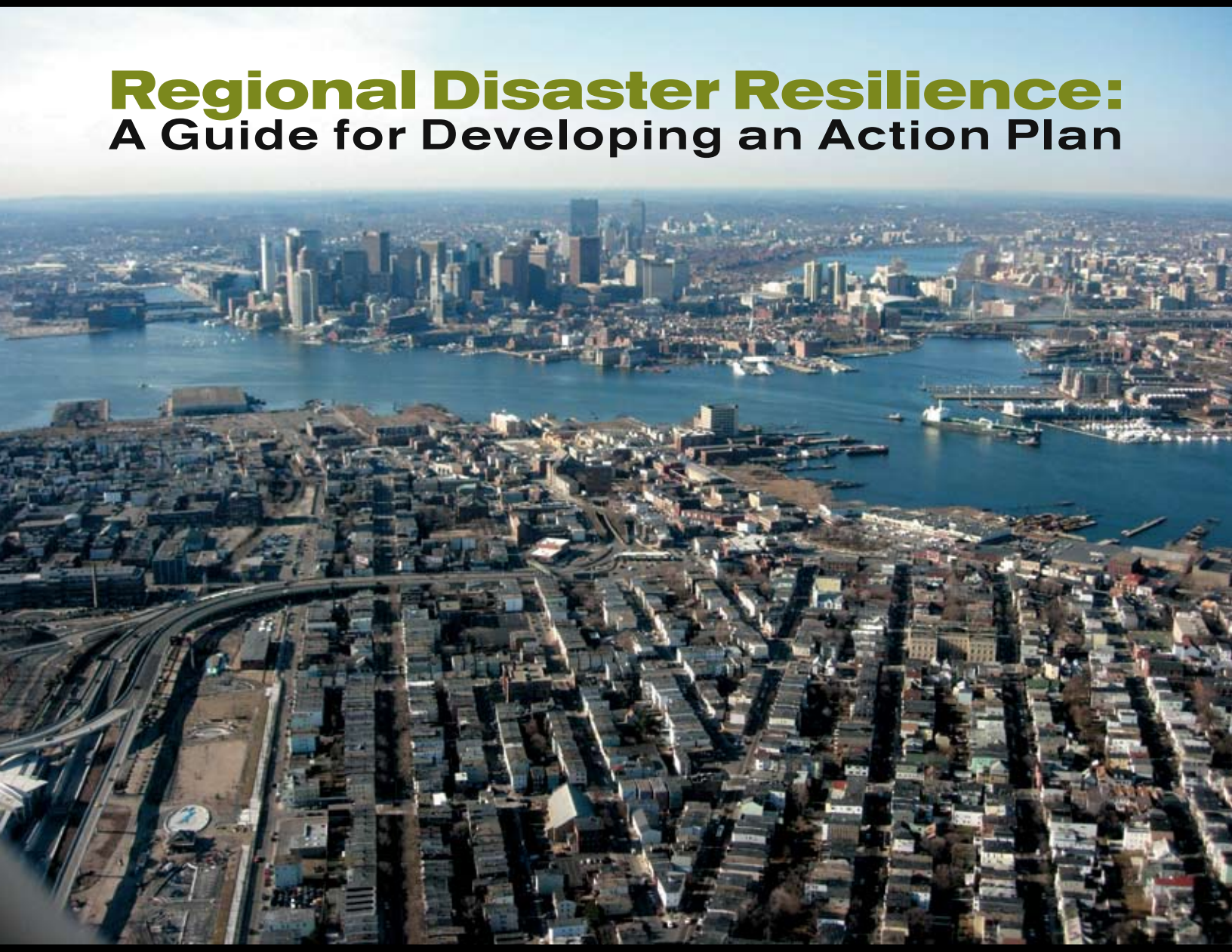
Regional Disaster Resilience:
A Guide for Developing an Action Plan



Developed by The Infrastructure Security Partnership (TISP)

■ June 2006 ■

Regional Disaster Resilience:
A Guide for Developing an Action Plan

Developed by The Infrastructure Security Partnership (TISP) • June 2006

ISBN 0-7844-0880-7
Manufactured in the United States of America.

