a continual learning process that informs CRA’s response to future incidents. Sustained private-sector involvement in emergency planning and response in the Bay Area has increased trust within the Emergency Services Sector and has led to a willingness to incorporate the private sector in emergency response.

Snapshots of Recent Success

- CRA facilitates private-sector representation in eight Bay Area county and city EOCs during emergencies and exercises by leveraging other regional organizations to staff private-sector liaison positions.
- Sustained private-sector involvement in emergency planning and response in the Bay Area has increased trust within the Emergency Services Sector and led to a willingness to incorporate the private sector in emergency response. See “Planning and Preparedness”
- CRA and its membership demonstrate a strong track record in private-sector integration during actual incidents. This continual learning process informs CRA’s response to future incidents.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Development Plan Workshops: CRA held a series of workshops in early October 2013 to assist in the development of the Bay Area Urban Areas Security Initiative (UASI) Restoration of Critical Lifelines Appendix to the Regional Logistics Plan. These workshops presented an opportunity for CRA members to learn more about their response and restoration responsibilities. Participation from key utilities also helped businesses inform their own business continuity plans. CRA presented the following workshops: <ul style="list-style-type: none"> – Fuel Lifelines Planning Workshop – Water/Wastewater Lifelines Planning Workshop – Power Lifelines Planning Workshop
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Statewide Exercise: CRA regularly participates in California’s annual statewide exercise, Golden Guardian, which assesses emergency operations plans, policies, and procedures for all-hazards/catastrophic incidents at the Federal, State, regional, county, and local levels. In 2013, the Golden Guardian exercise focused on an earthquake scenario in the San Francisco Bay Area. <ul style="list-style-type: none"> – Prior to the exercise, CRA hosted two training Webinars for private- sector participants. These Webinars helped CRA test a social media tool for interoperable chat discussions during an emergency. – CRA also hosted three Webinars to prepare volunteers for various EOC roles and responsibilities exercised during Golden Guardian. • Outreach: CRA promotes county and local exercises to raise members’ awareness of training and exercise opportunities.

Critical Infrastructure Activities

<p>Information Sharing</p>	<ul style="list-style-type: none"> • Situational Reports: CRA provides situational reports to its members to inform their decisionmaking process regarding employee safety and business continuity through a variety of mechanisms: <ul style="list-style-type: none"> – Members are able to access situational reports on the CRA Website – 500 emails contacts, with two-thirds representing the private sector – Regular updates are provided through the newsletter – Considering increase social media use. – Integration of private-sector liaisons in the State and county EOCs • Intelligence Information: CRA successfully advocated for a private-sector liaison at the Northern California Regional Intelligence Center (NCRIC), which was one of the first in the Nation. CRA is on the NCRIC mailing list and is also a participant in the Homeland Security Information Network – NCRIC (HSIN-NCRIC) portal.
<p>Emergency Response</p>	<ul style="list-style-type: none"> • The California Resiliency Alliance Disaster Asset Registry: The registry is a secured database—run by CRA—of pre-identified private-sector resources available to emergency management officials during an emergency, on either a voluntary or paid basis. It connects the emergency management personnel to private sector resources such as trucks, trailers, generators, staging facilities, and communications quickly and effectively during catastrophic events. • Business Operations Center (BOC): As part of its emergency management role, the CRA staffs the BOC during disasters. <ul style="list-style-type: none"> – The State of California has identified a critical need for the organized synchronous exchange of information and resources between public and private-sector organizations in mitigating the effects of, preparing for, responding to, and recovering from disaster events. – To meet that need, the California Office of Emergency Services (Cal OES) co-locates a BOC and a Utilities Operations Center next to the State Operators Center (SOC). This conveys the importance of co-locating private sector and utilities next to the State emergency management structure and facilitates a close working relationship between these entities. – Cal OES signed agreements with private-sector and nonprofit organizations that will provide support to the State during times of crisis. – Since formalizing the partnership through a memorandum of understanding (MOU) in 2008, CRA supported activation of the BOC during various incidents, including the H1N1 pandemic (2009–2010), the release of the Mehserle verdict (2010), and the San Bruno pipeline explosion (2010). • EOC Guide: CRA collaborated with its membership to develop a 2008 Private Sector EOC Representative Activation Guide to formalize the staffing of private volunteers in the BOC. With support from the Bay Area UASI, CRA is currently in the process of updating the activation guide and expects the updated versions to be available in early 2014. • Private-Sector EOC Representation: CRA facilitates private-sector representation in eight Bay Area county and city EOCs during real-life

Critical Infrastructure Activities

	<p>emergencies and exercises by leveraging other regional organizations to staff these private-sector liaisons:</p> <ul style="list-style-type: none"> – Each EOC needs approximately 3–4 volunteers. – To fully maximize its networks, CRA works closely with the Bay Area Response Coalition, the Business Recovery Managers Association, the Bay Area Building Owners and Managers Association, and the San Francisco Bay Area Chapter of the Association of Contingency Planners to identify qualified private-sector volunteers to staff these centers.
Partnerships	<ul style="list-style-type: none"> • Bay Area Public-Private Partnership Initiative: CRA is working with the private sector in San Mateo County, Santa Clara County, and the cities of San Jose and Oakland to facilitate pre-disaster planning and partnerships to support disaster response. The Bay Area UASI provides support for the project. The goal of the Bay Area Public-Private Partnership Initiative is to build more sustainable relationships, communications, and coordination between the private sector and local emergency management agencies. The partnership aims to achieve the following: <ul style="list-style-type: none"> – Launch Private Sector Resiliency Advisory Committees of business and association representatives to inform and continue public-private sector engagement and create a <i>Public-Private Partnership Strategic Plan</i> to serve as a capability-building roadmap. – Recruit and train a team of private-sector volunteers to represent the business community in EOCs, and develop an updated <i>Private Sector EOC Representative Activation Guide</i> to serve as a resource for those representatives. – Organize workshops with businesses and government participants to reinforce cross-sector relationships and gather input on the developed materials and plans. • Private-Sector Role: The State of California signed an MOU with the CRA to integrate the private sector into California’s emergency management system following CRA’s efforts during the 2007 Southern California wildfires. • Trade Associations: CRA collaborates closely with trade associations in its participation with the California BOC. Partners include the California Grocers Association and the California Utilities Emergency Association. • Regional Organizations: CRA functions as a “network of networks” for leveraging the resources and contacts of both trade and regional organizations to better meet the needs of the private sector.

Organization Background

Establishment, Governance, and Funding

<p>Establishment</p>	<p>CRA started as the Bay Area BENS in 2005 to bridge a divide between business and government. CRA became a stand-alone organization in 2010. A number of pivotal moments have driven the CRA’s growth since its establishment:</p> <ul style="list-style-type: none"> • 2005: CRA began working closely with Cal OES on integrating the private sector into the SOC and the State Incident Management System (the statewide version of the National Incident Management System). • 2006: California invited CRA and its private-sector members to observe the Golden Guardian exercise. The State-run exercise simulated a scenario similar to the 1906 San Francisco earthquake to test regional response capabilities. The exercise strengthened recognition of the value of having private-sector representatives in State and local EOCs. • 2007: During the Southern California wildfires, the State requested that CRA set up an ad hoc business desk at the SOC. CRA—along with the California Grocers Association and Wal-Mart—helped coordinate the delivery of supplies from private-sector donors to shelters, further validating the value of the private-sector liaison value to the SOC. • 2008: CRA signed an MOU with Cal OES, formalizing its integration into the State BOC. See “Emergency Response” and “Partnerships” for additional information about the BOC.
<p>Governance</p>	<p>A 501(c)(3) nonprofit, nonpartisan organization</p>
<p>Funding</p>	<p>CRA was originally driven by membership contributions. During the recession, the Alliance turned to a sponsorship model. CRA relies on the generosity of businesses and foundations. No membership fee is required to join or participate; CRA depends on donations to fund its work. Sponsors include financial institutions, a national retailer, utilities, a foundation, and other corporations.</p>
<p>Mission and Objectives</p>	
<p>Mission</p>	<p>The mission of CRA is to improve the following:</p> <ul style="list-style-type: none"> • Economic resilience and business recovery • Community resilience and corporate citizenship • Cross-sector disaster planning
<p>Goals</p>	<p>CRA seeks to improve disaster resilience statewide through effective public-private collaboration.</p>
<p>Critical Infrastructure Security and Resilience Initiatives</p>	<ul style="list-style-type: none"> • Cross-sector coordination • Public health collaboration • Disaster resources • Expertise and technology • Helping partnerships statewide

Organization Background

Points of Contact

Personnel

Peter Ohtaki, Executive Director
Jim Turner, Projects Director
Polly Zebrowski, Project Associate

Partnerships and Programs Leveraged

Federal Programs

- **Bay Area UASI:** Provides support for the Bay Area Public-Private Partnership Initiative.
- **Federal Emergency Management Agency (FEMA) Region IX Private Sector Liaison:** CRA co-organizes events with the FEMA Private Sector Liaison to maximize participation and provide a regional perspective.
- **FEMA's National Business Emergency Operations Center (NBEOC):** FEMA's NBEOC can be an effective information-sharing entity.

ChicagoFIRST connects financial firms through trusted information sharing, and engages the public sector to eliminate joint resilience issues and coordinate financial services emergency planning and operations. Annual tabletop exercises and workshops invite local responders to co-educate and drill on risk scenarios and information sharing. More than a decade of relationship-building has earned ChicagoFIRST and partner organizations two private-sector seats in the Chicago Emergency Operations Center (EOC). Now ChicagoFIRST and the city are finalizing a credentialing program for private-sector responders. With a national reputation, staff advises other cities as they establish a FIRST organization and build sustainable relationships.

Geographic Focus	Members
 <p>Chicago metropolitan area</p>	<p>27 member firms</p> <p>Private Sector</p> <ul style="list-style-type: none"> • Banks • Exchanges • Securities and futures firms • Brokerages • Technology service providers • Energy firms • Insurance companies

Sector(s) of Focus
 <p>Financial Services</p>

Establishment
<div style="border: 1px solid black; border-radius: 15px; padding: 10px; display: inline-block; margin-right: 20px;"> <p>2003</p> </div> <p>Under encouragement from the U.S. Treasury Department, ChicagoFIRST was established by 14 major Chicago-area financial firms to address issues faced during 9/11 attacks: credentialing, evacuation planning, and private-sector participation in emergency operations.</p>

Funding	Governance	Primary Activities
<ul style="list-style-type: none"> • Member dues 	<ul style="list-style-type: none"> • Nine-member Board of Directors 	<ul style="list-style-type: none"> • Operational (e.g., work within the National Incident Management System) • Educational • Information sharing

Keys Factors of Partnership Success

- Information sharing is conducted largely through tight-knit working groups of 20-25 members who have built trusted relationships over time. Three existing working groups include Business Continuity, Physical/IT Security, and a Cybersecurity Roundtable. A Regulation Working Group is being planned.
- Relationships are indispensable to the success of major activities that require regional public- and private-sector support. The success of multiyear, multi-partner efforts, such as ChicagoFIRST's credentialing program, hinges upon the strength of long-term relationships in place.
- Consistent, maintained contact with key partners builds trust and enables operational employees to tackle hard problems with limited direct involvement from senior leaders. Although senior-level engagement and buy-in is critical, direct senior involvement was previously the only way to make traction on complex multi-partner efforts. Now, day-to-day contact reinforces relationships among partners at lower levels and enables them to work together effectively during large projects and emergencies. Part of ChicagoFIRST's success is that members have daily interaction with the Financial Services Sector Coordinating Council (FSSCC), Financial Services Information Sharing and Analysis Center (FS-ISAC), and Government Coordinating Council (GCC).
- ChicagoFIRST classifies its information-sharing benefits in two ways: insurance and investment. "Insurance" information sharing is the information exchange members benefit from simply through membership: emergency alerts, Send Word Now mass communication messages during emergencies, and a password protected Website and message board. "Investment" information sharing comes from joining a working group, investing time, and receiving the value of what comes out of working group deliverables.

Snapshots of Recent Success

- After more than a decade of working with the city of Chicago's emergency response, law enforcement, and other public entities, ChicagoFIRST is finalizing the Business Recovery Access Program (BRAP), a credentialing program that includes a database of credentialed individuals from each member firm. The program puts the onus on ChicagoFIRST members and the private sector to actively participate if they want to have access to critical facilities following an emergency.
- In preparation for the 2012 NATO Summit, held in Chicago, ChicagoFIRST leveraged tools and partnerships to provide detailed information to members, and staffed the EOC leading up to and during the Summit. During Superstorm Sandy, ChicagoFIRST participated in the discussion to determine opening/closing the financial market. The FSSCC and the GCC worked with the organization to relay information to members.
- ChicagoFIRST holds leadership roles in several organizations in Chicago, Illinois, and at the national level. Through this involvement, the organization is able to build relationships, gain valuable information, and provide value to its members.
- ChicagoFIRST is a model for financial sector regional public-private partnerships and supports cities across the Nation in developing their own "FIRSTs." The Intelligence Reform and Terrorism Prevention Act of 2004 identified ChicagoFIRST as a model for financial regional public-private partnerships aimed at protecting employees and critical infrastructure through enhancing communication and coordination focused on business continuity and disaster preparedness. Staff now works to get other FIRSTs off the ground and relay information from RC3 to those that do not have the time or resources to participate in the RC3.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Member surveys: ChicagoFIRST conducts member surveys of best practices and shares results to facilitate member action plans and approaches to emergencies. The surveys aggregate best practices regarding business continuity, evacuations, and emergency telecommuting. <ul style="list-style-type: none"> – February to May 2013: several surveys planned facility closures, procuring hotel space for critical employees, and enhancing communication tools and protocols. – Blizzard of 2011: a series of surveys focused on business continuity.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Although ChicagoFIRST does not have a specific role in conducting training, it does assist in planning and running exercises and workshops. • Annual Tabletop Exercises: Since 2004, ChicagoFIRST has conducted at least one tabletop exercise annually with representatives from all levels of government and the private sector. Exercises span a variety of specific topics and risks, including bomb awareness, multipronged attacks, cyber attacks, and emergency telecommuting. Below are highlights from some of the events over the years: <ul style="list-style-type: none"> – 2013: ChicagoFIRST members along with the Federal Emergency Management Agency (FEMA), the Chicago Department of Public Health, and the Illinois Department of Public Health participated in a workshop on pandemic influenza conducted jointly with the financial community in New York City. – 2011: ChicagoFIRST conducted workshops on corporate communications during an event and on the disruption of light and heavy commuter rail traffic. – 2010: The U.S. Department of Energy and the Chicago Fire Department explained the difference between nuclear and dirty bombs at a ChicagoFIRST workshop and short exercise. ChicagoFIRST and the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) led a workshop/exercise focused on information sharing, which identified gaps in the public and private sector. ChicagoFIRST and InfraGard also conducted exercise on the need for physical security. – 2009: ChicagoFIRST hosted a workshop featuring the Chicago Police Department and the Federal Bureau of Investigation (FBI) about how a multipronged attack could affect financial institutions and ChicagoFIRST held a joint workshop with the Chicago Fire Department on hazardous materials. – 2008: ChicagoFIRST with the FBI, U.S. Secret Service, and InfraGard held a cybersecurity forum and exercise. The event also included discussion of the role the private sector could play following an earthquake and a forum with power and telecommunications experts to discuss resilience and steps that could be taken to address interdependencies. The DHS Office of Cybersecurity and Communications participated in the forum.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Telecommuting Exercise: Since 2010, ChicagoFIRST has conducted an annual telecommuting exercise to test company plans and help prepare employees in the event they are unable to access their normal work space. <ul style="list-style-type: none"> – 4,500 people participated in the 2012 telecommuting exercise. One-quarter of participants noted that the Internet slowed during the exercise. – As a result, ChicagoFIRST is working with the Federal Government to address the issue of Internet operability after a Government Accountability Office report supported the organization’s concerns. • Resource Simulation Exercise: The Regional Catastrophic Planning Team Private Sector Subcommittee, which ChicagoFIRST chairs, held a simulation exercise in 2012 to test the use of a communications tool to coordinate private-sector resources with public sector needs following an emergency. The RCPT includes 16 counties and the principal cities in northeastern Illinois, northwestern Indiana, and southeastern Wisconsin. • Focused Meetings: ChicagoFIRST conducts risk-specific meetings, workshops, and roundtables, inviting private- and public-sector perspectives to help members develop protocols for active shooters, cyber threats, and other risks. <ul style="list-style-type: none"> – Active Shooter: ChicagoFIRST’s 2012 Quarterly Strategic Partners & Members Meeting focused on active shooter preparedness. The meeting included both the public and private-sector perspectives after the ChicagoFIRST Working Group conducted roundtables on the topic. • Distributed Denial of Service Mitigation Program: In response to distributed denial of service (DDoS) attacks in 2011 and 2012, ChicagoFIRST and the Chicago Chapter of InfraGard co-hosted a DDoS Mitigation Program. The program included a keynote address, a demonstration of DDoS tools, and a panel discussion.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Categories: ChicagoFIRST divides its information sharing into two categories: <ul style="list-style-type: none"> – Investment: Shared by actively participating in working groups or other activities. – Insurance: Provided to all members, such as emergency alerts. • Formal Protocols: ChicagoFIRST developed formal, joint information-sharing protocols with State and local emergency response agencies in 2004 to ensure that members receive access to trusted, real-time information. • Networking: Quarterly meetings serve as opportunities to build relationships with other members and the public sector. • Mechanisms: ChicagoFIRST disseminates critical or emergency alert information to members through a number of formal mechanisms. <ul style="list-style-type: none"> – ChicagoFIRST disseminates critical or emergency alert information through an email list. – Members are on an email distribution list and can access a message board on a private, password-protected section of the Website, which includes updates and is used to communicate during significant events when

	<p>ChicagoFIRST staffs the EOC.</p> <ul style="list-style-type: none"> – The Send Word Now emergency notification service allows ChicagoFIRST to automatically call members with a recorded message to provide critical/emergency information or initiate a call/meeting. <ul style="list-style-type: none"> • ChicagoFIRST also uses a permanent conference call bridge and a permanent toll-free call in telephone line where a message can be left for members.
Emergency Response	<ul style="list-style-type: none"> • EOC Seats: ChicagoFIRST arranged to have two private-sector seats at the city’s EOC for varying partnerships in the area, including tourism, universities, retail, and health organizations. <ul style="list-style-type: none"> – ChicagoFIRST’s reputation and relationships with the public sector allow use of one of two seats at the EOC. The organization also participates in activity briefings, operational updates and provides that information using its communication tools. – ChicagoFIRST voluntarily drafted the protocol for how the private sector operates in the EOC. • Credentialing: ChicagoFIRST is finalizing a program with the city for credentialing. The program includes a database where a few people from each member firm can be pre-credentialed. <ul style="list-style-type: none"> – Because it is hard to know who is needed before an emergency occurs, credentialed individuals have the authority to vouch for others to provide essential functions following an event. – The program puts the onus on ChicagoFIRST members and the private sector to register in the database and update that information. – One of the key aspects of the program is its written protocols, which help both the public and private sectors understand what is expected and allowed under the program during an emergency. – ChicagoFIRST recently conducted a field test of the BRAP, with a larger test planned for the first quarter of 2014. • Local Level: ChicagoFIRST coordinates with local officials for small, day-to-day emergencies and for large events. ChicagoFIRST staff is paged 24/7 by the Chicago Office of Emergency Management and Communication’s (OEMC’s) 24-hour Operations Center. • State Level: ChicagoFIRST coordinates with the Illinois State Police and the Illinois Terrorism Task Force for day-to-day and event information. During more significant emergency situations, ChicagoFIRST provides and gathers information through the Illinois State Police’s Statewide Terrorism Intelligence Center (STIC). ChicagoFIRST may also have a seat at the State EOC depending on the size and duration of an emergency. • Federal Level: ChicagoFIRST is a member of the Executive Committee of the FSSCC, the organization through which the financial services industry coordinates with Federal agencies on homeland security and emergency management issues. <ul style="list-style-type: none"> – During Superstorm Sandy, ChicagoFIRST participated in the market open/close consideration discussion. The FSSCC and the GCC worked with the organization to relay information to members.

Partnerships	<p>Organization Involvement: ChicagoFIRST maintains consistent interactions with organizations at the local, State, and Federal level.</p> <ul style="list-style-type: none"> • Local Level: ChicagoFIRST coordinates with local officials for small, day-to-day emergencies, or for large events. ChicagoFIRST staff is paged 24/7 by the Chicago OEMC’s 24-hour Operations Center. • State Level: ChicagoFIRST coordinates with the Illinois State Police and the Illinois Terrorism Task Force for day-to-day or incident information. During more significant emergency situations, ChicagoFIRST provides information and gathers information through the STIC. ChicagoFIRST may also have a seat at the State EOC depending on the size/duration of an emergency. • Federal Level: ChicagoFIRST is a member of the Executive Committee of the FSSCC, the organization that the financial services industry coordinates with Federal agencies on homeland security and emergency management issues.
Cybersecurity	<ul style="list-style-type: none"> • Cyber Threat Workshop: In October 2012, ChicagoFIRST and the FS-ISAC conducted a workshop for members on building a cyber threat-management practice.

Organization Background

Establishment, Governance, and Funding

Establishment	<p>The nonprofit was started in 2003 by 14 major Chicago-area financial institutions to promote resilience by addressing homeland security, business continuity, and emergency management issues that require a coordinated approach among private firms and all levels of government. It was the first of its kind for the financial sector.</p> <ul style="list-style-type: none"> • The U.S. Treasury Department encouraged this type of organization following the September 11th attacks. The firms coalesced around three issues: credentialing, evacuation planning, and a private-sector seat at the EOC (all of which were issues during the September 11th attacks).
Governance	<p>Nine members (including a chair and vice chair) are elected to the Board of Directors.</p>
Funding	<ul style="list-style-type: none"> • Members pay dues to fund the organization’s two full-time employees. • The staff also assists organizations similar to and modeled after ChicagoFIRST that do not have staff by providing information and expertise.

Mission and Objectives

Mission	<p>ChicagoFIRST was formed to accomplish the following:</p> <ul style="list-style-type: none"> • Increase the resilience of the Chicago-area private sector in the event of an emergency, natural disaster, or terrorist event in collaboration with the City of Chicago; the State of Illinois, and Federal agencies, including the U.S. Department of the Treasury, DHS (including IP and FEMA), FBI, and U.S. Secret Service. • Improve the overall preparedness of employers and employees in the Chicago
---------	---

Organization Background

	<p>metropolitan area.</p> <ul style="list-style-type: none"> • Address the interdependencies among critical infrastructure within the Chicago metropolitan area, such as finance, insurance, banking, telecommunications, power, commercial facilities, and water systems. • Collaborate among member firms and with the public sector.
Working Groups	<p>Member Involvement: The working groups are separate from the governance structure, but provide value to the members by fostering discussion and extensive information sharing with specialists from other member organizations. Each working group includes 20-25 people and include:</p> <ul style="list-style-type: none"> • Business Continuity Working Group • Security Working Group • Cybersecurity Roundtable: Started in the fall of 2013 to foster discussions about cybersecurity threats, risks, and programs, at the enterprise level by both IT and business continuity professionals. • Regulation Working Group (pending): ChicagoFIRST plans to add this working group as a forum for members to discuss regulations, including the changes as a result of Dodd-Frank legislation passed in 2010.
Points of Contact	
Personnel	<p>Brian Tishuk, Executive Director Sara Alexander, Deputy Director</p>
Board of Directors	<p>The nine-member board includes representatives from major Chicago-area financial institutions.</p>
Partnerships and Programs Leveraged	
City	<ul style="list-style-type: none"> • Chicago Department of Public Health • Chicago Fire Department • Chicago OEMC • Chicago Police Department • Chicago Office of the Mayor
State	<ul style="list-style-type: none"> • Illinois Department of Financial and Professional Regulation • Illinois Department of Public Health • Illinois Emergency Management Agency • Illinois State Police • Illinois Cyber Task Force • Illinois Terrorism Task Force
Federal Government	<ul style="list-style-type: none"> • Commodity Futures Trading Commission • Federal Deposit Insurance Corporation • Federal Reserve Bank of Chicago • Federal Reserve Board

Organization Background

	<ul style="list-style-type: none"> • InfraGard-Chicago Chapter • Office of the Comptroller of the Currency • Securities and Exchange Commission, • U.S. Attorney’s Office—Northern District of Illinois • U.S. Department of Homeland Security (including FEMA Region V) • U.S. Department of the Treasury • U.S. Postal Inspector Service • U.S. Secret Service
National	<ul style="list-style-type: none"> • Financial and Banking Information Infrastructure Committee • FSSCC • Regional Partnership Council (RPC) • Regional Consortium Coordinating Council (RC3)
Private Sector	<ul style="list-style-type: none"> • American Red Cross of Greater Chicago • Building Owners and Managers Association • FS-ISAC • Financial Services Roundtable • Futures Industry Association • National Futures Association • Securities Industry and Financial Markets Association
Partnerships Founded by ChicagoFIRST	<ul style="list-style-type: none"> • Chicago Public/Private Task Force (CPPTF): In 2010, ChicagoFIRST founded the Chicago Critical Infrastructure Resilience Task Force with the City of Chicago’s OEMC. The Task Force was reconstituted in 2012 as the CPPTF. The task force is working to redevelop the city-wide notification system, NotifyChicago; the BRAP credentialing program; and formalize private-sector participation in the Chicago EOC. • Illinois Terrorism Task Force (ITTF) Private Sector Committee (PSC): ChicagoFIRST helped to found the ITTF PSC in 2004. The committee provides a private-sector perspective on terrorism issues. • RPCfirst: In 2005, ChicagoFIRST formed <i>RPCfirst</i> to foster collaboration between regional organizations similar to ChicagoFIRST. Seventeen out of the 20 such coalitions participated in the sixth annual <i>RPCfirst</i> meeting in October 2013. The meeting allowed participants to share best practices. • Regional Catastrophic Planning Team Private Sector Subcommittee: The subcommittee was formed in 2011 as part of the Regional Catastrophic Planning Team under FEMA’s Regional Catastrophic Grant Program. ChicagoFIRST chairs the subcommittee. In 2012, the subcommittee completed a private-sector integration plan focused on improving public-private communications during and following an emergency and developing a process for identifying private-sector resources and providing the resources to the public sector to assist in recovery from an event.
Federal Programs	Coordinating Councils (e.g., FSSCC, FSGCC, FS-ISAC)

Colorado Emergency Preparedness Partnership (CEPP) was formed to share information across sectors in preparation for the 2008 Democratic National Convention. It has since expanded its mission across the State by working to strengthen the region's capacity to prevent, respond to, and recover from natural and human-caused disasters through public-private collaboration, such as its asset registry.

Geographic Focus



State of Colorado

Members

700+
partners

Partners

- Leaders of the philanthropic community
- Federal, State, and local agencies
- Private sector
- Academia
- U.S. Northern Command

Sector(s) of Focus

CEPP focuses on community resilience rather than a specific sector.

Establishment

2008

CEPP is a collaborative enterprise that was created by the Denver Police Foundation, Business Executives for National Security, and the Philanthropy Roundtable in preparation for the 2008 Democratic National Convention.

Funding

- Donations from philanthropic foundations
- Grants
- In-kind donations from members

Governance

- Board of Directors

Primary Activities

- Preparedness
- Response
- Recovery

Keys Factors of Partnership Success

- An event was the catalyst for the group’s formation, but the success of the partnership allowed it to become a permanent entity and expand. CEPP was established to share information across sectors to aid first responders and emergency management officials in preparation for the 2008 Democratic National Convention. The organization was so successful it became a 501(c)(3) nonprofit and expanded its mission from Denver to encompass the entire State.
- Voluntary asset registries improve resilience because they allow for quick response and accessing all available resources whether they are in the public or private sector. The Cooperative Initiative for Emergency Capability Tracking in Colorado (CONNECT Colorado), the State’s voluntary asset registry, has been put to use to respond to flooding, wildfires, and water plant failures in the State allowing private-sector resources to be accessed as part of the response efforts.
- CEPP partners with State agencies, trade associations, and other established organization to leverage resources. Collaborating with trade associations and other organization to hold joint training opportunities and share lessons learned helps CEPP expand its outreach efforts.

Snapshots of Recent Success

- CONNECT Colorado is a voluntary registry of private-sector business resources such as trucks, equipment, skilled personnel, and power that can be called up by State and local emergency management organizations during disasters. The resource-sharing tool allows for detailed pre-incident planning by sharing substantial private-sector skills and assets that can be used to support State and local government emergency response efforts. Businesses are able to list equipment, services, and personnel that are available for use during an emergency. Colorado statute grants immunity to CONNECT participants, protecting them from liability and easing private-sector apprehension.
 - The asset registry was utilized effectively in Georgetown, Colorado, during a water plant failure. The town requested water storage tanks through CONNECT, and the tool helped the town locate these needed assets on short notice to avert any water shortages. It has since been used to respond to significant wildfire and flooding events in Colorado.
 - CEPP was recognized by the American Academy of Disaster Medicine for its role in developing the CONNECT Colorado resource registry.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Business Continuity Plans: CEPP connects membership with experts who can provide useful information to helps companies write their business continuity plans. • Raising Awareness: CEPP plays a critical role in educating members and nonmembers on the roles, responsibilities, and capabilities of both the public and private sectors. This includes connecting businesses with their local emergency managers to foster useful relationships that are essential to disaster response and recovery. • CONNECT Colorado: The voluntary asset registry and resource-sharing tool, allows for detailed pre-incident planning by sharing substantial private-sector skills and assets that can be used to support State and local government
----------------------------------	---

Critical Infrastructure Activities

	<p>emergency response efforts. See “Emergency Response” and “Snapshot of Recent Success” for more information.</p> <ul style="list-style-type: none"> • Compliance Session: CEPP hosted a session to educate partners on compliance with National Fire Protection Association codes to prevent and manage the effect of wildfires as well as protect member organizations and businesses.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • State Coordination: Colorado partners with CEPP to coordinate State-run exercises, such as tornado drills. CEPP also provides private-sector members with an opportunity to influence and strengthen the early planning, doctrine, exercise, and execution of government response in Colorado. • Simulation Exercise: CEPP played a key role in Colorado’s Vigilant Guard 2013 exercise held in July 2013. CEPP effectively communicated important information to 600+ listserv members in a real-time simulated disaster situation involving multiple incidents. In future disaster situations, CEPP will connect first responders and emergency management personnel with private-sector resources and assistance and act as a supplemental source of information during times of emergency or disaster. • Cyber Exercise: In July 2013, CEPP hosted a simulated cyber exercise for public- and private- sector partners sponsored by the Western Cyber Exchange, Colorado Technical University, and the Canadian Consulate. The exercise—which was attended by approximately 100 participants—involved a cyber attack scenario that began in southern Colorado and spread from a local threat to a national threat. The exercise identified numerous infrastructure interdependencies and vulnerabilities, raising participants’ understanding and better preparing them for potential future cyber events.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Mechanisms: With a focus on pushing rather than pulling information, CEPP primarily relies on its listserv to email its members. The partnership has found this to be more effective than mechanisms where members have to log on to see information. • Situational Awareness Tool: CEPP’s Situational Awareness Tool, hosted by the Colorado Department of Public Health and Environment, can host documents, message boards, and group chats. It can also act as a virtual operations center during an emergency. The tool is primarily used during long-term planning cycles, such as preparing for the pandemic flu. • Fusion Center Coordination: CEPP supports information sharing between the Colorado Information Analysis Center (CIAC) and the public and private sectors. The CIAC occasionally sends out bulletins to CEPP members. • Quarterly Meetings: CEPP hosts quarterly meetings on topics such as private-needs, cyber issues (including detection and awareness), active shooter, personnel surety, wildfires, recovery and restoration, and insurance issues. Sessions have taken place in Denver, Colorado Springs, and Grand Junction (Western Slope). <ul style="list-style-type: none"> – The June 2013 CEPP Western Slope meeting at Colorado Mesa University featured a presentation by a noted expert on workplace and school

Critical Infrastructure Activities

	<p>violence. Attendees included law enforcement, first responders, school personnel, and representatives from public- and private-sector organizations.</p> <ul style="list-style-type: none"> – The Southern Colorado CEPP 2013 winter meeting focused on lessons learned regarding recovering from major disasters, including Hurricane Sandy and the Waldo Canyon wildfire. Panelists leading the discussion included experts from emergency management, the insurance industry, and the American Red Cross.
Emergency Response	<ul style="list-style-type: none"> • CONNECT Colorado: The voluntary registry of private-sector business resources such as trucks, equipment, skilled personnel, and power that can be called up by State and local emergency management organizations during disasters, such as the 2013 wildfires in Colorado Springs. Colorado State statute grants immunity to CONNECT participants, protecting them from liability and easing private-sector apprehension (See “Planning”). • State Emergency Operations Center (SEOC): Staffing a private-sector seat in the SEOC during the 2008 Democratic National Convention raised both public- and private- sector recognition of the value of the partnership in sharing valuable information. Although a primary catalyst for the partnership’s creation, CEPP members do not regularly require a seat in the SEOC during emergencies. CONNECT Colorado is available to SEOC personnel, effectively acting as a communication mechanism between the partnership and the SEOC.
Partnerships	<ul style="list-style-type: none"> • Colorado Homeland Security and All-Hazards Senior Advisory Committee: The CEPP Executive Director was recently appointed to the committee, which is responsible for providing advice and counsel to the State Homeland Security Advisor; formulating recommendations on the State Homeland Security Strategy; reviewing grant funding opportunities; and providing policy guidance to the Division of Homeland Security and Emergency Management. • Counter-Terrorism Education Learning Lab (CELL): CEPP regularly co-hosts major events and speakers with CELL, which is a nonprofit organization dedicated to preventing terrorism through education, empowerment, and engagement. • Local Emergency Planning Committees (LEPCs): To expand outreach to rural parts of the State, CEPP leverages LEPCs that have established relationships with local businesses and emergency management agencies. • Professional Associations: CEPP works closely with professional associations to hold joint training opportunities and share lessons learned. This collaboration helps CEPP expand its outreach efforts.
Cybersecurity	<ul style="list-style-type: none"> • Raising Awareness: CEPP focuses on helping small businesses and nonprofits understand cyber issues, such as understanding the threat, how to protect their organization, and how to respond to a cyber attack.

Organization Background

Establishment, Governance, and Funding

Establishment	CEPP is a collaborative enterprise that was created by the Denver Police Foundation, Business Executives for National Security, and the Philanthropy Roundtable in preparation for the 2008 Democratic National Convention. Initially as a partnership it was formed to share information across sectors to aid first responders and emergency management officials in their preparation efforts, as well as to provide timely and valuable information to businesses about any disruption to their commercial activities. The success of this collaboration spurred the creation of a formal 501(c)(3). CEPP has since expanded its mission beyond Denver to include the entire State.
Governance	CEPP is governed by a board of directors with diverse backgrounds and leadership roles in government and the private sector.
Funding	<p>As a 501(c)(3) organization, CEPP primarily relies on funding from philanthropic foundations, particularly for personnel and operations. The organization aims for three-year funding cycles to aid in partnership sustainment. The following highlights other sources:</p> <ul style="list-style-type: none"> • A Federal Emergency Management Agency (FEMA) grant was leveraged to support CONNECT Colorado, a key CEPP initiative. • No dues are charged to members because the partnership wants to avoid potential impediments to participation. However, members offer in-kind donations, such as meeting space and refreshments.

Mission and Objectives

Mission	The mission of the partnership is to strengthen the region’s collective capacity to prevent, respond to, and recover from natural and human-caused disasters through effective public-private collaboration. This includes educating the private sector on emergency management practices and the public sector on private-sector roles and capabilities. CEPP also aims to create awareness of homeland security/emergency management issues and enable networking among members and nonmembers.
Objectives	Objectives include community resilience and a number of other resilience goals that are a core part of community preparedness concepts.
Path Forward	CEPP continues to expand its outreach and engagement beyond Denver to more rural parts of the State. Specific challenges with expanding outreach include working with small businesses that may not have the time or resources to focus on business continuity and partnering, identifying philanthropies to sustain local partnerships, and holding meetings in disaster-prone areas. As such, better communication platforms are an area of increasing importance in 2014.

Points of Contact

Executive Director	John Mencer
---------------------------	-------------

Organization Background

Board of Directors

The six-member board includes representatives from counter-terrorism organizations, emergency managers, energy companies, and insurance firms.

Partnerships and Programs Leveraged

Federal Programs

- **Federal Bureau of Investigation (FBI):** CEPP recently invited the FBI to present on cyber-intrusion issues. CEPP focuses its engagement with InfraGard exclusively on cybersecurity, specifically on general cyber trends and best practices for use by CEPP membership.
- **FEMA Region VIII:** CEPP collaborates closely with FEMA Region VIII and is actively engaged in its training opportunities and conferences.

Great Lakes Hazards Coalition (GLHC) was formed to coordinate public-private critical infrastructure security and resilience efforts in the Great Lakes region. The Coalition is focused on planning, sharing actionable information and best practices with its partners and conducting regional training exercises. GLHC plays an integral role in facilitating the U.S. and Canadian *Beyond the Border* initiative to build security in the maritime sector in the region by establishing new partnerships, creating information-sharing conduits, and engaging stakeholders.