Cataloging in Publication Data on file with the Library of Congress.

American Society of Civil Engineers
1801 Alexander Bell Drive
Reston, Virginia, 20191-4400

Cover Photographs: The city of Boston manifests the complexities and interdependencies of infrastructure systems that could be affected by a disaster—natural or man-made. Photographs by Marla Dalton

The Infrastructure Security Partnership (TISP)
1801 Alexander Bell Drive
Reston, VA 20191
Phone: (703) 295-6231
Fax: (703) 295-6361
http://www.tisp.org

Table of Contents

Overview

Regional Disaster Resilience: A Guide for Developing an Action Plan provides a much-needed strategy to develop the level of preparedness necessary for communities to adequately deal with major disasters in today's complex and interdependent world. The guide is meant for use by government, private-sector, and other organizations with specific missions or vested interests in assuring that the regions in which they reside can withstand the effects of multihazards and respond and recover rapidly when disasters strike.

The guide provides key definitions and a set of common assumptions that underpin regional disaster resilience. Using a simple, practical how-to approach, the guide lists 12 categories of typical "needs" gleaned from lessons learned from previous disasters—natural and man-made. The guide recommends short-term, medium-term, and long-term activities to address these respective shortfalls. A website devoted to best practices/solutions and related resources mapped to the recommended activities in the guide is under development at www.tisp.org. The aim is to provide users of the guide with the ability to examine and customize approaches, tools, and technologies already developed to foster standardization across interdependent infrastructures and regions and to avoid reinventing the wheel. The guide will be updated as needed to reflect new information on needs, activities, and solutions.

About The Infrastructure Security Partnership (TISP)

The Infrastructure Security Partnership (TISP) was established following the tragic events of September 11, 2001, as a national forum for public and private-sector organizations to collaborate on issues regarding the resilience of the nation's critical infrastructure against the adverse impacts of natural and man-made disasters. TISP members—who represent the design, construction, operation, and maintenance communities; local, state, and federal agencies; academe; and other organizations concerned about disaster preparedness, response, and recovery—work together to identify and develop cost-effective solutions by leveraging their collective resources, experience, technical expertise, research and development capabilities, and knowledge of public policy regarding natural and man-made disasters. Since its establishment, membership has grown to more than 100 organizations representing more than 1.5 million individuals and firms.

Background on the Guide

TISP is proud of its role as a national forum for stakeholders from all sectors, levels of government, and disciplines to share ideas to improve the resilience of our critical infrastrucure. In tapping the tremendous potential for collaboration among TISP partners, the Task Force on Regional Disaster Resilience was created at the conclusion of the fourth annual TISP Congress on Infrastructure Security for the Built Environment (ISBE 2005) held in October 2005. *Regional Disaster Resilience: A Guide for Developing an Action Plan* was developed by this task force as an unprecedented and much-needed model plan to improve multihazard preparedness. The task force included nearly 100 members representing various disciplines, sectors, and geographic regions with roles in ensuring that the infrastructures that underpin our way of life can withstand major disasters and be restored expeditiously if damaged or disrupted. Under the leadership of TISP vice chairs Edward Hecker of the U.S. Army Corps of Engineers and Paula Scalingi, Ph.D., of The Scalingi Group, LLC, the task force members worked as a virtual team to create the guide as a flexible, dynamic framework for use by all levels of government, key service providers, and other organizations in providing regional preparedness. On February 15, 2006, the guide was sent for external review to government, private-sector, and other organizations with expertise in disaster preparedness. The guide was updated and reviewed by the task force prior to its publication in June 2006.

TISP encourages readers to use the guide to bring together key regional stakeholders in partnership to implement a comprehensive regional strategy for disaster preparedness. TISP welcomes ideas on how to continuously develop the guide as additional information is obtained about what is necessary to achieve regional disaster resilience. The task force has been institutionalized within TISP as the Regional Disaster Resilience (RDR) Committee.

Special thanks go to the members of the task force who have volunteered their expertise to make this guide possible and to the American Society of Civil Engineers (ASCE) for providing editorial and graphics support during the final preparations of the guide.