Geographic Focus



States of Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania, and Wisconsin, as well as the Canadian provinces of Ontario and Quebec

Members

350 →

public and private sector members

Private Sector

- Security directors
- Business continuity planners
- Disaster recovery planners
- Representatives from academic institutions

Public Sector

- Representatives from State, province, urban areas, tribes, local jurisdictions
- Federal partners

Sector(s) of Focus



Communications Energy Food & Agriculture Transportation Water

Establishment

2008

Following the 2003 Northeast Blackout, the Great Lakes' public and private sectors discussed the need for a more coordinated effort to prepare and respond to critical incidents. Coupled with the growing number of regional partnerships across the Nation, this led to an increased recognition of the need for an effective regional public-private partnership. The Coalition was formed in 2008 through the Homeland Security Grant Program (HSGP), beginning with four States and key stakeholders from the private sector.

Funding

- DHS Homeland Security Grant Program
- Donations for specific purposes, such as tabletop exercises

Governance

- The Coalition is governed by a Board of Directors and bylaws.

Primary Activities

- Planning
- Training and exercises
- Information sharing

Keys Factors of Partnership Success

- The GLHC understands the need to involve partners at the regional level and across national jurisdictions.
 - The Coalition hosted a regional virtual tabletop exercise in January 2013 that focused on an improvised nuclear device (IND) event. The exercise included more than 300 participants from more than 125 different agencies, including Federal, State, and local governments; the private sector; and Canadian partners.
 - The Coalition conducted a cross-border, regional tabletop exercise with the National Guard in 2011. An after-action report was developed and presented at the GLHC December 2011 meeting.
- A diversified funding source is needed to maintain consistent operations. The GLHC was established using HSGP funds, but possible reductions in funding threaten to reduce the Coalition’s operations. It is exploring other potential funding opportunities, including pursuing 501(c)(3) nonprofit status.

Snapshots of Recent Success

- The GLHC, in collaboration with the Wisconsin Air National Guard and the Southeastern Wisconsin Homeland Security Partnership, scheduled its 2013 Fall Meeting in Milwaukee. Presentations focused on infrastructure security and resilience as well as underwater infrastructure as an emerging issue.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Sharing Best Practices: GLHC helps companies connect to share their security plans, which spurs the sharing of best practices for building a more resilient private sector across the region. • Interdependencies Study: The Coalition conducted a study on the Energy Sector and its interdependencies in the Great Lakes Region. The report is available to all GLHC members.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Virtual Tabletop: The Coalition hosted a regional virtual tabletop exercise in January 2013 that focused on an IND event. The exercise included more than 300 participants from more than 125 different agencies, including Federal, State, and local governments; the private sector; and Canadian partners. • National Guard Tabletop: The Coalition conducted a cross-border, regional tabletop exercise with the National Guard in 2011. An after-action report was developed and presented at the GLHC December 2011 meeting.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Mechanisms: The Coalition primarily uses email and its Website to share viable, readable information, including best practices and unclassified, publicly-available information of relevance to its partners. Members from academia often suggest documents that may not be readily available via open source. • Intelligence Information: The GLHC collaborates with the Michigan Intelligence Operations Center on cybersecurity issues, but does not currently have a seat in the State and major urban area fusion centers.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Meetings: The GLHC conducts monthly meetings focused on a critical infrastructure sector or homeland security topic. The meetings are conducted via Webinar or in person. • Biannual Conference: Spring and Fall conferences sponsored by the Coalition include participation from all eight States and the two Canadian provinces (See “Snapshots of Recent Success Stories”).
Partnerships	<ul style="list-style-type: none"> • Great Lakes Regional Maritime Commerce, Resiliency, and Security Initiative: In 2011, the United States and Canada jointly announced a bi-national initiative for economic commerce and security called <i>Beyond the Border</i>. Under the initiative, the U.S. Coast Guard and Transport Canada partnered for maritime economic commerce, resilience, and security. <ul style="list-style-type: none"> – First Phase (2011): The greater Seattle-Vancouver region, led by the Pacific Northwest Economic Region Foundation. – Second Phase (2013): The U.S. Coast Guard and Transport Canada asked the GLHC to facilitate the initiative throughout the Great Lakes region. GLHC established new partnerships, created information-sharing conduits, engaged stakeholders in response and recovery, and promoted maritime commerce resilience and security by building maritime public-private communities; hosting bi-national regional meetings, Webinars, and exercises; and producing reports. – Third Phase (2015): The New England and Eastern Canada region is targeted for the last phase of this bi-national initiative. • Southeastern Wisconsin Homeland Security Partnership: The Coalition collaborates closely with State, businesses and local partnerships within the region. For example, the Coalition collaborated with the Southeastern Wisconsin Homeland Security Partnership, Wisconsin Emergency Management, GE Healthcare, and others to organize GLHC’s 2013 Fall Meeting in Milwaukee. • The Infrastructure Security Partnership (TISP): The Coalition’s Chairman spoke at a TISP-sponsored conference in Iowa on community and infrastructure resilience to raise awareness of the partnership and identify new best practices to bring back to members. • Trade Associations: The Coalition leverages partnerships with trade associations for critical infrastructure sectors as conduits for sharing information and best practices.

Organization Background

Establishment, Governance, and Funding

Establishment	Following the 2003 Northeast Blackout, the Great Lakes’ public and private sectors discussed the need for a more coordinated effort to prepare and respond to critical incidents. Coupled with the increase of regional partnerships across the Nation, this
---------------	--

Organization Background	
	led to an increased recognition of the need for an effective regional public-private partnership. The Coalition was formed in 2008 through the HSGP, beginning with four States and key stakeholders from the private sector.
Governance	The Coalition is governed by a Board of Directors and existing bylaws. The Board is represented by various public- and private- sector officials and academia, and it provides strategic guidance for the activities and sustainability of the Coalition.
Funding	The majority of the Coalition’s funding was obtained through the HSGP, which supported the Coalition’s Executive Director and operations. The Coalition also receives donations for specific purposes, such as tabletop exercises. The Coalition is exploring other funding avenues because the grant program is expected to diminish. One option the Coalition is reexamining is pursuing status as a 501 (c)(3) because it could potentially open up new funding sources.
Mission and Objectives	
Mission	A mutually beneficial association of public- and private- sector stakeholders collaborating to reduce the vulnerabilities of the Great Lakes Region for our citizens, communities, and nations. Although this mission has remained consistent throughout the Coalition’s history, implementation has evolved over time to reflect new challenges and obstacles.
Vision	Protecting the future of the Great Lakes Region from all hazards and promoting our collective resilience through effective information sharing.
Goals	<p>The goal of the Coalition is to strengthen communication, collaboration, and planning in the Great Lakes Region in order to enhance the protection, preparedness, mitigation, response, and recovery of the Region's critical infrastructure. The GLHC accomplishes this bi-national goal through the following activities:</p> <ul style="list-style-type: none"> • Promoting and enhancing critical infrastructure and key resources protection and resilience efforts. • Improving information sharing and communication throughout the region. • Providing the foundation for regional cross-sector collaboration. • Enhancing preparedness and response needs.
Path Forward	The Coalition is currently undergoing a self-assessment to update its bylaws and examine its mission, value proposition, and sustainability in light of decreases in HSGP funding.
Points of Contact	
Executive Coordinator	Brit Weber
Board of Directors	The 12-member board includes representatives from State emergency management agencies, a telecommunications company, academia, and two ex-officio members from FEMA Region V.

Organization Background

Partnerships and Programs Leveraged

Federal Programs

- **U.S. Coast Guard Collaboration:** In 2011, the United States and Canada jointly announced a bi-national initiative for economic commerce and security called *Beyond the Border*. Under the initiative, the U.S. Coast Guard and Transport Canada partnered for maritime economic commerce, resilience, and security (See “Partnerships”).
- **HSGP:** The majority of the Coalition’s funding has been obtained through the HSGP, which has supported the Coalition’s Executive Director and operations (See “Funding”).

Minnesota InfraGard, the State chapter of the Federal Bureau of Investigation (FBI) program, works to promote collaboration and information sharing among its members made up of representatives from the public and private sector, academia, and service providers. Through its Public-Private Coordination Action Team (P2CAT), Minnesota InfraGard formalized a process for communication and incident response between the public and private sector before, during, and after an incident.

Geographic Focus		Members	
 <p>State of Minnesota</p>		<p>1,500+ →</p> <p>public, private, nonprofit, and association partners</p> <p><i>All members are vetted by the FBI</i></p> <p>Private Sector</p> <ul style="list-style-type: none"> • Corporations • Academic institutions • Service providers • Information technology consultants <p>Public Sector</p> <ul style="list-style-type: none"> • State law enforcement • Local law enforcement • Emergency managers 	
Sector(s) of Focus			
 Chemical	 Commercial Facilities	 Communications	 Critical Manufacturing
 Dams	 Defense Industrial Base	 Emergency Services	 Energy
 Financial Services	 Food & Agriculture	 Government Facilities	 Healthcare & Public Health
 Information Technology	 Nuclear	 Transportation	 Water
Establishment			
<p>1996</p>		<p>The FBI started the InfraGard program in its Cleveland Field Office in 1996. It started as a local effort focused on information technology and cybersecurity. It has since expanded in its scope and now has chapters across the country, with the FBI's 56 field offices each supporting at least one InfraGard chapter.</p>	
Funding		Governance	Primary Activities
<ul style="list-style-type: none"> • Membership Dues 		<ul style="list-style-type: none"> • Executive Board 	<ul style="list-style-type: none"> • Information sharing • Raising awareness • Training and education • Emergency response

Keys Factors of Partnership Success

- Minnesota InfraGard provides value to its members by sharing timely information and holding meetings on relevant topics. Following NSA contractor Edward Snowden’s release of information, the meeting focused on big data. Prior to the start of tornado season, the monthly meeting was about emergency management.
- P2CAT provides a formal structure for information sharing and response coordination between critical infrastructure owners and operators and the public sector before, during, and after an incident. The team connects private-sector resources with public-sector needs during an emergency.
- As a chapter of an FBI program, Minnesota InfraGard has the backing and support of a well-known agency. This could help it to develop relationships with critical infrastructure partners and broaden the reach of its information-sharing activities and exercises.

Snapshots of Recent Success

- Minnesota InfraGard started P2CAT in 2007 to formalize a structure and process for information sharing and response coordination between critical infrastructure owners and operators and the public sector before, during, and after incidents that involve activation of the Minnesota State Emergency Operations Center (SEOC).
- The P2CAT team reaches out to private-sector members to determine resource availability to fill a need during an emergency.
 - For example, during one flood event P2CAT was able to locate and transport a 20-ton generator. It also arranged the movement of animals from a veterinary clinic threatened by flooding, as well as coordinated with companies to provide items for victims of a bridge collapse and the crews working to rebuild it.
 - The group was first activated during the 2008 Republican National Convention in St. Paul, Minnesota. The SEOC was activated for three days and P2CAT provided real-time information gathering that helped with the State’s coordination efforts.
- P2CAT was awarded the Homeland Security and Emergency Management Award of Excellence for Outstanding Private Partnership in 2011.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Minnesota InfraGard’s Crisis Management Committee: The committee identifies and coordinates preparedness and critical infrastructure protection efforts.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Multistate Exercise: Minnesota InfraGard partnered with the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) and Safeguard Iowa Partnership in 2010 to create and implement the “Northern Lights” exercise. The exercise spanned Iowa, Minnesota, Nebraska, North Dakota, and South Dakota to test critical assets in the region. <ul style="list-style-type: none"> – The scenario-based exercise focused on terrorism to improve awareness about potential threats, identify gaps in information sharing and emergency response, and develop long-term opportunities to improve resilience in the region.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Minnesota InfraGard’s Education and Training Committee: The committee identifies available education and training opportunities and plans InfraGard-sponsored events. <ul style="list-style-type: none"> – Recent examples include raising awareness of available Webinars and trainings provided by DHS (including IP and the Federal Emergency Management Agency) and the Small Business Administration on topics such as insider threats and business continuity planning.
Information Sharing	<ul style="list-style-type: none"> • Mechanisms: Minnesota InfraGard connects with its members and the public using the following mechanisms: <ul style="list-style-type: none"> – Chapter Website: Minnesota InfraGard posts relevant information, including information from sector partnerships and meeting notices. Members are able to connect, create a profile page, and access information posted by Minnesota InfraGard and other members. – Main Website: More high-value information is posted by the FBI on the main InfraGard Website, which Minnesota members are able to access. – Social Media: Minnesota InfraGard uses Facebook, Twitter, and YouTube to interact with members and the public. It uses the site to draw attention to blog posts; relevant resources and information; and events, such as the Minnesota Prepare Fair.
Emergency Response	<ul style="list-style-type: none"> • P2CAT: Minnesota InfraGard created P2CAT in 2007 to formalize a structure and process for information sharing and response coordination between critical infrastructure owners and operators and the public sector before, during, and after incidents that involve activation of the Minnesota SEOC. <ul style="list-style-type: none"> – The idea for P2CAT came from a conversation following a conference in Washington, D.C., but it took several years to put it into action. – P2CAT volunteers must complete emergency management training, take FEMA-sponsored courses on the chain of command and emergency management, and sign up to be a volunteer for a few years. – The team currently consists of seven people, with at least two people deployed to the SEOC during an emergency. – P2CAT reaches out to private-sector members to determine resource availability to fill a need during an emergency (See “Snapshot of Recent Success”).
Partnerships	<ul style="list-style-type: none"> • Minnesota American Society for Industrial Security • Association of Minnesota Emergency Managers • Business Continuity Planners Association • Emergency & Community Health Outreach Minnesota • Hennepin County Emergency Preparedness • International Association of Emergency Managers • Metropolitan Emergency Managers Association • Minnesota Homeland Security and Emergency Management • Minnesota Voluntary Organizations Active in Disaster

Critical Infrastructure Activities

- Ramsey County Emergency Preparedness
- State Emergency Operations Center
- U.S. Department of Homeland Security

Organization Background

Establishment, Governance, and Funding

Establishment	The FBI started the InfraGard program in its Cleveland Field Office in 1996 as a local effort focused on information technology and cybersecurity. It has since expanded in its scope and now has chapters across the country, with the FBI's 56 field offices each supporting at least one InfraGard chapter.
Governance	Minnesota InfraGard is a 501(c)(3) organization sponsored by the FBI to encourage public-private coordination and cooperation to improve the resilience and robustness of critical infrastructure in the region. It is governed by an Executive Board.
Funding	Individual membership dues (\$25). The organization is not able to fundraise but it does accept donations, which often come in the form of event venues being offered for use or beverages and snacks being sponsored/donated for events.

Mission and Objectives

Mission	The InfraGard program, including the Minnesota chapter, fosters collaboration and information sharing to enhance the Nation's ability to address threats to critical infrastructure through a robust public-private partnership.
Goals	<p>The goal of InfraGard, including its Minnesota chapter, is to promote ongoing dialogue and timely communication between members and the FBI, which helps to achieve the following:</p> <ul style="list-style-type: none"> • Increase interaction and information sharing among InfraGard members and the FBI regarding threats to critical infrastructure, vulnerabilities, and interdependencies. • Provide members with value-added threat-advisories, alerts, and warnings. • Promote interactions with local, State, and Federal agencies, including DHS IP and FEMA. • Provide a forum for education and training on relevant topics, such as counterterrorism, counterintelligence, and cybercrime.
Committees	<ul style="list-style-type: none"> • Communications Committee • Crisis Management Committee • Education & Training Committee

Organization Background

	<ul style="list-style-type: none"> • Intelligence Committee • Marketing & Partnerships Committee (under development) • Programs Committee
Points of Contact	
FBI Coordinator	Special Agent Liz Lehrkamp
Deputy Director	Sara Alexander
Board of Directors	Minnesota InfraGard is governed by a 10-member board
Partnerships and Programs Leveraged	
State	<ul style="list-style-type: none"> • Minnesota American Society for Industrial Security • Association of Minnesota Emergency Managers • Business Continuity Planners Association • ECHO Minnesota • Hennepin County Emergency Preparedness • International Association of Emergency Managers • Metropolitan Emergency Managers Association • MN Homeland Security and Emergency Management • Minnesota Voluntary Organizations Active in Disaster • Ramsey County Emergency Preparedness • State Emergency Operations Center
Federal Government	<ul style="list-style-type: none"> • U.S. Department of Homeland Security (IP and FEMA) • Federal Bureau of Investigation
Federal Programs	<ul style="list-style-type: none"> • DHS Protective Security Advisor (PSA): Minnesota InfraGard occasionally works with DHS IP through the local PSA. • FBI: As an FBI program, Minnesota InfraGard works closely with the agency.

Missouri Public-Private Partnership

www.dps.mo.gov/dir/programs/ohs/initiatives/mop3

Missouri Public-Private Partnership (MOP3) fosters private-sector engagement in critical infrastructure security and resilience. The partnership focuses primarily on information sharing, preparedness, and emergency response. MOP3 is the private-sector point of contact for the State's fusion center and it has a seat in the State's Emergency Operations Center (SEOC). These positions allow MOP3 to provide valuable information to both the public and private sector before and during an emergency. Its operation of the private-sector resource registry allows the State's public-sector partners to know what private-sector assets or resources are available, if needed, following an emergency.

Geographic Focus



State of Missouri

Members

250

public and private sector members

Sector(s) of Focus



Establishment

2006

The Missouri Homeland Security Advisory Council (HSAC) authorized MOP3 in October 2006 to foster private-sector engagement to support the State's overall homeland security and emergency management mission.

Funding

- State funding for capital expenditures

Governance

- The chairman, first vice chairman, second vice chairman, and third vice chairman all represent the private sector or nonprofits. Two co-chairs have also been appointed for each critical infrastructure sector.

Primary Activities

- Information sharing
- Emergency response
- Planning

Keys Factors of Partnership Success

- MOP3 recognizes the importance of involving the private sector in disaster preparedness and response. The Business Emergency Operation Center (BEOC) provides direct private-sector expertise to the State during disasters and is co-managed by the Missouri State Emergency Management Agency (SEMA) and MOP3.
- The organization also operates the Missouri Emergency Resource Registry (MERR) is a secure database operated by MOP3 that businesses can voluntarily provide information about resources, including goods, services, equipment, or volunteers that they would be willing to make available during an emergency or disaster.

Snapshots of Recent Success

- Following an EF-5 tornado that hit Joplin, Missouri in May 2011, the BEOC was activated and with MOP3, coordinated private-sector resources and contributions, including working with more than 25 companies and neighboring States to deliver first-responder equipment and medical supplies. The BEOC also assisted in obtaining private company approvals needed to clear debris to stand up staging and disaster response areas.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Planning Guidance: MOP3 provides preparedness and response planning guidance to help businesses understand how best to protect their workplace and employees. • State Plan Assistance: MOP3 plans to assist in the development of the State’s Critical Infrastructure Protection Plan, which will mirror the <i>National Infrastructure Protection Plan</i>.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Participation and Outreach: MOP3 does not host exercises, but it participates in planning, conducts outreach to encourage private-sector participation. Joint training exercises with the public and private sector topics included pandemics such as H1N1, the New Madrid Earthquake, long-term recovery, and disaster response.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Mechanisms: MOP3 uses email alerts, text messages, in-person meetings, events, and its Website to communicate with members. Relevant information received from DHS (e.g., Office of Infrastructure Protection, Office of Cybersecurity and Communications, Office of Intelligence and Analysis, Federal Emergency Management Agency) is forwarded to members as needed. • Quarterly Meetings: Members meet quarterly at the Missouri Office of Homeland Security. Discussion generally focuses on how the State can assist private sector in disaster response. MOP3 is also an authorized recipient within the Missouri Alert Network and members receive notifications. • Resources: MOP3 members have access to the State Homeland Security Information Network (HSIN) site and WebEOC. <ul style="list-style-type: none"> – MOP3 helped to develop private-sector boards for WebEOC.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> – MOP3 is an authorized recipient within the Missouri Alert Network and members receive notifications • Fusion Center Partnership: MOP3 is the private-sector point of contact for the Missouri Information Analysis Center (MIAC), the State fusion center. The MIAC collects, evaluates, analyzes and disseminates information it receives from the private sector and Federal, State, and local agencies. MOP3 has its own secure database on MIAC.
Emergency Response	<ul style="list-style-type: none"> • SEOC: During an event, MOP3 staffs a seat at the SEOC. • BEOC: Missouri SEMA and MOP3 co-manage the BEOC, which provides direct private-sector expertise to the State during disasters. <ul style="list-style-type: none"> – The BEOC rapidly disseminates information, determines the needs and possible solutions, and ensures the fulfillment of critical requirements during an emergency. – The BEOC is activated at the request of SEMA to assist during catastrophic events. MOP3 also has some authority to activate the cells of the BEOC, which include the Critical Infrastructure and Key Resources Cell, Business Disaster Response Cell, and the External Resources Assistance Cell. • The MERR: MOP3 operates the database that businesses can voluntarily provide information about resources, including goods, services, equipment or volunteers, that they would be willing to make available during an emergency or disaster. The MERR uses a secure database accessible only to State and local emergency management personnel and becomes actionable upon declaration by authorized personnel of a disaster or State of Emergency in the State. • Private-Sector Liability: As the private sector increases its role in disaster recovery and response, the State wants to ensure that the private sector and nongovernmental organizations receive the same liability protection as other first responders in the State. To do this, MOP3 is surveying State statutes and legislation regarding public-sector liabilities during an emergency event and plans to push for legislative initiatives to protect the private sector when they assist in response efforts.
Partnerships	<ul style="list-style-type: none"> • Regional Partnerships: MOP3 works with New Jersey Business Force’s Business Emergency Operation Center Alliance and the Safeguard Iowa Partnership.
Cybersecurity	<ul style="list-style-type: none"> • Working Group: MOP3 established a cybersecurity working group led by a private-sector member to start a dialogue and build relationships with Federal agencies. MOP3 members are also available to advise the State on cyber issues as needed.

Organization Background

Establishment, Governance, and Funding

<p>Establishment</p>	<p>The Missouri HSAC authorized MOP3 in October 2006 to foster private-sector engagement to support the State’s overall homeland security and emergency management mission. The State recognized the need for private-sector assistance in disaster preparedness and response following a series of disasters.</p> <ul style="list-style-type: none"> • The Missouri Office of Homeland Security partnered with Business Executives for National Security to develop MOP3. MOP3 is a recognized committee within State government and was formed and chartered as a public-private partnership.
<p>Governance</p>	<p>The chairman, first vice chairman, and third vice chairman represent the private sector or nonprofits. There are also two co-chairs for each critical infrastructure sector.</p> <ul style="list-style-type: none"> • A standing committee made up of private-sector companies and representatives from State agencies is the main coordinating body. • That committee is augmented by a separate committee of representatives from the Urban Areas Security Initiative, national homeland security organizations, and subject matter experts.
<p>Funding</p>	<p>Capital expenditures are funded through the State’s discretionary homeland security funding.</p>
<h3>Mission and Objectives</h3>	
<p>Mission</p>	<p>MOP3 seeks to foster direct public-sector involvement to enhance and support Missouri’s prioritized homeland security and emergency management initiatives.</p> <ul style="list-style-type: none"> • The goal is to increase the private sector’s ability to respond after an incident. • It also improves the State’s situational awareness following an event by enabling it to reach out to critical infrastructure sector MOP3 co-chairs to determine how certain sectors were affected.
<p>Goals</p>	<ul style="list-style-type: none"> • Involve businesses, trade associations, and other nongovernmental organizations as part of the solution to improve the State’s practices, processes, and procedures in support of disaster response; • Provide advice, information, and recommendations on issues associated with Missouri’s Homeland Security Strategy from a private-sector perspective; • Promote the application of best practices to improve the State’s homeland security and response capability. • Collaborate on planning, training and exercise development • Provide a platform for the private sector to address issues and concerns for homeland security and emergency management initiatives.

Organization Background

Points of Contact

Chairman	William Lawson
-----------------	----------------

Partnerships and Programs Leveraged

State Partners	<ul style="list-style-type: none">• Missouri National Guard
-----------------------	---

Federal Partners	<ul style="list-style-type: none">• Federal Bureau of Investigation• U.S. Secret Service• U.S. Department of Homeland Security, Office of Infrastructure Protection (including the PSA)
-------------------------	---

New Jersey Business Force/Business Emergency Operations Center Alliance

web.njit.edu/~beoc/
www.beoalliance.org

New Jersey Business Force (NJBF) was established following the September 11th attacks to strengthen critical infrastructure security and resilience in New Jersey by connecting businesses, academia, and government. The organization was the first of its kind and served as a model for similar organizations across the Nation. NJBF helped create the Business Emergency Operations Center Alliance (BEOC Alliance) to build collaboration and communication between the public and private sector before and during emergencies.

Geographic Focus	Members
 <p>NJBF focuses on the Philadelphia and New York-New Jersey metropolitan regions. The BEOC Alliance is a national organization based in New Jersey</p>	<p>59 → NJBF members</p> <p>37 → BEOC Alliance members</p> <p>Representatives from:</p> <ul style="list-style-type: none"> • State agencies • Healthcare providers • Utilities • Corporations • Partnerships <p>Members</p> <ul style="list-style-type: none"> • Present • Former

Sector(s) of Focus

No specific sector identified. NJBF and the BEOC Alliance focus on community-level issues, such as supply chain, value chain, and resilience, in a cross-sector, cross-discipline approach. Outreach is targeted not only to owners and operators, but also to other businesses not otherwise connected to national organizations.

Establishment

2003

NJBF Establishment: NJBF was launched in 2003 by the Business Executives for National Security (BENS) to strengthen homeland security following the September 11th attacks.

BEOC Alliance Establishment: The BEOC Alliance was created as a collaboration between partners, including academia (led by New Jersey Institute of Technology [NJIT]); business (represented by NJBF); and government organizations like the Armament Research Development and Engineering Center (ARDEC) at Picatinny Arsenal, New Jersey.

Funding	Governance	Primary Activities
<ul style="list-style-type: none"> • Member dues • Contributions • Grants 	<ul style="list-style-type: none"> • Governance Committee 	<ul style="list-style-type: none"> • Education • Applied research • Information sharing • Community outreach

Keys Factors of Partnership Success

- NJBF and BEOC Alliance status as nonprofit organizations allow them to pursue diversified funding sources. Nonprofit status gives both NJBF and the BEOC Alliance flexibility and independence to pursue initiatives based on their priorities.
- NJBF and the BEOC Alliance provide partners with timely information necessary for informed decisionmaking. Businesses operate on a different decisionmaking cycle and need different information before, during, and after an event.
- With connections to universities and research institutions, NJBF and the BEOC Alliance are able to share applied research with private-sector entities, allowing the entities to test the effectiveness of the findings in their operations. NJBF describes this process as “information sharing through interoperability.”
- NJBF and BEOC Alliance personnel serve as subject matter experts by observing and providing advice on company preparedness and business continuity discussions and helping companies develop and run exercises. This could help in developing relationships prior to incidents.

Snapshots of Recent Success

- NJBF and the BEOC Alliance helped define the BEOC concept and developed a capabilities matrix. The BEOC Alliance states that it is “evolving into a national collaborative model for private-sector information sharing and is being further developed as an information-sharing exchange between the private sector and public sector during emergency management scenarios.” This model can be replicated in other regions, across the Nation, or in other countries.
- NJBF and the BEOC Alliance cite their ability to have an influence during a crisis as one of their biggest successes, such as their activities following Superstorm Sandy:
 - Local officials worked with Amtrak, a BEOC Alliance partner, and the Federal Emergency Management Agency (FEMA) to bring supplies to Newark, New Jersey by adding train cars to Amtrak’s Northeast Regional route.
 - Collaborated with America Recovers to transport supplies and clothing by rail from Connecticut to Newark, NJ for delivery to New Jersey communities affected by Superstorm Sandy.
 - Provided “on-the-ground” assessments to other nongovernment organizations outside of New Jersey
 - Students embedded in the New Jersey EOC during the storm shared their lessons learned with the private sector through NJBF and BEOC Alliance engagements.

Critical Infrastructure Activities

Planning and Preparedness	<ul style="list-style-type: none"> • Subject Matter Experts: NJBF and BEOC Alliance personnel serve as subject matter experts by observing and providing advice on company preparedness and business continuity discussions and helping companies develop and run exercises.
Training and Exercises	<ul style="list-style-type: none"> • Exercise Involvement: Since 2003, NJBF hosts, helps organize, and participates in a number of exercises, roundtables, and conferences. <ul style="list-style-type: none"> – A partnership between the NJIT and the ARDEC at Picatinny Arsenal allows NJBF and the BEOC Alliance access to the ARDEC facility to hold

Critical Infrastructure Activities

	<p>training, modeling, and simulations.</p> <ul style="list-style-type: none"> – An upcoming exercise will focus on unmanned aerial vehicle systems and how they can provide situational awareness following a catastrophic event, including communications relay, imaging, and mapping. <ul style="list-style-type: none"> • U.S. Department of Homeland Security (DHS) Top Officials (TOPOFF) Program: NJBF regularly participates in the TOPOFF program, which involves seminars, planning sessions, and a comprehensive assessment of the Nation’s capacity to prevent, prepare for, respond to, and recover from terrorist attacks or catastrophic disasters. <ul style="list-style-type: none"> – The Looking Glass Exercise was conducted in October 2007 as part of the TOPOFF program and included 15 private sector and nonprofit organizations, and 10 representatives from county, State, and Federal governments. The exercise tested the ability to execute the functions of the BEOC following an emergency.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Addressing Member Needs: Businesses operate on a different decisionmaking cycle than government; therefore, they need different information before, during, and after an event. This is particularly true if a corporation has facilities or employees outside the region or Nation. NJBF and the BEOC Alliance provide partners with the timely information necessary for informed decisionmaking. • Mechanisms: The BEOC Alliance and NJBF share information with members through email alerts (to more than 400 recipients); text messages; quarterly meetings, monthly teleconferences on planning, special events, or other relevant topics; seminars on topics such as hurricane scenarios; and a secure information-sharing Web-portal. <ul style="list-style-type: none"> – Alert messages and situation briefs are compiled based on regional reports and daily critical infrastructure reports posted by DHS (e.g., Office of Infrastructure Protection, Office of Cybersecurity and Communications, Federal Emergency Management Agency) and disseminated daily to the BEOC Alliance and NJBF networks. – Twice a month, NJBF disseminates awareness notes to members on a variety of topics, including cybersecurity, terrorism, public health, and natural disasters. – The BEOC Alliance holds weekly research meetings to discuss public- and private-sector information sharing. – At annual conferences, information is presented on topics such as active shooter preparedness and response, a Superstorm Sandy – The NC4 CyberCop Portal provides a secure platform for sharing sensitive information. Members are vetted before they receive a username and password. The BEOC Alliance used CyberCop when it provided support to the Colorado Emergency Preparedness Partnership during the 2008 Democratic National Convention and continued to use it following that event.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Applied Research: With connections to universities and research institutions, NJBF and the BEOC Alliance are able to share applied research with private-sector entities, allowing the entities to test the effectiveness of the findings in their operations. NJBF describes this process as “information sharing through interoperability.” • Emergency Notification Platform: NJIT heads the BEOC Technology Committee under its role as the State of New Jersey Homeland Security Technology Center. The goal is to integrate existing technologies into an effective platform to be used during an emergency to provide notifications and alerts, collaboration, communication, incident management support, modeling and simulations, and integration with other regional partners.
Emergency Response	<ul style="list-style-type: none"> • BEOC: The BEOC is a private-sector organized, managed, and staffed emergency coordination/operations center focused on all-hazards disaster prevention, preparation, response, and recovery. Its goal is to make the private sector self-reliant and self-sufficient during emergencies and disasters. <ul style="list-style-type: none"> – The BEOC functions as a private-sector version of a fusion center, conducting many of the same functions including notifications, intelligence analysis, communications, incident management, planning, and collaboration for shared situational awareness. • Volunteer Partnerships: A memorandum of understanding was signed with World Cares Center (WCC) in New York City to administer the volunteer component of the BEOC. WCC is a nonprofit organization specializing in the training, management, and effective use of spontaneous volunteers. • Pilot Project: Using data on 10,000 Walgreens stores, The BEOC Alliance facilitated the real-time mapping and reporting of assets and services. This pilot project is now being examined for applicability to other types of data, assets, and services.
Partnerships	<ul style="list-style-type: none"> • Regular Partners: NJIT, ADP, Prudential, MSA Security, Mutualink, NJ Edge, American, Aerospace Advisors, Inc., NJ Resources, Bank of America, Atlantic Health Systems, SAIC, NC4, Safeguard Iowa Partnership. • Regional Consortium Coordinating Council (RC3): NJBF and BEOC Alliance use their RC3 membership to stay informed on critical infrastructure security and resilience issues. • FEMA Personnel: Personnel involved with Emergency Support Function 15 – External Affairs (e.g., the FEMA Private Sector Office) aid the organization in expanding its network of contacts. • Associations: NJBF and BEOC Alliance leadership are active in several State boards and associations, including State emergency management associations, the New Jersey Domestic Security Preparedness Planning Group, Burlington County Office of Emergency Management, and chapters of the Association of Contingency Planners and ASIS International. Through interactions at conferences and on conference calls, NJBF and BEOC Alliance leadership build

Critical Infrastructure Activities

	relationships with the organizations they are able to leverage during a crisis. By developing relationships with people in these organizations, they are able to maintain connections if the contacts switch jobs.
Cybersecurity	<ul style="list-style-type: none"> • Education and Outreach: NJBF and the BEOC Alliance have recently increased their activities related to cybersecurity. The approach includes studying it as asymmetric warfare, learning more about the issues, and focusing education and outreach to the private sector concerning prevention and what to do in the event of a cyber attack.

Organization Background

Establishment, Governance, and Funding

NJBF Establishment	<p>NJBF was launched in 2003 by BENS to strengthen homeland security following the September 11th attacks.</p> <ul style="list-style-type: none"> • The founding NJBF members represent the organizations and business leaders that met following the attacks to discuss the need for a working relationship between the private sector and government. • NJBF was the first business force established. • In 2009, NJBF transitioned from BENS to regional sponsorship under NJIT until it received 501(c) (3) status through the BEOC Alliance.
NJBF Member Types	<ul style="list-style-type: none"> • Representatives from State agencies, healthcare providers, utilities, universities, corporations, and partnerships • 12 founding members that met following the September 11th attacks to structure the national business force concept • 10 NJBF charter members joined shortly after the initial founding members meeting • 15 NJBF members (present and former) • 22 affiliates serve as BEOC Alliance participants
BEOC Alliance Establishment	The BEOC Alliance was created as a collaboration between partners, including academia (led by NJIT); business (represented by NJBF); and government organizations such as ARDEC at Picatinny Arsenal, New Jersey.
Governance	A Governance Committee of senior-level management from member organizations provides leadership to guide NJBF efforts, oversees BEOC Alliance policy, and interacts with public-sector partners. It meets semi-annually.
Funding	<p>As nonprofit organizations, both entities rely on membership dues, contributions, and grants. Nonprofit status gives both NJBF and the BEOC Alliance flexibility and independence.</p> <ul style="list-style-type: none"> • Levels of BEOC Alliance membership are based on an annual fee and range from \$2,500 to \$25,000+. Access, privileges, and benefits depend on the level.

Organization Background

Mission and Objectives

NJBF Mission	To improve and strengthen the capacity of New Jersey, FEMA Region 2, and business partners in preventing, preparing for, responding to, and recovering from disasters of magnitude through a dynamic partnership triad comprising academia, private-sector entities, and government.
NJBF Functional Areas	<ul style="list-style-type: none"> • Providing private-sector perspective in facilitation. • Fostering effective communications for shared situation awareness through adaptive technologies. • Leveraging best practices through cross-sector collaboration. • Testing effectiveness through exercises and experimentation.
BEOC Alliance Mission	Enhance collaboration and communication during response and recovery to catastrophic events.
BEOC Alliance Goals	<ul style="list-style-type: none"> • Private-sector advocacy • Business-to-business collaboration, communications, and information sharing • Interface with public-sector emergency operations centers • Business-to-nongovernmental organization collaboration • Research
BEOC Alliance Critical Infrastructure-Related Objectives	<ul style="list-style-type: none"> • Planning • Non-classified intelligence and information sharing • Physical protective measures • Supply chain integrity and security • Long-term vulnerability reduction • Infrastructure systems • Operational communications • Situational assessment • Economic recovery
Points of Contact	
NJBF	Henry Straub, Executive Director
BEOC	Dr. Mike Chumer, Alliance Advisory Board Director
Partnerships and Programs Leveraged	
Federal Programs	<ul style="list-style-type: none"> • U.S. Department of Defense: NJBF uses the ARDEC EOC technology test facility as the primary BEOC physical and virtual hub location. • FEMA Personnel: See “Partnerships.” • National Level Exercise: See “Training and Exercises.”

The Northeast Disaster Recovery Information X-Change (NEDRIX) was started 1991 as a nonprofit to coordinate government agencies during emergencies, but a decade later it expanded its focus to include public-private coordination. The organization has grown from a public-private partnerships between one State emergency management agency and a few critical infrastructure industry partners has grown to include the governments of eight States and thousands of critical infrastructure business professionals. Through initiatives like its NEDRIX Notify, NEDRIX is able to connect public and private partners by providing coordinated real-time incident assessment information.

Geographic Focus



Northeast United States, including the States of Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, and Vermont

Members

2,700
active participants

Members

- Public- sector professionals
- Private- sector professionals

Sector(s) of Focus

No specific critical infrastructure focus. NEDRIX focuses on business continuity and disaster recovery.

Establishment

1991

NEDRIX was founded in 1991 as a nonprofit organization to coordinate emergency management among government agencies in the Northeast United States. In 2001, NEDRIX changed its focus toward public-private coordination for business continuity and disaster recovery.