Member participation in TISP and its important initiatives will help raise awareness that will lead to sustainable security improvements to our nation's infrastructure. Threats to the country's infrastructure remain all too real. TISP relies on the efforts of all of its partners to participate in TISP activities and to help guard against complacency.

Regional Disaster Resilience:
A Guide for Developing an Action Plan

Purpose

Regional Disaster Resilience: A Guide for Developing an Action Plan is intended to provide a flexible, dynamic, high-level framework for use by all levels of government, service providers, and other organizations to create an action plan to help develop or improve comprehensive regional preparedness. The guide is intended to be as comprehensive as possible in offering the range of actions that organizations can collectively and individually take—on the basis of their perceived needs—to achieve regional disaster resilience. The focus is on bringing together public and private-sector organizations as well as other entities with roles and missions or vested interests in disaster preparedness to address multihazards, the goals being to sensibly and cost effectively secure interdependent cyber and physical critical infrastructures.

Key Definitions

- **Disaster resilience** refers to the capability to prevent or protect against significant multihazard threats and incidents, including terrorist attacks, and to expeditiously recover and reconstitute critical services with minimum damage to public safety and health, the economy, and national security.

- **A region** is any area that is defined as such by resident stakeholders responsible for disaster preparedness and management. A region can be a municipality, a single state (or province), or a portion of a state and may be multi-jurisdictional or cross national borders. Regions generally have certain accepted cultural characteristics and geographic boundaries and tend to coincide with the service areas of the infrastructures that serve them.

- **Key stakeholders** include public and private-sector organizations that play major roles in providing essential services and products that underpin the economic vitality of a region, the welfare of its citizens, support national security, and that are necessary for disaster response and recovery.

- **Critical infrastructure** includes systems, facilities, and assets so vital that if destroyed or incapacitated would disrupt the security, economy, health, safety, or welfare of the public. Critical infrastructure may cross political boundaries and may be built (such as structures, energy, water, transportation, and communications systems); natural (such as surface or groundwater resources); or virtual (such as cyber, electronic data, and information systems).

- **Multihazards** include significant events such as infrastructure deterioration, natural disasters, accidents, and malevolent acts.

- **Sensible security** is the level of protection achieved through design, construction, and operation that mitigates adverse impact to systems, facilities, and assets in proportion to their value to society and their likelihood of being affected by natural and/or man-made events.

Scope

This guide provides a set of comprehensive preparedness guidelines and a benchmark for gauging the level of regional disaster resilience. The guide is intended to build upon existing plans and procedures of jurisdictions and organizations and to demonstrate remaining readiness gaps to be addressed. It includes a detailed inventory of validated needs that have been identified through infrastructure vulnerability assessments and studies, interdependencies exercises, and lessons learned from major events, including natural disasters (recent hurricanes—particularly Katrina—floods, earthquakes, and forest fires); man-made major technological disruptions (such as the August 14, 2003, power blackout that affected some 50 million Americans); and terrorist events (such as the September 11 and anthrax attacks in the fall of 2001). In addition, the guide recommends specific short-, medium-, and long-term tasks, activities, and projects designed to meet these needs. A web site providing examples of best practices and solutions keyed to the recommended activities in this guide is currently under development at www.tisp.org to enable guide users to minimize costs and foster standardization across regions.

The guide is a "living document" that will be updated on a regular basis to reflect evolving knowledge, further lessons learned, and new solutions. It is assumed that guide users will develop and foster public-private partnerships to improve their region's preparedness capabilities, test for readiness shortfalls, and make additional improvements as a continuous process of moving toward disaster resilience.

Fundamental Assumptions Underlying an Action Plan

An action plan is based on the following assumptions:

1. Comprehensive regional preparedness is key to ensuring that communities, states, and the nation can expeditiously respond to and recover from disasters of all types, particularly extreme events.

2. National and global infrastructures are increasingly complex and interconnected, resulting in physical and cyber vulnerabilities that we are only just beginning to understand. Stakeholder organizations are becoming increasingly aware of infrastructure interdependencies but need to broaden their knowledge of the extent of these linkages and their effects on responsibilities, operations, and business practices, particularly regarding large-scale and/or long-term disruptions.