Funding

- Private donations
- Conference fees
- Government support
- Business sponsorship

Governance

- Board of Directors

Primary Activities

- Information sharing
- Public-private sector coordination

Keys Factors of Partnership Success

- Recognizing the role the private sector can play in critical infrastructure security and resilience, NEDRIX expanded its original focus from solely public-sector entities. NEDRIX is able to improve regional resilience by coordinating with public- and private-sector partners before, during, and after an event.
- NEDRIX provides real-time incident information through an automated alert notification tool, NEDRIX Notify. The tool provides an effective platform for government and private-sector stakeholders to share and receive information.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Plan Assistance: NEDRIX assists its members with the development and adaptation of preparedness and business continuity plans, based on the collective best practices and expertise of its membership.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • NEDRIX designs, hosts, and conducts symposia, conferences and simulation exercises for its members, with participation from public-sector agencies and partners. • Annual Conference Exercise: NEDRIX conducts at least one annual Simulation Exercise for its members at its annual conference held in Newport, Rhode Island. NEDRIX designs and conducts the interactive exercise with scenario events. Government resources are utilized for direction on the accuracy of the exercise, and government representatives are invited to participate as panel members at the exercise. • Academic Programs: NEDRIX partners with several colleges and universities located within the region to develop and maintain academic emergency preparedness programs available to students and the public. Current programs are offered from Boston University, Bryant University, Massachusetts Maritime Academy, and Norwich University. • Internship Opportunities: NEDRIX maintains an Internship Opportunities page on its Website that allows college graduates to post their resumes and companies to post their internship openings. The goal is to help emergency management or business continuity students obtain real experience with NEDRIX member companies.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Categories of Information Sharing: <ul style="list-style-type: none"> – Steady state: general, non-emergency information such as preparedness and resilience best practices and guidance – Situational awareness: the NEDRIX Website includes a visual situational awareness tool to highlight active incidents in the region – Event/threat-specific: through its NEDRIX Notify alert tool specific incident or threat-information such as weather alerts, cyber threats, or response status updates are distributed throughout the membership to keep members informed of current events and emerging threats

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Mechanisms Used: NEDRIX uses email alerts; text messages; in-person monthly meetings in some States as well as ad- hoc meeting requests as specific initiatives present themselves; conferences and other events; and announcements on the NEDRIX Website. • NEDRIX Notify: NEDRIX Notify is an automated alert notification tool that provides NEDRIX with the ability to coordinate communications and disseminate real-time incident assessment information to a broad group of regional stakeholders. <ul style="list-style-type: none"> – Government representatives can use NEDRIX Notify to disseminate information to critical infrastructure owners and operators and other regional stakeholders regarding critical situations, including severe weather, cyber threats, terrorist attacks, and evacuation updates. – Those that receive information from NEDRIX Notify can also submit information (anonymously if preferred) regarding individual business operations or cross-sector effects. – 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.
Emergency Response	<ul style="list-style-type: none"> • NEDRIX Notify: The automated alert notification tool is used by the partnership’s members as a primary conduit for real-time emergency response information. This information is critical to informing the decisions of public and private members of NEDRIX (See “Information Sharing”).
Partnerships	<ul style="list-style-type: none"> • Emergency Management Agencies: NEDRIX maintains strong relationships with State emergency management agencies in the Northeast United States., including: <ul style="list-style-type: none"> – Massachusetts Emergency Management Agency – Connecticut Division of Emergency Management and Homeland Security – Rhode Island Emergency Management Agency • Academia: NEDRIX also maintains strong relationships with several colleges and universities located within the region (See “Training and Exercises”).

Organization Background

Establishment, Governance, and Funding

Establishment	NEDRIX was founded in 1991 as a nonprofit organization to coordinate emergency management among government agencies in the Northeast United States. In 2001, NEDRIX changed its focus toward public-private coordination for business continuity and disaster recovery. What began with public-private partnerships between one State emergency management agency and a few critical infrastructure industry partners has grown to include the governments of eight States and thousands of partners.
Governance	The Board of Directors governs the organization.
Funding	NEDRIX is a 501(c)(3) nonprofit organization and relies on private donations, conference fees, and governmental support to fund its activities. Multiple levels of sponsorship are offered for businesses to annually pledge support.

Mission and Objectives

Mission	To provide continuity and crisis management professionals access to real-time governmental agency information during a crisis or event.
Critical Infrastructure-Related Goals and Objectives	<ul style="list-style-type: none"> • Instill the culture and importance of preparedness and response with members through public-private partnerships. • Supply members with reliable information for use during an emergency. • Provide members with effective resources to assist in their emergency preparedness planning for their company, their families, and their community. • Continue broadening awareness on emergency preparedness.
Committees	<p>Committees are composed of seasoned members with wide-ranging areas of expertise that volunteer their time to support members, industry, and partnerships. By volunteering, Committee Members expand their professional networks and gain valuable lessons in industry best practices, teamwork, and leadership. Committees relating to critical infrastructure security and resilience:</p> <ul style="list-style-type: none"> • Simulation Committee: This Committee engages with NEDRIX members and partners to develop disaster exercise scenarios. • Public-Private Partnership Committees: A regional Committee for each of the eight NEDRIX States is focused on developing and supporting public-private partnerships for emergency preparedness and response in their area.

Points of Contact

President	Christine Glebus, Glebus Continuity Consulting
Vice President	Lori C. Adamo, President, Code Red Business Continuity Services
Board of Directors	Includes representatives from the public health and information technology fields.

Partnerships and Programs Leveraged

Federal Programs	<ul style="list-style-type: none"> • U.S. Department of Homeland Security, Urban Areas Security Initiative
-------------------------	---

The Pacific NorthWest Economic Region (PNWER) established the Center for Regional Disaster Resilience (CRDR) following the September 11th attacks to help educate first responders on infrastructure interdependency issues. Today it serves as a nexus between the public and private sectors to build trust, share information, and improve the Pacific Northwest's ability to protect its critical infrastructure from all hazards.

Geographic Focus



States of Alaska, Washington, Idaho, Montana, and Oregon and the Canadian provinces and territories of Alberta, British Columbia, Saskatchewan, Yukon, and the Northwest Territories

Members

150

business members

Private Sector

- Major multinational corporations
- Regional business associations
- Canadian companies
- State- and local-level businesses

1,000

stakeholders

Public Sector

- Representatives from State, local, tribal, and territorial government departments and agencies
- Representatives from Federal Government Agencies
- National laboratories

Sector(s) of Focus

No specific sectors identified. The primary focus of the CRDR is on community resilience and identifying infrastructure interdependencies.

Establishment

2001

PNWER established the CRDR following the September 11th attacks to educate first responders on infrastructure interdependency issues.

Funding

- Sponsors

Governance

- Board of Directors

Primary Activities

- Planning
- Information sharing
- Training and exercises
- Disaster recovery

Keys Factors of Partnership Success

- Focusing on issues affecting an entire region allows a partnership to cross-jurisdictional lines to build resilience. PNWER launched its CRDR to specifically address interdependency issues. With its members including Washington, Oregon, Idaho, Montana, and Alaska in the United States and British Columbia, Alberta, Saskatchewan, and Yukon Territory in Canada, PNWER already understood how threats can cross jurisdictions. The established, trusted relationships aid in quick, effective response and building resilience.
- Relationships are indispensable to the success of major activities that require regional public- and private-sector support. Trust is the result of the CRDR's long history of partnership efforts. This is evident during major incidents and conveyed by the organization's resilience during turbulent economic times that may have ended other partnerships.

Snapshots of Recent Success

- CRDR's long history of partnership efforts has resulted in trusted relationships with members. This is evident during major incidents and conveyed by the organization's resilience during turbulent economic times that may have ended other partnerships.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Recovery Planning: The CRDR aims to step beyond traditional response planning into more recovery planning efforts. Instead of a focus on testing a plan during exercises, focus remains on developing and sustaining the relationships essential to disaster planning and recovery. • Regional Supply Chain Resilience Project: The CRDR is working with the Puget Sound Regional Catastrophic Planning Team and influential private-sector members on a series of stakeholder-identified strategies to strengthen the region's ability to withstand and rapidly recover from disasters. The goal of the project is to develop a supply chain resilience public-private sector working group that is able to provide input and advice on issues related to regional supply chain resilience. This includes examining the Regional Catastrophic Transportation Plan and its Maritime Annex. A recent kickoff meeting launched the initiative in September 2013. • Port Security: As a regional facilitator of public-private partnerships, the CRDR works closely with the eight Puget Sound ports to foster collaboration on contingency plans and fill planning gaps. • Pacific Northwest Emergency Management Arrangement: The CRDR participated in the development of this bi-national plan for recovering from a disaster in a cross-border area.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Earthquake Exercise: The CRDR planned to support an earthquake exercise in February 2014 focused on regional recovery from a seismic incident. More than 1,000 stakeholders have been invited to the exercise, including representatives from the Communications, Energy (Oil and Natural Gas), and Transportation Systems (Railroads and Maritime modes) Sectors.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> • Blue Cascades Exercise Series: The CRDR developed the Blue Cascades Exercise Series to explore regional infrastructure interdependencies in the Pacific Northwest. After each exercise, stakeholders contributed to an action plan to address the issues uncovered during the exercise. From 2002–2010, the CRDR has held six exercises on the following topics: <ul style="list-style-type: none"> – Energy grid disruptions (2002) – Physical disruptions/cyber disruptions (2004) – A major subduction zone earthquake (2005) – Pandemic preparedness (2007) – Supply chain resilience (2008) – Public health and safety effects of major flooding (2010) • Private-Sector-Led Exercises: The CRDR also participates in private-sector-led exercises, with trusted relationships as a primary benefit. For example, one port security exercise aided ports in working together and developing mutual aid agreements.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Social Media: One CRDR goal is to raise the capability of first responders to use social media. The CRDR received a grant from the FirstToSee Emergency Support System to develop a backend structure for Emergency Operations Center (EOCs) to sort social media feeds. This will enable these EOCs and first responders to add extra pairs of eyes—through social media—to create a clearer common operating picture and provide a more targeted response during a crisis. • Regional Alert and Warning System: The CRDR helped develop the Northwest Warning, Alert & Response Network (NWWARN) to maximize real-time sharing of situational information without delay and provide immediate distribution of analytical products/information to water sector professionals in the field. <ul style="list-style-type: none"> – Approximately 3,000 vetted professionals use NWWARN. – The CRDR has led this effort in cooperation with the U.S. Department of Homeland Security (DHS) (including the Office of Infrastructure Protection and Federal Emergency Management Agency) the Federal Bureau of Investigation (FBI), and the Washington State Fusion Center (WSFC). – The WSFC uses NWWARN as the primary means to virtually connect with vetted critical infrastructure and private-sector stakeholders. • Homeland Security Information Network (HSIN): CRDR was one of the original pilots for HSIN. The center is currently migrating to HSIN to fulfill a similar role as NWWARN. • Fusion Center: The CRDR successfully advocated for the WSFC to develop a critical infrastructure component. • Type of Information: The CRDR has found that the private sector is interested in information that helps it build a common operating picture through accurate, timely information shared in a bidirectional information-sharing relationship.

Critical Infrastructure Activities

<p>Emergency Response</p>	<ul style="list-style-type: none"> • Supply Chain Resilience Task Force: During an emergency, the CRDR may activate this task force to communicate directly with an EOC about what the critical elements and decisions are that would affect the region three to six months from the time of the incident. • Recovery: The CRDR sent representatives to survey the Gulf Coast Oil Spill in 2010. Their findings greatly influenced recovery plans in the Pacific Northwest.
<p>Partnerships</p>	<ul style="list-style-type: none"> • <i>Beyond the Border Working Group:</i> In 2011, the United States and Canada jointly announced a bi-national initiative for economic commerce and security called <i>Beyond the Border</i>. Under the initiative, the U.S. Coast Guard and Transport Canada partnered for maritime economic commerce, resilience, and security. They initiated the first phase of the program in late 2011 in the greater Seattle-Vancouver region, requesting PNWER CRDR to lead the effort. • Critical Infrastructure Protection (CIP) Task Force: The CRDR initiated the coordination of CIP managers in 2005 from the States and provinces as well as Federal partners to share information and best practices on a regular basis. In 2007, these CIP managers met in person at Microsoft in Redmond, Washington. Since that meeting, conference calls have continued on a quarterly basis and several informal meetings have occurred throughout the region. • Region 6 Critical Infrastructure Protection Work Group (CIP WG): The Region 6 (King County) CIP WG is made up of key county and city agencies and voluntary private-sector representation from some of the county’s largest employers and owners and operators. The Region 6 CIP WG and the DHS Protective Security Advisor (PSA) have worked with the CRDR to facilitate interdependency workshops, tabletop exercises, and other partnership-building activities. The Work Group’s WSFC member also serves on the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The Region 6 CIP WG also utilizes PNWER through a memorandum of understanding to provide project management for initiatives funded through the Homeland Security Grant Program (HSGP).

Organization Background

Establishment, Governance, and Funding

<p>Establishment</p>	<p>Following the September 11th attacks, PNWER established the CRDR to bring first responders up to speed on infrastructure interdependency issues.</p> <ul style="list-style-type: none"> • October 2001: Launched its first meeting of critical infrastructure owners and operators. The group advocated for a deeper examination of interdependencies. • Summer 2002: Hosted the first Blue Cascades exercise, focusing on energy grid disruptions. This exercise heavily involved public-private interaction that raised State and local emergency managers’ awareness of infrastructure interdependencies.
----------------------	---

Organization Background	
Governance	PNWER is a statutory, nonprofit public-private 501(c)(6) organization.
Funding	Sponsors have the opportunity to support the CRDR through either a Premier (\$2,500 annually) or Sustaining (\$1,000 annually) Sponsorship. Sponsors receive a varying range of benefits based on their contribution. Contributions are not tax deductible.
Mission and Objectives	
Mission	Providing a nexus between the public and private sectors to build trust and share information.
Goal	Improving the Pacific Northwest's ability to withstand, recover, and protect its critical infrastructure from all-hazards disasters.
Critical Infrastructure Security and Resilience-Related Objectives	<ul style="list-style-type: none"> • Creating and fostering cross-sector partnerships focused on infrastructure security and disaster resilience. • Developing and conducting regional infrastructure interdependency initiatives focused on various threat-scenarios that include regional cross-sector/cross-discipline workshops and exercises to better understand threats and vulnerabilities and develop strategies for action to address them. • Seeking funding and other resources to support regional pilot projects and other activities and to enable State and local agencies to address regional preparedness needs. • Overseeing the implementation of priority projects and activities in a cost-effective, timely, and ethical manner. • Conducting outreach and developing and facilitating seminars, workshops, and targeted exercises to raise awareness and test the level of preparedness.
Working Groups	<p>CRDR works with public- and private-sector stakeholders to create and implement workable solutions to regional and local infrastructure vulnerabilities and other needs. Specific working groups for these issues include:</p> <ul style="list-style-type: none"> • Banking and Financial Sector • Cybersecurity • Interdependencies • Maritime Resilience • Public Health • Social Media and Information Sharing • Supply Chain Resilience
Points of Contact	
Personnel	<p>Matt Morrison, PNWER CEO Eric Holdeman, PNWER CRDR Director</p>

Organization Background

Partnerships and Programs Leveraged

Federal Programs

- ***Beyond the Border Initiative:*** Under the bi-national initiative, the U.S. Coast Guard and Transport Canada partnered to improve maritime economic commerce, resilience, and security. See “Partnerships” for more information.
- **DHS IP PSA:** Through the Region 6 Critical Infrastructure Protection Working Group, CRDR worked with PSA facilitate exercises, workshops, and other activities.
- **HSGP:** PNWER provides project management through a memorandum of understanding on HSGP-funded initiatives.

The ReadySanDiego Business Alliance is a volunteer organization coordinated by the County of San Diego Office of Emergency Services (OES) to improve business preparedness in the region. The organization was established following a summit between higher education, private-sector, and government entities. ReadySanDiego's coordinated response when wildfires engulfed the county showcased the benefits of the partnership, specifically its resource identification.

Geographic Focus	Members
 <p>San Diego metropolitan area</p>	<p>300+ members</p> <p>Private Sector</p> <ul style="list-style-type: none"> Major corporations State- and local- level businesses Volunteer organizations <p>Public Sector</p> <ul style="list-style-type: none"> State departments and agencies Municipalities Representatives from Federal Government agencies

Sector(s) of Focus			
 <p>Commercial Facilities</p>	 <p>Communications</p>	 <p>Emergency Services</p>	 <p>Healthcare & Public Health</p>

Establishment	
<p>2007</p>	<p>ReadySanDiego was established following a September 2007 preparedness and business continuity summit that brought together higher education, private-sector, and government entities.</p>

Funding	Governance	Primary Activities
<ul style="list-style-type: none"> County government funding In-kind donations 	<ul style="list-style-type: none"> Advisory Council San Diego County Government 	<ul style="list-style-type: none"> Information sharing Emergency response Planning and preparedness

Keys Factors of Partnership Success

- Partners dictate the organization’s activities and initiatives to address needs they see in the region. Rather than a top-down approach, with the county determining what initiatives to pursue, the ReadySanDiego Business Alliance takes a bottom-up approach allowing partners to determine what they need from the county to improve preparedness.
- Private-sector members are able to leverage county San Diego Emergency Operations Center to receive timely information during an event. Not all private-sector member companies have the staff to spare for deployment to the EOC. Leveraging OES employees as representatives limits the possibility of any one company having a competitive advantage in emergency situations.