3. An integrated and complementary cyber and physical approach is required to determine how best to secure interdependent infrastructures, ensure expeditious response and recovery, and build resiliency to address regional disasters. Consequently, there needs to be increased interaction among physical and cyber security personnel and emergency managers and operators to raise awareness of threats and vulnerabilities.

4. Today's preparedness needs require a comprehensive, multihazards regional approach that addresses natural disasters of all types, human error, systems failures, pandemics, and malevolent acts, including those involving cyber systems and weapons of mass destruction (chemical, biological, radiological, and nuclear devices).

5. Hurricane Katrina clearly demonstrated that existing federal, regional, state, and local disaster management plans need improvement in order to successfully deal with extreme disasters, natural or man-made. New thinking, approaches, training, and exercises as well as unprecedented intergovernmental collaboration and planning are required. This all must be accomplished in cooperation with private-sector and other key stakeholders.

6. The creation of regional public-private partnerships is necessary to bring together key stakeholders to build trust, foster information sharing and coordination, identify and assess vulnerabilities and other preparedness needs, and develop and implement solutions. Such partnerships should include all levels of government, utilities and other service providers, commercial enterprises (including businesses essential to localities; manufacturers; producers; processors; and distributors of important commodities and products), nonprofits, and community and academic institutions.

7. Extensive work has already been accomplished by the multihazards community that can be used to assist in preparedness for terrorist attacks.

8. Advances in information technology, engineering, materials, and biosciences as well as other disciplines are creating new vulnerabilities that we must anticipate.

9. Because of infrastructure interdependencies, protection of "critical assets" by means of physical security is only one important element of the holistic approach necessary to ensure essential services and products. There is also a need for cost-effective mitigation of potential and actual damage from disruptions, particularly those causing cascading effects that can incapacitate a region and impede rapid response and recovery.

10. Security and disaster resilience should be incorporated into cyber and physical systems in the development phase on the basis of assessed risk under various scenarios. Resilience can include system hardening, building in redundancies, implementing backup systems, and other mitigation measures.

11. Determining the criticality of infrastructure assets presents a major challenge, particularly for states and local governments that must make investment tradeoffs on security and mitigation measures. Criticality is often in the eyes of the beholder and is dependent upon a given situation. The large and diverse number of critical assets within a region,

constrained state and local resources, and our need to gain better understanding of infrastructure interdependencies require the development of criteria for and a risk-based approach to identifying critical assets.

12. Environmental protection is integral to infrastructure protection and resiliency. Waste products and toxic holding sites, for example, should be considered security risks as well as environmental risks.

13. A major challenge is obtaining the necessary data on infrastructure interdependencies to enable the development of assessment and decision tools to provide greater understanding of associated cyber and physical vulnerabilities and how best to minimize them. Surmounting this challenge requires cooperation and finding ways to identify, collect, securely store, and share information provided by stakeholders that play significant roles in regional disaster preparedness.

14. Development and maintenance of mutual assistance agreements, user agreements, memorandums of understanding (MOUs), and other types of cooperative arrangements are essential to sound preparedness planning and disaster management. Such mechanisms enable jurisdictions, private-sector organizations, and other stakeholders to resolve resource requirements and allocations, security and legal issues, sharing of proprietary information, and cost reimbursement in advance of emergencies.

15. Disaster response, recovery, and restoration are local and state missions, not the sole responsibility of the federal government.

16. Sorting out and defining roles and responsibilities—including determining who is in charge of particular functions—is fundamental to ensuring effective disaster preparedness, response, recovery, and restoration.

17. The federal government—historically through the Federal Emergency Management Agency's (FEMA's) regional offices and other regional federal offices—provides necessary guidance and assistance in preparedness and disaster response at the local and state levels. This regional approach should be continued and enhanced.

18. Integration of federal defense assets into regional preparedness in an appropriate manner is essential in addressing extreme disasters that require resources above and beyond those available at the state/provincial and local level.

19. Assuring supply chains and the delivery of critical products, materials, and components is essential to disaster resilience and the vitality of the industrial base and has a direct and profound impact on regional/national economies and national security.

20. Where useful, codes, standards, and guidelines should be applied within and across organizations and jurisdictions to enhance security and preparedness and to minimize costs.

21. Channels of communication must be established conscientiously and comprehensively to include representatives and spokespersons from all key stakeholders; must be tested frequently to improve and correct shortcomings and to ensure that they work and have redundancy and resiliency to withstand infrastructure deterioration or destruction; must be maintained efficiently and regularly to ensure availability when needed; and must be owned by a well-established and defined entity with responsibility for administration and ongoing operations.

22. Law enforcement and public safety personnel at all levels should recognize the value of coordination with the public and private-sectors when developing strategies to protect critical infrastructures. Proactive involvement with operators of critical infrastructure should provide the basis for sharing information that mitigates vulnerabilities and creates an awareness of threats to a system or facility.

23. Progress has been made to better manage large-scale events by means of the creation of the National Incident Management System and other measures. However, sorting out roles and responsibilities during major disasters and terrorist attacks remains one of the greatest challenges. Disasters know no jurisdictional boundaries, and key stakeholders must collectively define their responsibilities under various scenarios, taking into account the evolving roles of federal agencies—for example, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Defense (DoD).

24. The private-sector and nonprofit community possess a wealth of available resources and capabilities that must be incorporated into regional disaster response and restoration planning and activities.

25. Health care and public health organizations play a unique and highly important role in disaster response and should be integrated into disaster planning.

26. Community institutions, the general public, and individuals with special needs must be involved in planning and exercises, and particular emphasis should be placed on education and awareness of threats, impacts, and local emergency response procedures. Evacuation plans must be realistic in taking into account infrastructure interdependencies and individuals with special needs.

27. The media play a unique and integral role in disaster management, performing an information dissemination and education function—occasionally as first responders—and as essential stakeholders with business continuity needs. The media need to participate in preparedness planning and exercises.

28. Any system or technology solution requiring confidential or sensitive information must be developed from inception through production with the highest appropriate level of information security. At the same time, the need for information security must be balanced with stakeholder need to know to increase understanding of interdependencies and facilitate preparedness planning.

29. Costs for technology solutions, maintenance, and upgrades must be affordable to states, localities, and private-sector organizations.

The Overall Goal and Objectives of an Action Plan

Goal

The goal of an action plan is to provide stakeholders with a flexible, dynamic, and comprehensive set of guidelines to assist in evaluating progress and to help them build on existing preparedness capabilities to achieve regional disaster resilience.

Objectives

- To provide a baseline of identified, stakeholder-validated, regional preparedness needs and activities/projects to address these needs in the following areas:

  I Awareness and understanding of interdependencies
  II Appreciation of cyber threats and incidents
  III Resilient and interoperable communications and information systems
  IV Risk assessment and mitigation
  V Cooperation and coordination
  VI Roles and responsibilities
  VII Response challenges
  VIII Recovery and restoration
  IX Business continuity and continuity of operations
  X Logistics and supply chain management
  XI Public information/risk communications
  XII Exercises, training, and education.

- Identify cost-effective short-term activities that can be implemented rapidly at little cost; medium-term (18-month to two-year) projects; and long-term (multiyear) activities to develop solutions to address preparedness shortfalls.

- Provide examples of available plans, technologies, and methodologies (best practices and solutions) that can be utilized to develop regional resilience in the following areas:

  - Prevention, protection, monitoring, detection, and sensor systems
  - Facility and systems design
  - Vulnerability and risk assessment methodologies
  - Analysis and decision support systems
  - Response and restoration tools, technologies, plans, and procedures.

An Action Plan to Develop Regional Disaster Resilience

Focus Areas

I. Awareness and Understanding of Interdependencies

A. Needs

1. Greater awareness of interdependencies-related vulnerabilities and what this means for creating the level, extent, and duration of self-sufficiency necessary for organizations and citizens in a major disaster.

2. Tools and approaches to "map" (identify and assess) regional and organizational physical and cyber interdependencies and associated vulnerabilities under normal conditions and under disruption scenarios, including extreme natural or man-made disasters, while safeguarding these data.