Snapshots of Recent Success

- The Business Alliance’s information-sharing tool, San Diego Partnership Connection, has become a widespread success and is an integral part of critical infrastructure security and resilience activities in the San Diego region. See “Information Sharing” for more information.
- After the Fukushima Daiichi nuclear disaster in 2011 and the subsequent instances of radioactive material escaping from the site, the Business Alliance shared up-to-date, accurate information with its members to calm fears and quell misinformation about threats of radioactive contamination (of the ocean, air, and goods from Japan).
- In 2009, OES began an unprecedented wildfire awareness campaign for businesses and residents of the San Diego region. The Business Alliance garnered about \$500,000 in donations and in-kind support to effectively distribute campaign messages. Distribution methods included radio and television advertising, cellular messaging, and announcements during San Diego Padres Major League Baseball games.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Business Mentoring Program: A mentoring program for continuity planning is currently in development. Member organizations proficient in continuity planning are encouraged to develop training for other members. • Workshops: The Business Alliance conducts planning and strategy workshops, which are hosted and/or directed by members based on topical expertise (e.g., communications companies with advanced plans/strategies conduct workshops for other communications companies). • Continuity and Employee Preparedness Plans: The Business Alliance provides assistance to members for the development of business continuity and employee preparedness plans.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Active Shooter Training: The San Diego Law Enforcement Coordination Center recently conducted an active shooter training and exercise event for Business Alliance members.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • San Diego Partnership Connection: The online tool was developed by the Business Alliance and serves as its information-sharing hub. The tool coordinates the flow of steady-state and emergency information between members, as well as

between various information-sharing systems. Key features of the site include the following:

- Structured similarly to a social networking site for ease of use.
- Password-protected, with access limited only to members.
- Subgroups based on common interests or issues (e.g., faith-based groups, native tribes, and industry sectors) are available for members to join.
- Customizable automated notifications to members include the following: RSS feeds, mass emails (for emergency and non-crisis events), AlertSanDiego messages, and EOC/WebEOC notifications.
- **AlertSanDiego:** AlertSanDiego is the region’s emergency telecommunications alert system for businesses and individuals. Users can register their landline and cellular numbers and email addresses with the system to be notified about emergency situations or pending disasters in the region.
- **San Diego EOC:** The San Diego EOC is a central facility operated by OES for regional emergency response coordination. OES has designated staff positions to act on behalf of Business Alliance members to increase the Business Alliance’s overall situational awareness.
 - Not all private-sector member companies have the staff to spare for deployment to the EOC. Leveraging OES employees as representatives limits the possibility of any one company having a competitive advantage in emergency situations.
 - OES EOC personnel are trained in the use of the Partnership Connection and WebEOC. They report on topics such as utility status, fuel supply status, and collaboration with the OnStar driver notification system (for data and information shared by those with the system installed).
 - **WebEOC:** WebEOC is an online crisis information management system that provides secure, real-time information sharing. When WebEOC is activated, Business Alliance members are notified and prompted to log in to receive and share information on unfolding events.
 - **Social Media:** Business Alliance members leverage social media outlets (e.g., Facebook, Twitter, and YouTube) to increase education and awareness of security and resilience activities, initiatives, and programs.
- **Quarterly Meetings:** The Business Alliance hosts quarterly large-scale meetings and workshops to bring together more than 100 business members representing 89 industries to discuss current developments in critical infrastructure security, continuity, and preparedness in the region.
 - Meeting locations are regional in order to tailor topics to specific needs.
 - Meeting duration is brief (sometimes 1.5 hours) in order to encourage participation.
 - Although vendors are invited to participate, solicitation is prohibited; this encourages collaborative partnerships.
 - Topics: cybersecurity presentation by InfraGard, active shooter training, and training on the Partnership Connection communications tool.

Critical Infrastructure Activities

Emergency Response	<ul style="list-style-type: none"> • Role: The Business Alliance participates in response and recovery activities, with the county’s economic recovery being a priority, such as: <ul style="list-style-type: none"> – Coordination and donation of needed resources: Platforms or mechanisms used for incidents include AlertSanDiego, the San Diego Partnership Connection, and WebEOC. – Education on available assistance: ReadySanDiego will provide information on evacuation procedures and shelters and aid businesses in applying for Small Business Administration disaster loans. • EOC: As described in “Information Sharing,” a Business Alliance representative sits at the EOC when activated. Relevant security and resilience information from the EOC (e.g., status of area food/financial/energy supplies or member operations) is also shared by OES staff in the EOC.
Partnerships	<ul style="list-style-type: none"> • Collaboration: The Business Alliance collaborates with other leading critical infrastructure security and resilience partnerships in California (e.g., Business Executives for National Security [BENS] California, California Resiliency Alliance [CRA], and the Association of Continuity Planners) to network, coordinate events, share best practices, and increase education and awareness of security and resilience partnership efforts. • Voluntary Organizations Active in Disasters: National and State-level organizations such as the American Red Cross and religious institutions serve as force-multipliers for the Business Alliance by directly connecting available assistance with those in need. • Benefits: Positive working relationships built between the county and its business partners help to break down competitive barriers, ensure that the partnership remains relevant, and enable the county to offer assistance directly targeted to partner needs.
Cybersecurity	<ul style="list-style-type: none"> • Information Sharing: Other partnerships fulfill cybersecurity information sharing in the region. Cyber-related threat-information is provided to the Business Alliance by InfraGard. • Federal Training: Members recently participated in an InfraGard training session on cybersecurity.

Organization Background

Establishment, Governance, and Funding

Establishment	<p>ReadySanDiego Business Alliance was established following a September 2007 preparedness and business continuity summit that brought together higher education, private-sector, and government entities.</p> <ul style="list-style-type: none"> • Wildfires engulfed the county in October 2007 while ReadySanDiego leadership was attempting to build momentum for the Business Alliance. ReadySanDiego’s
---------------	---

Organization Background

	<p>coordinated response regarding resource identification proved the benefits of such a partnership.</p> <ul style="list-style-type: none"> • In 2008, a public relations firm was hired to provide general program support to the Business Alliance, especially in terms of increasing regional education and awareness of the partnership. • Today, rather than a top-down approach, whereby the county determines what would be of interest to owners and operators, the organization focuses on a bottom-up approach in which the partners determine what they need from the county.
<p>Governance</p>	<p>The ReadySanDiego Business Alliance Advisory Council oversees the organization’s efforts. It’s responsibilities include:</p> <ul style="list-style-type: none"> • The Council is composed of business leaders from throughout the San Diego region that act as corporate spokespersons, leveraging business relationships to help promote program initiatives in the region. • The Council works in conjunction with OES staff to identify strategic goals of the Business Alliance partnership program and help oversee its path forward. • During times of crisis, the Council works with OES to lead the Business Alliance’s response and recovery activities, including the coordination of needed resources from its members. • The Advisory Council and OES staff collaborate to define the Business Alliance’s goals and objectives. The Business Alliance membership has until recently been organized by eight of its own broadly defined sectors, representing 13 of the 16 critical infrastructure sectors defined by NIPP 2013. • A reorganization is under development to delineate regional chapters of the Business Alliance based on subregions within the county. ReadyCarlsbad is a current regional chapter, representing the northern portion of San Diego County.
<p>Funding</p>	<p>Sustainment of the Business Alliance partnership is primarily funded by the County of San Diego government, with some support from private-sector members.</p> <ul style="list-style-type: none"> • In-kind donations are provided by members to host meetings, workshops, and summits. • There is no cost associated with membership, which is maintained at the discretion of each member organization. • The Business Alliance has examined the cost structure of other security and resilience partnerships and does not envision a favorable return on investment for collecting fees or dues from its members. This is due in part to most of the services being provided free of charge to members by the county government.
<p>Members</p>	<ul style="list-style-type: none"> • Private- sector members include major corporations (e.g., Cox Communications, Lowe’s, Target, and Wells Fargo), regional businesses and associations (e.g., BENS, CRA, and San Diego County Hotel-Motel Association), and State- and local-level businesses (e.g., banking, communications, food and agriculture, and healthcare companies). Private sector members constitute roughly 90 percent of

Organization Background

	<p>membership.</p> <ul style="list-style-type: none"> • State and local government members include major departments and agencies (e.g., OES, the County of San Diego Health and Human Services Agency, and the Governor’s Office of Emergency Services) as well as local municipalities (e.g., the cities of Carlsbad, Imperial Beach, and San Diego). • Federal Government members include the U.S. Department of Homeland Security (including the Office of Infrastructure Protection and Federal Emergency Management Agency [FEMA]), U.S. Department of State, and Federal Bureau of Investigation (FBI). • Volunteer organization members include the American Red Cross and local-level volunteer organizations.
Mission and Objectives	
Mission	To create a coalition of businesses which contribute resources and senior expertise before, during, and after a time of crisis in the San Diego region.
Critical Infrastructure Security and Resilience Objectives	<ul style="list-style-type: none"> • Raise awareness of the need to prepare businesses and their employees for emergencies. • Promote private-public partnerships to extend the Business Alliance message into the community. • Develop tools to reach all segments of the community.
Points of Contact	
Personnel	Holly Crawford, Director, County of San Diego OES Leslie Luke, Group Program Manager, County of San Diego OES
Partnerships and Programs Leveraged	
Federal Programs Leveraged	<ul style="list-style-type: none"> • FEMA Private Sector Office: This office helped open doors for discussions with large entities, such as Major League Baseball, at which the Business Alliance did not have contacts. • FEMA Ready.gov/business: The Business Alliance encourages its members to leverage the resources available from the Ready.gov/business Website to enhance business preparedness. • InfraGard: See “Information Sharing.”

Safeguard Iowa Partnership (SIP) is focused on strengthening the State of Iowa's ability to prevent, prepare for, respond to, and recover from disasters through public-private collaboration. As a nonprofit, SIP serves as a neutral third-party, enabling buy-in from both sides. SIP also helps to bring business to the table, explain what information the government is looking for, and why they need it. By serving as an intermediary, SIP allows business and government to build relationships outside of standard regulatory interactions. During an emergency, SIP plays a critical role in the response through its Emergency Operation Center (EOC) Liaison program that puts private-sector representatives in a position where they can provide expertise and pass along necessary information to other private-sector partners.

Geographic Focus		Members
 <p>State of Iowa</p>		<p>Membership</p> <p>437 → public, private, nonprofit, and association members</p> <ul style="list-style-type: none"> Membership has shifted to more private-sector partners, which reflects the larger number of private-sector companies compared to government agencies in the State.
Sector(s) of Focus		
  <p>Emergency Services Financial Services</p>		
Establishment		
<p>2007</p> <p>SIP was started by the Iowa Business Council and key State agencies, including the Iowa Department of Public Health, Iowa Department of Public Safety, and Iowa Homeland Security and Emergency Management. It became a 501(c)(3) nonprofit in 2008.</p>		
Funding	Governance	Primary Activities
<ul style="list-style-type: none"> Grants State funding for specific activities Private-sector sponsors 	<ul style="list-style-type: none"> 12-member Board of Directors 	<ul style="list-style-type: none"> Preparation Emergency response Recovery (planned action)

Keys Factors of Partnership Success

- As a nonprofit, SIP has flexibility in pursuing funding sources and it is able to act as an intermediary between the private and public sector. SIP is able to connect the private and public sectors and facilitate discussions regarding critical infrastructure disaster preparedness. These conversations build relationships prior to a disaster and help all parties understand roles and responsibilities.
- The private sector has an active role in emergency response. Through its EOC Liaison program, SIP private-sector volunteers are available for deployment to State and county EOCs, where they can provide resources and information to emergency managers during a disaster. The Business Resource Registry, a catalogue of private-sector assets available for possible use during an emergency, which also provides value information and resources during a crisis.

Snapshots of Recent Success

- Since 2008 SIP's EOC Liaison Program has embedded private-sector volunteers in State and county EOCs during an emergency. The liaisons relay important information to the private sector and provide knowledge and expertise about privately owned and operated critical infrastructure to EOC staff. Liaisons are also able to identify and secure resources from the private sector to help with emergency response that the State is unable to secure through normal channels.
- For National Preparedness Month in September, SIP partnered with Iowa Homeland Security and Emergency Management and the Iowa Emergency Management Association (IEMA) to develop a public service campaign to encourage businesses, employers, and residents to prepare for disasters.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Plan Development: Through a Critical Infrastructure and Key Resources (CIKR) Planning Committee, SIP coordinates the development and implementation of multiyear improvement plans. • Business Continuity Planning Resources: SIP provides business continuity planning resources for small- and medium-sized companies, including a mentorship program that connects businesses to provide each other assistance in developing plans. Topics discussed include the importance of business continuity and best practices, such as how to address regulatory issues by sharing their own experience. • Outreach and Awareness: SIP created an annual event, the Prepare Fair, to improve awareness among residents about the importance of preparedness. On its Website, SIP offers a “20 Weeks to Preparedness” calendar to help individuals create an emergency supply kit and prepare for emergencies. • Flu Vaccine Toolkit: SIP partnered with the Iowa Department of Public Health to increase influenza vaccination rates in the State. A SIP survey of businesses was able to identify barriers and best practices for employers. Using this information, a flu vaccine toolkit was developed for businesses.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Training: SIP regularly hosts CIKR training across the State. <ul style="list-style-type: none"> – The training is followed by a tabletop exercise to help identify key resources and improve capabilities in the event of a disaster.

Critical Infrastructure Activities

	<ul style="list-style-type: none"> – Convening public and private partners from across the State has built relationships and developed creative solutions to gaps identified through the exercises. • Texas A&M Engineering Extension Service (TEEX): TEEX provides training on topics such as, critical infrastructure, threat-assessments, and cybersecurity, at no cost to the States. • Multistate Exercise: In September 2010, SIP worked with the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection and Minnesota InfraGard to create and implement the “Northern Lights” exercise. The exercise spanned Iowa, Minnesota, Nebraska, North Dakota, and South Dakota to test targeted regionally critical assets. • Webinars: SIP frequently hosts Webinars on topics such as the Homeland Security Information Network (HSIN), navigating State government, regional and Federal emergency management practices and policies, cybersecurity, and the aid available during disasters. <ul style="list-style-type: none"> – Webinars are recorded and are available as a resource on the SIP Website. – Exercise tools, including presentations, facilitator notes, templates, and after-action reports are also posted on the Website.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Facilitate Discussions: As a neutral third party, SIP is able to connect the private and public sectors and facilitate discussions regarding critical infrastructure and disaster preparedness. These conversations help all parties understand roles and responsibilities and build relationships prior to a disaster. • Online Survey: SIP worked with the IEMA to develop an online survey to provide an easy way for businesses to communicate damage information following a disaster. • Website: The majority of SIP’s information sharing is accomplished through its Website, which allows partners to update their profile and contact information, share information, donate to the organization, and access content from other providers, such as the Federal Emergency Management Agency’s daily situation briefing. • Emails: SIP utilizes weekly emails to push out relevant information to partners, including links to content uploaded to the Website that week. In preparation for or during an event, information is disseminated more frequently. SIP shares with and receives virtual information from the State’s fusion centers.
<p>Emergency Response</p>	<ul style="list-style-type: none"> • EOC Liaison program: SIP private-sector volunteers are available for deployment to State and county EOCs, where they can provide resources and information to emergency managers during a disaster. <ul style="list-style-type: none"> – Liaisons provide the EOC staff with information on key operational time lines, facility locations, relocation logistics, and security needs. They can also identify private-sector resources available, including those not available through the regular emergency procurement process. – For the private sector, EOC liaisons assess the effect of a disaster on their

Critical Infrastructure Activities

	<p>businesses and track their needs. Liaisons also disseminate relevant information and guidance from the EOC to authorized private-sector contacts.</p> <ul style="list-style-type: none"> • Business Resource Registry: SIP operates the catalogue of private-sector assets available for possible use during an emergency. • Recovery Toolkit: SIP is in the process of developing a recovery toolkit for businesses to use following a disaster.
Partnerships	<ul style="list-style-type: none"> • Federal: SIP partners with InfraGard and similar organizations to coordinate efforts and avoid duplicating services, given membership overlap.
Cybersecurity	<ul style="list-style-type: none"> • Training and Tabletop: SIP is planning a cybersecurity training and tabletop exercise focused focus on what a cyber attack would mean for the community, government roles and responsibilities. It would also address ways to protect businesses from a cyber attack.

Organization Background

Establishment, Governance, and Funding

Establishment	<p>SIP was started in 2007 by the Iowa Business Council and key State agencies, including the Iowa Department of Public Health, Iowa Department of Public Safety, and Iowa Homeland Security and Emergency Management. It became a 501(c)(3) nonprofit in 2008.</p> <ul style="list-style-type: none"> • As a nonprofit, SIP serves as a neutral third-party, enabling buy-in from both sides. • SIP also helps bring business to the table, explains information the government is looking for, and why they need it. By serving as the intermediary, SIP allows businesses and government to build relationships outside of standard regulatory interactions.
Governance	<p>SIP is led by a full-time executive director responsible for coordinating administrative and operational functions. The executive director also works closely with the Board of Directors and full-time program coordinator to implement initiatives.</p>
Funding	<p>Its status as a nonprofit enables SIP to accept public- and private- sector funding.</p> <ul style="list-style-type: none"> • About 50 percent of its funding is provided by public sources, such as the Homeland Security Grant Program (HSGP) and funding from State agencies for specific activities, including immunization awareness efforts. • The rest of SIP's funding is derived from private-sector sponsors. • The mix of public and private funding offers SIP flexibility and allows it to sustain operations without relying solely on public funding, which is often unpredictable and with restrictions.

Organization Background

Mission and Objectives

Mission	Strengthen the capacity of the State to prevent, prepare for, respond to, and recover from disasters through public-private collaboration.
Vision	The leader in empowering business and government to collaborate around disaster efforts.
Strategic Goals 2014-2016	<ul style="list-style-type: none"> • Growth: Increase SIP's statewide membership annually, while sustaining and engaging current partners and relationships. • Services: Ensure core services are defined, marketed, and implemented. • Funding: Ensure sufficient and sustainable funding to fulfill the vision of SIP through maintaining dedicated staff to support daily business operations and core services.
Objectives 2014-2016	<ul style="list-style-type: none"> • Growth: Use a marketing strategy to showcase SIP's image to recruit potential partners and increase membership statewide and measure SIP's ability to meet partner satisfaction. • Services: Identify key deliverables for each core service area and ensure adequate staffing. • Funding: Secure private funding from existing partners for 2015 equal to or greater than 115 percent of 2013 levels, locked in by the end of 2014; secure five new contributors from the top 20 businesses currently not partners; apply for government funding as appropriate.
Working Groups	SIP uses three initiative teams (Preparedness, Response and Recovery) to develop, implement, and maintain its operational plans.
Chapters	The Board of Directors can authorize and charter SIP chapters based on geographical area of the State. The chapters help to identify gaps for strategic planning, distribute information, improve networking, and execute the SIP strategic plan. There are currently two chapters: Cedar Rapids-Iowa City Corridor and the Central Iowa Chapter.

Points of Contact

Personnel	Jami Haberl, Executive Director Jesse Truax, Program Coordinator
Board of Directors	The 12-member board includes representatives from financial corporations and county and State emergency management and public health agencies.

Partnerships and Programs Leveraged

State	SIP regularly works with South Dakota and Nebraska. Omaha, Nebraska is located directly across the Missouri River, representing a mutual interdependency for Iowa and Nebraska.
--------------	---

Organization Background

Federal Government	<ul style="list-style-type: none">• National Weather Service• U.S. Department of Homeland Security (including IP and the Federal Emergency Management Agency)• U.S. Department of Housing and Urban Development• U.S Small Business Administration
Federal Programs	<ul style="list-style-type: none">• HSGP: SIP uses funding through the HSGP to administer its initiatives, including the Business Resources Registry, EOC Liaison program, critical infrastructure and key resources exercises, business recovery, and business continuity planning.• Federal Programs: SIP works closely with the State’s critical infrastructure protection program and has included information on its Website about various Federal critical information programs available through the State, such as the Automated Critical Asset Management System, Protected Critical Infrastructure Information Program, the Buffer Zone Protection Program, the Integrated Common Analytical Viewer, and HSIN.

SouthEast Emergency Response Network

www.seern.org;
www.linkedin.com/company/southeast-emergency-response-network-seern

The SouthEast Emergency Response Network (SEERN) was started in 2004 as one of four pilot U.S. Department of Homeland Security (DHS) regional Homeland Security Information Network (HSIN) emergency response networks. The organization primarily conducts information sharing, exercises, and develops best practices to meet its goals to improve critical infrastructure security and resilience.