3. Methods to raise awareness of organizations' dependency upon information technology (IT)-related resources to maintain critical operations and to prepare for and execute response and recovery plans to deal with disruptions and disasters that involve loss or damage to electronic systems.

4. Incorporation of interdependencies into vulnerability and risk assessments and emergency response/restoration and business contingency plans.

5. Information for key stakeholders on the impacts of prolonged electric power disruptions and rolling blackouts on interdependent infrastructures.

6. Integration of emergency management/physical security functions and cyber security.

7. Increased understanding of U.S.-Canadian and U.S.-Mexican cross-border interdependencies.

8. Recognition of the unique situation of Hawaii and Alaska: these states are dependent on external products and services and the supply chains that provide them.

9. Increased understanding of worldwide dependencies and vulnerabilities associated with the use of the Internet for trade and communication.

10. Development of modeling and simulation capabilities at universities and research institutions to enable quantitative and qualitative assessments related to infrastructure interdependencies issues and decision points.

11. Understanding of interdependencies-related restoration needs in regional disruptions—for example, mitigation strategies, priorities, sequencing, and work-arounds.

12. Interdependencies exercises and related training.

B. Recommended Actions

Short-Term

1. Develop an infrastructure interdependencies template for use by stakeholder organizations to enable mapping physical and cyber linkages on a regional basis.

2. Develop a secure database for high-level information provided by stakeholders that includes mutually agreed upon security and information protection safeguards.

3. Compile a list—including point of contact (POC) information—of public and private organizations in the region that have similar interdependencies programs under way.

4. Conduct a regional infrastructure interdependencies tabletop exercise to provide initial baseline knowledge for regional stakeholders, explore particular interconnections in more depth, and test preparedness improvements.

5. Develop a web-based lessons-learned database to capture and share interdependencies-related knowledge from exercises and training conducted in various regions.

Medium-Term

6. Revise and improve existing preparedness and disaster management plans to address interdependencies, including those focused on nuclear/radiological, biological, and chemical incidents. Provide a strong focus on concepts of operations (CONOPS).

7. Examine evacuation and sheltering or shelter-in-place plans to ensure that they are realistic, taking into account facilities' limitations and regional interdependencies and using extreme disaster scenarios as baselines; revise plans to meet existing realities; and identify and implement preparedness activities, mitigation measures, and resource strategies necessary to achieve optimal evacuation and shelter procedures, revising plans accordingly.

8. Identify the economic and health and human safety ramifications of various security measures that may be put in place during a disruption or attack—for example, closing ports, interstates, tunnels, airports, bridges, or borders—to assess how these activities could complicate or facilitate response and recovery activities.

9. Develop a program addressing ongoing regional and targeted infrastructure interdependencies tabletop and field exercises to explore particular interconnections in greater depth and to test preparedness improvements.

10. Create incentives for academic studies to assess and understand worldwide interdependencies and vulnerabilities inherent in the ongoing use of the Internet for financial transactions and communications. Develop alternatives and redundancies that would increase resilience in times of deterioration or destruction of Internet-based systems.

Long-Term

11. Create an interdependencies analysis system for mapping, visualizing, and analyzing cyber and physical interdependencies. Organizations would provide agreed upon high-level information and legal and liability procedures would be in place. The system may be virtual and should be available to the broad range of key stakeholder organizations under secure access procedures.

12. Develop a secure high-level database to house contributing organizations' information with agreed upon security safeguards and legal provisions regarding unauthorized disclosure of information.

13. Establish an integrated analysis capability (a "tool set" of models and systems) that can be used to assess and provide cost-effective protection and mitigation decisions regarding interdependent infrastructures and organizations for use during preparedness planning, response, and restoration.

14. Develop a regional infrastructure security plan that is centered on interdependencies and comprehensive in focus, including all regional jurisdictions and covering multihazards. This regional plan would incorporate and be synergistic and compatible with existing local and state disaster preparedness and management plans.

15. Provide incentives for key private-sector stakeholders to undertake vulnerability assessments (physical, cyber, and interdependencies focused) and share information, as appropriate.

II. Appreciation of Cyber Threats and Incidents

A. Needs

1. Educational tools and approaches to:
   - » Increase the knowledge of key stakeholder organizations about new and emerging cyber threats and vulnerabilities to operational and business systems, including supervisory control and data acquisition (SCADA) and process control systems;
   - » Address misconceptions about the technical capabilities of computer networks to withstand attacks and recover quickly as well as the challenges of resorting to manual operations;
   - » Enable incident response;
   - » Provide an understanding of the impacts of weapons of mass destruction or electromagnetic pulse (EMP) attacks on information technology systems; and
   - » Prevent or mitigate cyber vulnerabilities and attacks.

2. Ways to share information on cyber threats and incidents for regional cyber incident management.

3. Risk assessment approaches that take into account the virtual and interdependent nature of information technology and communications systems.

4. Development of criteria to determine when to stand up an emergency operations center (EOC) for a cyber attack.

5. Technologies for intrusion detection and protection.

6. Backup and alternative computer and communications capabilities (local, long distance, and wireless) for use during significant disasters.

7. Development of plans to restore electronic and communications systems expeditiously among all communications systems/providers (military, private, or public sector) during a disaster.

8. Information security training for appropriate key stakeholder personnel.

B. Recommended Actions

Short-Term

1. Develop cyber incident threshold criteria for emergency operations center stand-up.

2. Create cyber security and incident response awareness workshops customized for stakeholder personnel, the media, and the general public.

3. Produce a cyber security first aid handbook for government and private-sector organizations that includes information on such basics as data recovery, backup, and systems restoration.

4. Incorporate cyber security challenges into regional and other exercises.

5. Incorporate cyber incident management into collaborative federal, state, and regional incident management procedures.

6. Create a regional cyber security coordination group of key stakeholder chief information security officers (CISOs) and other interested managers to raise awareness of threats, incidents, and challenges; share information; and focus on activities to improve regional cyber resilience.

7. Establish regional and national cyber centers of excellence to share best practices and offer low-cost or no-cost penetration testing, application threat modeling, and security assessments of cyber solutions.

8. Enlist volunteers drawn from or sponsored by cyber security-focused entities who offer their time and expertise to help small organizations or businesses increase their information security operations and awareness.

9. Determine sources for cyber security-related intelligence that can be shared with stakeholders.

10. Establish data backup and off-site storage procedures to minimize issues with respect to cyber or other attacks and to assist in rapid restoration.

Medium-Term

11. Create a cyber regional incident management system that includes means for key stakeholders to communicate electronically during significant disruptions.

12. Develop automated and user-friendly threat modeling and application information security assessment tools.

Long-Term

13. Undertake studies and develop assessment tools to measure the impacts of catastrophic disasters on cyber systems, including electromagnetic pulse attacks or attacks involving weapons of mass destruction.

14. Develop methods and technologies to harden systems to better withstand catastrophic events.

15. Develop tools and systems to better prevent and thwart cyber attacks.

III. Resilient and Interoperable Communications and Information Systems

A. Needs

1. An overall plan for regional communications and critical information technology infrastructure resilience.

2. Interoperability among stakeholder communications and information system and standardized communications systems that link emergency operations centers and individual governmental and private-sector utilities, other key stakeholders, and responders.

3. Contingency plans that include alternate mobile communications, satellite, and other backup systems to ensure redundancy to compensate for outages of phone, cell phone, and e-mail communications that could result in prolonged regional cascading disruptions.

4. A rapid and effective way to quickly reach and inform community organizations, schools, and residents of impending disasters that require either sheltering in place or evacuation-related information.

B. Recommended Actions

Short-Term

1. Develop an inventory and assessment of available backup and alternative communications systems and resources when phone, cell phone, and Internet services are disrupted.

2. Conduct an assessment of regional interoperable communications needs that includes key private-sector and nonprofit organizations.

3. Establish access for interested public and private-sector organizations to the Government Emergency Telephone System (GETS) priority communication system and any other government emergency network, the Wireless Priority Service (WPS), and the Telecommunications Service Priority (TSP) Program.