Geographic Focus



Southeast United States, including Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Missouri, Mississippi, North Carolina, South Carolina, and Tennessee

Members

No member information provided

Sector(s) of Focus

No sector information provided

Establishment

2007

SEERN was established in 2004 as one of four pilot DHS regional HSIN emergency response networks.

Funding

- Member dues
- Donations

Governance

- Executive Board

Primary Activities

- Information sharing
- Educational
- Operational (e.g., working within the National Incident Management System)

Keys Factors of Partnership Success

- SEERN provides stakeholders with timely, actionable information using a variety of mechanisms, such as regional and incident- or threat-specific reports, emergency response coordination, critical infrastructure security and resilience best practices, and public- and private- sector preparedness, risk management, and emergency response plans and strategies.
- SEERN uses a secure Web-portal for information exchange so members can share libraries of documents and case studies, situational awareness tools, send secure email, and participate in ongoing threaded discussions, create and distribute surveys, and share online briefings.

Snapshots of Recent Success

- SEERN actively participated in National Level Exercise 2011 (NLE11), which simulated the response and recovery to a catastrophic earthquake in the New Madrid Seismic Zone. The exercise focused on evaluating catastrophic event preparedness by assessing the ability of the Nation’s incident management systems to respond to a catastrophic earthquake, implement lifesaving and life-sustaining mission essential functions, and identify capability and resource gaps and solutions.

Critical Infrastructure Activities

<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Role: SEERN hosts and participates in joint training and exercises with public and private-sector partners. • NLE11: SEERN actively participated in NLE11, which simulated the response and recovery to a catastrophic earthquake in the New Madrid Seismic Zone. The exercise focused on evaluating catastrophic event preparedness by assessing the ability of the Nation’s incident management systems to respond to a catastrophic earthquake, implement lifesaving and life-sustaining mission essential functions, and identify capability and resource gaps and solutions.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Mechanisms and Information Types: Using email alerts, text messages, in-person meetings, conferences and other events, video conferences, media outreach, real-time alerts, and a secure Web-portal, SEERN shares the following information: <ul style="list-style-type: none"> – Regional and incident- or threat-specific critical infrastructure security and resilience situational awareness – Emergency response coordination – Critical infrastructure security and resilience best practices – State, local, tribal, and territorial (SLTT) and private sector preparedness, risk management, and emergency response plans and strategies • CyberCop: SEERN’s private portal is housed inside the CyberCop Web-portal. CyberCop is a proprietary secure information exchange network designed for efficient and effective information sharing among law enforcement, first responders, homeland security, and related business professionals. The portal allows its members to share libraries of documents and case studies, examine situational awareness tools, send secure email, participate in ongoing threaded discussions, create and distribute surveys, and share online briefings.

Critical Infrastructure Activities

Emergency Response	<ul style="list-style-type: none"> • Independent Third Party: Functioning as an independent third party, linking public and private stakeholders and resources for emergencies is a major focus of SEERN. The partnership’s many available interfaces with government and business networks allows for increased efficiency in emergency response—effectively cutting through red tape. • Emergency Operations Center (EOC) Integration: A position for a SEERN representative is designated in the region’s State EOCs. • Fusion Center Coordination: SEERN frequently coordinates with the region’s fusion centers on threat- and situational-awareness information sharing.
Partnerships	<ul style="list-style-type: none"> • State Government Strategic Partners: SEERN’s Executive Board has direct State government representation from Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Missouri, Mississippi, North Carolina, South Carolina, and Tennessee. • Federal Government Strategic Partners: As with the region’s Fusion Centers, SEERN also coordinates information sharing with DHS divisions and agencies, including Protective Security Coordination Division Regional Directors and Protective Security Advisors and the FEMA Region IV Office of the Regional Administrator.

Organization Background

Establishment, Governance, and Funding

Establishment	SEERN was established in 2004 as one of four DHS regional HSIN emergency response networks. In 2007, SEERN was re-established as a 501(c)(3) nonprofit organization focused on critical infrastructure information sharing.
Governance	The Executive Board governs the organization.
Funding	SEERN is a 501(c)3 nonprofit organization and relies on donations and membership dues to fund its activities.

Mission and Objectives

Mission	To foster a true public, private, and academic partnership—connecting to one common operating picture—communicating in real time.
Goals	<ul style="list-style-type: none"> • Become the one common conduit for critical infrastructure security and resilience information sharing in the Southeast United States. • Drive actionable, real-time, street-level information sharing between the public and private sectors. • Coordinate regional opportunities for all elements of SLTT governments to interface directly with the private sector.

Organization Background

- Share and drive critical infrastructure security and resilience best practices across the region.
- Act as a broker and translator between SLTT governments, Federal Government, and the private sector to achieve vital preparedness goals and become a more resilient region and Nation.

Points of Contact

President	Ian Hay
------------------	---------

The U.S. Chamber of Commerce is the world's largest business organization representing the interests of more than 3 million U.S. businesses of all sizes, sectors, and regions. These interests include critical infrastructure security and resilience. In recent years, the Chamber has been particularly active in cybersecurity develops establishing a Cybersecurity Working Group and working to improve its partners' education and awareness of cybersecurity issues and threats.

Geographic Focus		Members
 <p>National organization headquartered in Washington, D.C.</p>		<p>3 million → members</p> <p>Private Sector</p> <ul style="list-style-type: none"> • Small shops • Local chambers • Leading industry associations • Large corporations
Sector(s) of Focus		
No specific sectors identified		
Establishment		
<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; border-radius: 15px; padding: 10px; margin-right: 20px;"> <p style="font-size: 24px; margin: 0;">1912</p> </div> <p>A group of 700 delegates from various commercial and trade organizations came together to create a unified body of business interest that today is the U.S. Chamber of Commerce in response to President Taft's call for a "central organization in touch with associations and chambers of commerce throughout the country."</p> </div>		
Funding	Governance	Primary Activities
<ul style="list-style-type: none"> • Member dues 	<ul style="list-style-type: none"> • Board of Directors 	<ul style="list-style-type: none"> • Information sharing

Keys Factors of Partnership Success

- As a national organization with more than 3 million members, the U.S. Chamber of Commerce has clout and reach that smaller partnerships do not. Because of this, it can bring attention and resources to issues it deems crucial for critical infrastructure security and resilience, such as cybersecurity. Best practices can also be easily disseminated from one region to another through the organization.

Snapshots of Recent Success

- The U.S. Chamber held Cybersecurity Summits in 2012 and 2013, and will host another in the fall of 2014. The Summits bring together top experts and leaders from government and business to discuss the importance of public-private coordination in addressing cybersecurity issues, what actions the business community is taking to protect its systems from cyber threats, and international issues.
- The U. S. Chamber partnered with Sam’s Club in 2012 to hold Small Business Preparedness Expos at Sam’s Clubs in hurricane and disaster-prone areas of the Southeast. The expos aimed to bridge a major gap in a community’s resilience and recovery efforts in times of disasters.
- Regional U.S. Chamber Offices in Indiana and Texas promoted Domestic Preparedness Resiliency Workshops in their regions in 2012. The workshops brought together local chambers of commerce, associations, and small businesses to help create regional resilience reports to be published and shared with Washington, D.C. officials.
- The U.S. Chamber will be hosting a Global Supply Chain Summit in May 2014, which will examine the global web of interconnected, predictable, and efficient supply chains and how they contribute to the competitiveness of global business. The Summit will highlight supply chain efficiency and resilience issues of importance to businesses and develop solutions for global policy makers.
- The U.S. Chamber partners with the Office of the Director of National Intelligence (ODNI) and other elements of the U.S. Intelligence Community to create public-private information-sharing avenues with high-level officials and subject-matter experts to better protect the Nation from threats to national security.

Critical Infrastructure Activities

<p>Planning and Preparedness</p>	<ul style="list-style-type: none"> • Business Mentoring: The U.S. Chamber facilitates business-to-business mentoring activities (e.g., conference calls, workshops, forums, summits) to assist its members with developing emergency response and business continuity plans. Recent examples include the Sam’s Club Small Business Preparedness Expos, the Domestic Preparedness Resiliency Workshops, and the Global Supply Chain Summit, all highlighted as recent success stories.
<p>Training and Exercises</p>	<ul style="list-style-type: none"> • The U.S. Chamber participates in the National Level Exercise.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Real-Time Information Sharing: U.S. Chamber members receive real-time information on issues that affect their businesses and strategies to influence the legislative process. Members and supporters have access to policy information, news, marketing tools, networking opportunities, and events. Information is distributed to members by email, open letter, social media, and Website.

Critical Infrastructure Activities

Partnerships	<ul style="list-style-type: none"> • Federal: The U.S. Chamber collaborates with key White House administration decision makers, congressional lawmakers, and other Federal Government leaders to advance its national security and emergency preparedness mission, including: <ul style="list-style-type: none"> – National Institutes of Standards and Technology (NIST) – ODNI – Small Business Administration – U.S. Congress – U.S. Departments of Commerce, Defense, Health and Human Services, Homeland Security (DHS), and Transportation
Cybersecurity	<ul style="list-style-type: none"> • Cybersecurity Working Group: Since 2008, the Cybersecurity Working Group has advocated for legislation and policies that would build balanced and sustained relationships between business and government—unencumbered by legal and regulatory penalties—so that individuals could experiment freely and quickly counter extraordinarily fast-paced cyber threats to the U.S. business community. • Education and Awareness: The U.S. Chamber has partnered with the DHS Office of Cybersecurity and Communications (CS&C) since 2008 to increase businesses’ awareness of, and investments in, cybersecurity from an enterprise risk-management perspective. <ul style="list-style-type: none"> – Through its national network of partners, the Chamber has coordinated outreach to business owners and operators as well as incorporated participation from regional, State, and local government security officials. – The U.S. Chamber stresses the potential consequences of a cyber attack on businesses, and it calls upon business leaders to better integrate cybersecurity into their organizations’ enterprise risk management, emergency or disaster management, business continuity, and cost-benefit decisionmaking programs. – Regional cybersecurity roundtables give U.S. Chamber members a valuable opportunity to showcase their viewpoints and offer suggested practices for protecting cyberspace. – Recent outreach and education initiatives include: U.S. Chamber releases its <i>Internet Security Essentials for Business</i> guidebook (October 2010); U.S. Chamber and four association partners release <i>Improving Our Nation’s Cybersecurity through the Public-Private Partnership</i> to educate policy makers in the White House administration and Congress (March 2010); U.S. Chamber and the White House launch the National Strategy for Trusted Identities in Cyberspace (April 2011). • NIST Cybersecurity Framework: Following the release of the NIST Cybersecurity Framework in early 2014, the U.S. Chamber plans to explore partnership opportunities with NIST and DHS CS&C to educate small- and medium-size businesses on the benefits of adopting the framework into businesses risk- management processes.

Organization Background

Establishment, Governance, and Funding

Establishment	On April 22, 1912, in response to President Taft's call for a "central organization in touch with associations and chambers of commerce throughout the country and able to keep purely American interests in a closer touch with different phases of commercial affairs," a group of 700 delegates from various commercial and trade organizations came together to create a unified body of business interest that today is the U.S. Chamber of Commerce.
Governance	The Board of Directors is the principal governing and policymaking body of the U.S. Chamber of Commerce. The Board's membership is diverse, with more than 100 corporate and small business leaders serving from all sectors and sizes of business, and from all regions of the country. Directors determine the U.S. Chamber's policy positions on business issues and advise the U.S. Chamber on appropriate strategies to pursue.
Funding	The U.S. Chamber is a 501(c)(6) professional association. Membership dues are its primary source of funding.

Mission and Objectives

Mission	To develop and implement policy on major issues affecting businesses in the United States.
Critical Infrastructure-Related Goals and Objectives	<ul style="list-style-type: none"> • Critical Infrastructure Protection and Resilience: Analyze, develop, and advocate for risk-based policies to protect the country's critical infrastructure; advocate for greater resilience within the business community and especially among the sectors critical to the healthy functioning of the U.S. economy and government. • Cybersecurity: Promote outcome-oriented information sharing (e.g., greater situational awareness) between the public and private sectors regarding cyber threats to critical infrastructure; remove outdated legal barriers to information sharing while protecting personal privacy; increase awareness and education of U.S. through a public-private partnership with Federal, State, and local entities to promote an enterprise approach to cybersecurity and preparedness. • Emergency Preparedness and Response: Provide DHS, including the Federal Emergency Management Agency with policy information and business expertise to improve national disaster preparedness, response, and logistics capabilities; convene events with State chambers, business leaders, and Federal agencies to spur businesses to plan, prepare, and test their emergency management and business continuity plans against multiple hazards, whether manmade or natural. • Supply Chain Security: Promote a trade framework that facilitates the efficient movement of goods through the global supply chain; ensure public- and private-sector cooperation when identifying threats and creating appropriate solutions to maximize the effect on security and minimize the effect on business and trade.

<p>Working Groups</p>	<p>Fulfilling the mission is the voluntary work of committees, subcommittees, task forces, and councils involving more than 1,500 representatives of member corporations, organizations, and the academic community.</p> <ul style="list-style-type: none"> • National Security and Emergency Preparedness Department: This Department is responsible for the development and implementation of the U.S. Chamber’s homeland and national security policies. It works in tandem with 160 of the Chamber’s members—commonly referred to as the National Security Task Force—who have a direct interest in homeland and national security issues and who represent nearly every commercial sector. The Department develops recommendations and offers solutions to Federal leaders on an array of homeland and national security challenges that affect the Nation and the global economy. • Cybersecurity Working Group: In 2008, the U.S. Chamber launched a Cybersecurity Working Group to educate its members and influence the cybersecurity policy debate (See “Cybersecurity”).
<p>Points of Contact</p>	
<p>Personnel</p>	<p>Thomas J. Donohue, President and CEO David C. Chavern, Executive Vice President and COO Myron Brilliant, Executive Vice President and Head of International Affairs Ann Beauchesne, Vice President of National Security & Emergency Preparedness</p>
<p>Board of Directors</p>	<p>More than 100 Directors provide leadership for the organization.</p>
<p>Partnerships and Programs Leveraged</p>	
<p>Federal Programs</p>	<ul style="list-style-type: none"> • ODNI: The U.S. Chamber partners with the ODNI and other elements of the U.S. Intelligence Community to create public-private information-sharing avenues with high-level officials and subject-matter experts to better protect the Nation from threats to national security. In 2012, the U.S. Chamber placed nominated members with the ODNI / DHS Office of Intelligence and Analysis Intelligence Community Analyst Private Sector Partnership Program. This initiative, which began in 2010, gives intelligence analysts and industry experts a forum to study security risks to the United States and its allies in areas of mutual interest, including telecommunications, emerging technologies, border security, supply chain security, and bio-defense.

Western Cyber Exchange (WCX) is a consortium of business owners, information technology professionals, and public-sector representatives focused on improving cybersecurity at the regional level. Based in Colorado Springs, Colorado, the nonprofit promotes a cross-sector, regional approach to cybersecurity. It was started to engage private- and public-sector partners in an innovative, integrated approach to address collective risk at the community level, particularly because of the number of military installations, national laboratories, critical infrastructure, and other high-value targets in the area.

Geographic Focus	Members
 <p>States of Colorado, New Mexico, and Wyoming</p>	<p>Participants</p> <ul style="list-style-type: none"> • Small- and medium-sized businesses • City of Colorado Springs • Utility providers • Academic institutions • Colorado Division of Homeland Security and Emergency management • Colorado Information Analysis Center • Transportation Security Administration <div style="text-align: center;">  <p>35 participants</p> </div>

Sector(s) of Focus			
 <p>Communications</p>	 <p>Defense Industrial Base</p>	 <p>Energy</p>	 <p>Information Technology</p>

Establishment	
<div style="border: 1px solid black; border-radius: 15px; padding: 10px; display: inline-block;"> <p>2010</p> </div>	<p>WCX, founded in 2010, is a consortium of business owners, information technology (IT) professionals, and government representatives.</p>

Funding	Governance	Primary Activities
<ul style="list-style-type: none"> • Private-sector funding • FEMA grants 	<ul style="list-style-type: none"> • Housed within a 501(c) (6) nonprofit 	<ul style="list-style-type: none"> • Information sharing • Emergency operations • Partner education and exercises

Keys Factors of Partnership Success

- Through exercises, WCX raises awareness about the potential widespread effect of a cyber attack. This helps build support and is a practical way to address cybersecurity, a broad, national issue. WCX activities and work in the region enabled a paradigm shift within the community; leaders now recognize the organization as a mechanism for addressing cybersecurity and preparedness issues and sharing information.

Snapshots of Recent Success

- The WCX Forum Initiative involves a series of virtual sessions that help build trust, share best practices and cyber attack information, and facilitate dialogue on how to build cyber resilience. In an effort to build trust, the initiative includes a nomination and validation process, including requiring forum members to sign a confidentiality agreement.
- WCX partnered with the Federal Emergency Management Agency (FEMA), the State of Colorado, the Colorado Emergency Preparedness Partnership (CEPP), and Colorado Technical University to hold a community emergency preparedness cyber exercise to raise awareness for emergency management personnel about the potential widespread effect of a cyber attack.
- WCX has been nominated twice for community business excellence awards.

Critical Infrastructure Activities

<p>Training and Exercises</p>	<ul style="list-style-type: none"> • Training and exercises sponsored by WCX generally focus on increasing awareness of cybersecurity issues within the community. • Cybersecurity Training and Awareness Seminar: WCX partnered with a training group to conduct two seminars to raise awareness about cybersecurity preparedness at the local level. • Emergency Management Cyber Attack Exercise: WCX partnered with CEPP and the Colorado Technical University to educate local emergency managers and critical infrastructure leaders about cybersecurity issues and interdependencies. • Workforce Development: Through its partnerships with universities, students are able to secure internships with WCX to assist in research and analysis. The goal of the internship program is to teach and develop the skill sets needed to address cybersecurity issues. The trained interns could possibly return to WCX in the future as analysts, thus enabling WCX to be self-sustaining.
<p>Information Sharing</p>	<ul style="list-style-type: none"> • Threat Exchange Platform: WCX has developed a threat-exchange platform, integrating two partners' technologies to share information in real time about what is happening on networks and allow participants to increase defenses and get ahead of cyber attacks (using MITRE Corporation's Collaborative Research Into Threats, Structured Threat Information eXpress, Trusted Automated eXchange of Indicator Information approaches and systems). In addition to supplying a collaboration platform for information sharing, WCX plans to establish an analysis capability to develop and disseminate actionable reports based on the information gathered in the collaboration portal. • Fusion Center: WCX is not integrated with the Colorado Information and

Critical Infrastructure Activities

	<p>Analysis Center, the State’s fusion center; however, the two entities share information on occasion. A possible future partnership with the WCX as a resource for cybersecurity issues has been discussed.</p> <ul style="list-style-type: none"> • WCX Forum Initiative: These forums are a series of virtual sessions that help build trust, share best practices and cyber attack information, and facilitate dialogue on how to build cyber resilience. In an effort to build trust, the initiative includes a nomination and validation process, including requiring forum members to sign a confidentiality agreement. WCX also has an agreement to address State sunshine laws and security exclusions. <ul style="list-style-type: none"> – IT User Forum: This forum is targeted for technical experts to collaborate and share information. – Management Forum: WCX is currently developing this forum, composed of business owners and leaders, to enable discussion and decisionmaking on recommendations and solutions developed by the IT User Forum.
<p>Emergency Response</p>	<ul style="list-style-type: none"> • Future Role: WCX is not currently involved in emergency response, but it is in regular communication with the Colorado Springs Emergency Manager. It is unclear whether WCX will eventually have a seat at the Emergency Operations Center; it could serve as a facilitator and resource in the event of a cyber emergency.
<p>Partnerships</p>	<ul style="list-style-type: none"> • Primary Partners: See “Members” for a full listing of partners. • Supporting Partners: Colorado Networks; CB Insurance; Rocky Mountain Technology Alliance; Colorado Springs Regional Business Alliance; Imprimis Inc.; S3; Viridity Energy; Count Sheriffs of Colorado; University of Colorado, Colorado Springs, Center for Homeland Security; DSoft; CSOC; Imprimis; i2IS; Security Horizons; Amnet; S3; Auburn Research and Technology Foundation; and Colorado Technical University. As new States are identified for collaboration, such as New Mexico and Wyoming, additional partners will be identified. • Strategic Partners: WCX signed strategic alliance agreements with the Advanced Cyber Security Center in Boston, Cyber Huntsville in Alabama, and the Auburn Resource and Technology Foundation. The strategic partnerships allow sharing of best practices, drive advocacy, and raise awareness about cybersecurity. Recently, a consortium has emerged involving the WCX, University of Colorado at Colorado Springs, and Pikes Peak Community College to pursue research, education, internships, and knowledge sharing related to cyber resilience and the role of public-private partnerships. • Regional Consortium Coordinating Council (RC3): The WCX Co-Founder serves as the current Chair of the RC3 Cybersecurity Working Group.

Organization Background

Establishment, Governance, and Funding

Establishment	WCX, founded in 2010, is a consortium of business owners, IT professionals, and government representatives. Based in Colorado Springs, Colorado, the nonprofit promotes a cross-sector, regional approach to cybersecurity. It was started to engage private- and public-sector partners in an innovative, integrated approach to address collective risk at the community level, particularly because of the number of military installations, national laboratories, critical infrastructure, and other high-value targets in the area.
Governance	WCX is currently housed within the Rocky Mountain Technology Alliance, a 501(c)(6) nonprofit organization. It was established through a charter signed by the city of Colorado Springs, utility providers, the University of Colorado, and Colorado Technical University, and others. WCX is working toward becoming a separate nonprofit organization. As part of a nonprofit, WCX is able to be a trusted broker between all participants, allowing for a free exchange of information.
Funding	Two companies, Imprimis and I2IS, are providing the principal backing for the initiative as it moves toward a fee-for-service model and begins attracting members. Other community backers provide in-kind support including expertise and labor. It has also received a FEMA Community Resilience Innovation Challenge grant.
Personnel	WCX staff includes about five people, who are supplemented with in-kind support from backers. As membership grows, WCX expects it will need to add personnel (e.g., analysts) to shift from a structure similar to a help desk to 24/7 operations.

Mission and Objectives

Mission	WCX's mission is to transcend the information-sharing barriers that exist between government and industry to improve cybersecurity.
Objectives	<ul style="list-style-type: none"> • Be the source for cybersecurity information to improve capabilities at the regional level. • Share, analyze and provide actionable cyber attack threat-data among the membership. • Validate community cybersecurity interdependencies and confirm WCX operations model, role, and responsibilities. • Expand membership and partnerships, and establish a cybersecurity marketplace that improves readiness. • Improve business climate by creating a cyber-resilient, cyber-aware, and cyber-capable community. • Extend WCX mission and partners, and facilitate cybersecurity readiness integration between local, regional, and national organizations. • Conduct pilots, demonstrations, and projects that integrate WCX with Smart Grid, national programs, and other important initiatives.

Organization Background

Working Groups	<ul style="list-style-type: none">• Economic Development Team• Technical and Operations Team• Membership and Programs Team• Community Mobilization Committee• IT User Forum• Management Forum
----------------	--

Points of Contact

Co-Founder	Doug DePeppe
------------	--------------

Partnerships and Programs Leveraged

Federal Programs	<ul style="list-style-type: none">• DHS Transportation Security Administration (TSA): Personnel from TSA participate in WCX activities.• FEMA Community Resilience Innovation Challenge Grant: See “Governance and Funding” for additional information.
------------------	--

Acronym List

AHC	All Hazards Consortium
APIP	Alaska Partnership for Infrastructure Protection
ARDEC	Armament Research Development and Engineering Center
BAESIC	Bay Area Emergency and Security Information Collaborative
BayCOP	Bay Area Common Operating Picture
BCS	Business Continuity Services
BENS	Business Executives for National Security
BEOC	Business Emergency Operations Center
BOC	Business Operations Center
BRAP	Business Recovery Access Program
CAL OES	California Office of Emergency Services (formerly the California Emergency Management Agency)
CATEX	Catastrophic Exercise CATEX
CELL	Counter-Terrorism Education Learning Lab
CEPP	Colorado Emergency Preparedness Partnership
CIAC	Colorado Information Analysis Center
CIKR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
CONNECT Colorado	Cooperative Initiative for Emergency Capability Tracking in Colorado
CPPTF	Chicago Public/Private Task Force
CRA	California Resiliency Alliance
CRDR	Center for Regional Disaster Resilience
CS&C	DHS Office of Cybersecurity and Communications
DDoS	Distributed denial of service
DHSEM	Alaska Division of Homeland Security and Emergency Management
DHS	U.S. Department of Homeland Security
DRIPP	Delaware River Infrastructure Protection Project
EF	Enhanced Fujita (scale)
EOC	Emergency operations center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FRAC	First Responder Authentication Credential
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
GCC	Government Coordinating Council
GLHC	Great Lakes Hazards Coalition

HSAC	Homeland Security Advisory Council
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
HSIN-APIP	Alaska Partnership for Infrastructure Protection, Homeland Security Information Network portal
IEMA	Iowa Emergency Management Association
IND	Improvised nuclear device
ITTF	Illinois Terrorism Task Force
IP	DHS Office of Infrastructure Protection
IT	Information technology
JTTF	FBI Joint Terrorism Task Force
LEPC	Local Emergency Planning Committee
MERR	Missouri Emergency Resource Registry
MIAC	Missouri Information Analysis Center
MOP3	Missouri Public-Private Partnership
MOU	Memorandum of understanding
NBEOC	FEMA National Business Emergency Operations Center
NLE	National Level Exercise
NLE11	National Level Exercise 2011
NCR	National Capital Region
NCRIC	Northern California Regional Intelligence Center
NEDRIX	Northeast Disaster Recovery Information X-Change
NIPP	National Infrastructure Protection Plan
NIPP 2013	<i>National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience</i>
NIST	National Institutes of Standards and Technology
NJBF	New Jersey Business Force
NJIT	New Jersey Institute of Technology
NWWARN	Northwest Warning, Alert & Response Network
ODNI	Office of the Director of National Intelligence
OEMC	Chicago Office of Emergency Management and Communication
OES	Office of Emergency Services
OHA	DHS Office of Health Affairs
P2CAT	Public-Private Coordination Action Team
PG&E	Pacific Gas and Electric
PIV-I	Personal Identity Verification Interoperable
PNWER	Pacific NorthWest Economic Region

PSA	DHS Protective Security Advisor
PSC	Private Sector Committee
RC3	Regional Consortium Coordinating Council
RCPGP	Regional Catastrophic Preparedness Grant Program
RCPT	Regional Catastrophic Planning Team
RPC	Regional Partnership Council
RRAP	Regional Resiliency Assessment Program
S&T	DHS Science and Technology Directorate
SEERN	SouthEast Emergency Response Network
SEMA	State Emergency Management Agency
SEOC	State Emergency Operations Center
SIP	Safeguard Iowa Partnership (SIP)
SLTT	State, local, tribal, and territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SOC	State Operators Center (SOC)
STIC	Statewide Terrorism Intelligence Center
TEEX	Texas A&M Engineering Extension Service
TISP	The Infrastructure Security Partnership
TOPOFF	Top Officials Program
TSA	Transportation Security Administration
UASI	DHS Urban Areas Security Initiative
US-CERT	United States Computer Emergency Readiness Team
VOADs	Voluntary Organizations Active in Disasters
WCC	World Cares Center
WCX	Western Cyber Exchange
WG	Working Group
WSFC	Washington State Fusion Center

Reference Library

The following resources are referenced in the Regional Consortium Coordinating Council's *Member and Mission Landscape Study* (2014). Direct links are provided to access the resources, sponsors, and additional information.

Infrastructure Resilience and Interdependencies Resources

[Regional Disaster Resilience Guide 2011 Edition](#): The Bay Area Center for Regional Disaster Resilience led a Critical Infrastructure and Regional Resilience Task Force to develop guidelines for regional resilience planning for [The Infrastructure Security Partnership](#) (TISP). The resulting *Regional Disaster Resilience Guide 2011 Edition* is currently in use by organizations across the Nation. Other TISP publications can be found here: <http://www.tisp.org/index.cfm?pid=10261>.

[Regional Catastrophic Earthquake Logistics Plan](#): The [California Resiliency Alliance](#) held a series of stakeholder workshops in early October 2013 to inform the development of a Bay Area restoration of critical lifelines appendix to a regional logistics plan. View the *Regional Catastrophic Earthquake Logistics Response Plan* (2014), complete with *Appendix G: Critical Lifelines* here: <http://www.bayareauasi.org/node/1170>.

[Domestic Preparedness Action Plan-- Building Resilient Regions for a Secure and Resilient Nation](#): Regional [U.S. Chamber of Commerce](#) offices in Indiana and Texas promoted Domestic Preparedness Resiliency Workshops in their regions in 2012. The workshops brought together local chambers of commerce, associations, and small businesses to help create a regional resilience report to be published and shared with Washington, D.C. officials. View the *Building Resilient Regions for a Secure and Resilient Nation* report here: <http://www.domesticpreparedness.com/Commentary/DP40>.

[Regional Transportation Recovery Annex](#): The PNWER Center for Regional Disaster Resilience (CRDR) established a supply chain resilience public-private sector working group that is able to provide input and advice on issues related to regional supply chain resilience. For this supply chain resilience project, [PNWER CRDR](#) is working with the [Puget Sound Regional Catastrophic Planning Team](#). The project includes examining the *Puget Sound Transportation Recovery Annex* of the [Catastrophic Disaster Coordination Plan](#) (2013) and in particular, the maritime information. View the *Puget Sound Transportation Recovery Annex* and other regional catastrophic preparedness documents here: http://www.emd.wa.gov/plans/plans_index.shtml#R.

Energy Systems and Interdependencies Study: The [Great Lakes Hazards Coalition](#) (GLHC) conducted a study on the Energy Sector and its interdependencies in the Great Lakes Region. A copy of the report is available to [GLHC members](#). More information on GLHC's initiatives can be found here: <http://www.theglhc.org/currentinitiatives.htm>.

Information-Sharing Resources

[Situation Reports](#): The [California Resiliency Alliance](#) provides situational reports to its members to inform their decisionmaking process regarding employee safety and business continuity through a variety of mechanisms. View the Situation Reports here: <http://calpartnership.ning.com/group/sitreps>.

Awareness Resources: The [Business Emergency Operations Center \(BEOC\) Alliance](#) disseminates alert messages, notifications, and briefings on a variety of topics. The [New Jersey Business Force](#) disseminates, twice a month, awareness notes to members on a variety of topics, including cybersecurity, terrorism, public health, and natural disasters.

- [CyberCop Portal](#): The BEOC Alliance disseminates For Official Use Only (FOUO) information and controlled unclassified information to members through the NC4 Cybercop Portal.
- Background information on awareness communications can be found here: http://www.beoalliance.org/#!about_us/csgz.

Emergency Operations Resources

Bay Area Public-Private Partnership Initiative: The [California Resiliency Alliance](#) is working with the [Bay Area Urban Areas Security Initiative](#), under a public/private sector partnership project, to facilitate pre-disaster planning and partnerships to support disaster response through the two products below. The Bay Area UASI posts project products on its [Resources Search Page](#).

- Private Sector Resiliency Advisory Committees of business and association representatives will inform a *Public-Private Partnership Strategic Plan* to serve as a capability-building roadmap.
- Under the Bay Area Public-Private Partnership Initiative an updated *Activation Guide: for Private Sector EOC Representatives* to formalize the staffing of private volunteers in the Business Operations Center will be developed. The existing [Bay Area EOC Private Sector Liaison Guide](#) (2012) and other resources can be viewed here: <http://calpartnership.ning.com/group/eoc>.

Emergency Operation Center Protocols: [ChicagoFIRST](#) voluntarily drafted the protocol for how the private sector operates in the Chicago emergency operation center (EOC). The protocols and other resources can be found through the [ChicagoFIRST search page](#).

Emergency Operations Center Capabilities Matrix: [New Jersey Business Force](#) and the [Business Emergency Operations Center \(BEOC\) Alliance](#) helped define the BEOC concept and developed a capabilities matrix. The BEOC model can be replicated in other regions, across the Nation, or in other countries. In addition, the BEOC capabilities matrix builds a deeper understanding of capabilities for collaboration and communication in emergency response. The BEOC capabilities matrix can be viewed within Dr. M.J. Chumer's paper: [The Business Emergency Operations Center \(BEOC\) - A Model for Inter-Agency and Inter-Sector Communication and Collaboration](#).

Pacific Northwest Emergency Management Arrangement: The PNWER Center for Disaster Resilience participated in the development of a bi-national plan for recovering from a disaster in a cross-border area. The plan can be viewed here: <http://www.gpo.gov/fdsys/pkg/PLAW-105publ381>. An overview of the framework for bi-national communications and information sharing can be viewed here: <http://www.regionalresilience.org/PNEMA>.

Recovery Toolkit: [Safeguard Iowa Partnership](https://safeguardiowa.wildapricot.org/recovery) (SIP) is in the process of developing a recovery toolkit for businesses to use following a disaster. SIP's existing recovery resources can be viewed here: <https://safeguardiowa.wildapricot.org/recovery>.

Exercises and Lessons Learned

[Multi-State Fleet Response Working Group Workshop Report](#): The [All Hazards Consortium](#) assessed lessons learned from Superstorm Sandy and identified opportunities for improving movement of fleets in response to emergency events. As part of the [Multi-State Fleet Response Working Group's](#) workshop, the U.S. Department of Energy held an Energy Roundtable on the effects of the storm on the Energy Sector, focusing on fuel availability. Following the workshop, information was captured in a final report, *The Multi-State Fleet Response Working Group Workshop Report: Rapid Critical Infrastructure Restoration Through Joint Integrated Planning For the Movement of Private Sector Resources in Response to Hurricane Sandy*. The report can be viewed here: <http://www.fleetresponse.org/resources/fleet-wg-reports/>.

Cross-Border Issues: The [Great Lakes Hazards Coalition](#) (GLHC) conducted a cross-border, regional tabletop exercise with the National Guard in 2011. An after-action report was developed and presented at the GLHC December 2011 meeting. [GLHC members](#) can find the after-action report in the Document Library on GLHC's Web site. More information on GLHC's initiatives can be found here: <http://www.theglhc.org/currentinitiatives.htm>.

[Blue Cascades Regional Exercise Series Integrated Action Plan](#): The [Center for Regional Disaster Resilience](#) developed the Blue Cascades Exercise Series to explore regional infrastructure interdependencies in the Pacific Northwest. After each exercise, stakeholders contributed to an action plan to address the issues uncovered during the exercise. The *Blue Cascades Regional Exercises Integrated Action Plan* (2010) can be viewed here: <http://www.regionalresilience.org/CurrentInitiatives/BlueCascades.aspx>.

Cybersecurity Resources

[Internet Security Essentials for Business Guidebook](#) (October 2010): The [U.S. Chamber of Commerce](#) released this guidebook to urge business owners, managers, and employees to adopt fundamental Internet security practices to reduce network weaknesses and make the price of successful hacking increasingly steep. The Guidebook can be viewed here: <https://www.uschamber.com/internet-security-essentials-business-20>.

[Improving Our Nation's Cybersecurity through the Public-Private Partnership](#) (March 2010): [U.S. Chamber of Commerce](#) and four partners released a paper to educate policy makers in the White House administration and Congress. The White Paper can be viewed here: <http://www.uschamber.com/sites/default/files/legacy/issues/defense/files/2011cybersecuritywhitepaper.pdf>.

Public Health and Preparedness Resources

[Community Health Resilience Guide](#): In partnership with the [U.S. Department of Homeland Security \(DHS\) Office of Health Affairs](#) and a national stakeholder group of practitioners, the Bay Area Center for Regional Disaster Resilience developed a community health resilience planning template and toolkit of stakeholder-validated best practices, tools, and technologies.

The goal of the initiative is to enhance the national resilience for the health effects of all hazards. The Community Health Resilience Guide can be viewed here:
<http://www.naccho.org/topics/emergency/upload/CHRI-Updated-Annotated-Guide-Outline-with-Stakeholder-Comments.pdf>.

Flu Vaccine Toolkit: [Safeguard Iowa Partnership](#) (SIP) partnered with the Iowa Department of Public Health to increase influenza vaccination rates in the State. A SIP survey of businesses was able to identify barriers and best practices for employers. Using this information, a flu vaccine toolkit was developed for businesses. The Toolkit can be viewed here:
<https://safeguardiowa.wildapricot.org/LPHA-employer-vaccination-toolkit>.

Preparedness Outreach and Awareness: [Safeguard Iowa Partnership](#) (SIP) created an annual event, the [Prepare Fair](#), to improve awareness among residents about the importance of preparedness. On its Website, SIP offers a [“20 Weeks to Preparedness” calendar](#) to help individuals create an emergency supply kit and prepare for emergencies. The emergency supplies calendar can be viewed here: <https://safeguardiowa.wildapricot.org/20-weeks-to-preparedness>.

Surveys

Best Practices: [ChicagoFIRST](#) conducts member surveys of best practices and shares results to facilitate member action plans and approaches to emergencies. The surveys aggregate best practices regarding business continuity, evacuations, and emergency telecommuting.

Business Damage Survey: [Safeguard Iowa Partnership](#) worked with the Iowa Emergency Management Association to develop an online survey to provide an easy way for businesses to communicate damage information following a disaster. Information on the Business Damage Survey can be viewed here: <https://safeguardiowa.wildapricot.org/business-damage-survey>.