4. Establish emergency communications contingency plans for public and private-sector organizations that include backup systems to ensure redundancy to deal with outages of phone, cell phone, and Internet service.

5. Develop a structure to reestablish command and control when there is disruption or destruction of communications capabilities.

6. Develop alternative methods of communication, including mobile capabilities and information technology systems that provide greater use of high-speed Internet voice transmissions and data, customer contact, hotline numbers, satellite phones, and text messaging.

7. Identify sources of emergency power generators, investigate extended-life batteries, batteries that are standardized and can be easily changed, and standardized charger connections.

8. Create a mechanism by which to identify and provide low-cost or no-cost technical expertise for telecom/critical information technology infrastructure assessment, disaster preparedness, and management.

9. Devise methods for shipping and transporting essential information technology and communications equipment and supplies during a regional crisis.

10. Develop a plan and procedures for integrating Department of Defense capabilities into communications/critical information technology disaster preparedness/response.

11. Create greater public awareness of interdependencies-related communications and critical information technology vulnerabilities and of what this means for creating the level and extent and duration of self-sufficiency necessary for organizations and communities in a major disaster.

Medium-Term

12. Engage relevant public and private stakeholders to define requirements and develop a regionwide interoperable communications capability for threat, response, and recovery information that includes technical requirements, identifies which organizations should be included and what type of information should be conveyed, and establishes appropriate security procedures governing access and data storage for sensitive information.

13. Undertake a regional needs assessment that includes an inventory of government, private-sector, and other essential primary communication systems—including those used for emergencies—their general vulnerabilities under certain disaster scenarios, mitigation alternatives to address these vulnerabilities, and alternative communications links if disrupted.

14. Establish criteria to be used to identify and prioritize communications/critical information technology infrastructure assets and facilities.

15. Develop a plan for providing situational awareness of regional telecom and critical information technology capabilities during a disaster.

16. Establish procedures for determining flexible prioritization of service restoration, taking interdependencies into account.

17. Establish an automatic emergency response network to access regional residents and community organizations and businesses to alert them via phone or cell phone to major emergency situations.

18. Link key stakeholder emergency operations centers and command centers in a region—including utility emergency operations centers—through a regional, interoperable communications network based on radio and satellite phone systems.

19. Investigate methods to link first responders and local and private-sector emergency operations centers to local radio stations to provide notification of outages, threat information, and general public information when phone lines, networks, and/or e-mail are not available.

20. Establish a schedule to ensure routine testing of existing communications systems and incorporate it into regional and in-house organization exercises.

Long-Term

21. Install, upgrade, and test resilient and interoperable regional communications systems on a regular basis.

22. Develop tools and technologies to foster better communications and critical information technology infrastructure resilience.

IV. Risk Assessment and Mitigation

A. Needs

1. An assessment capability to predict accurate and comprehensive consequences to a full spectrum of threats—including a pandemic—over a wide range of time frames to include the destabilization of various markets and the reestablishment of new forms of business.

2. A metrics-based regional threat assessment approach that examines risk from a systems standpoint and takes multihazards into account.

3. Identification and assessment of existing risk assessment tools that could be customized for regional needs.

4. An inventory of current protection and mitigation measures in use or in the planning stage.

5. Improved ways to identify and prioritize critical assets and facilities.

6. Access to no-cost or low-cost technical expertise for assessment, protection, and mitigation.

7. Detection, monitoring, and sensor systems.

8. Decontamination and cleanup systems.

9. Analysis systems to realistically determine the consequences of disruptions to a region over meaningful scales of scope, gravity, and duration.

B. Recommended Actions

Short-Term

1. Bring together government, private-sector, and other key stakeholders to identify what incentives and liability protection would be most useful to encourage organizations to undertake vulnerability and risk assessments.

2. Establish criteria by which to identify critical assets and facilities within the context of regional needs.

3. Undertake a regional threat assessment.

4. Create regional centers of expertise to provide low-cost or no-cost technical expertise and tie them together virtually to reinforce the sharing of lessons learned and best practices.

Medium-Term

5. Develop a system for quantitatively and qualitatively ranking identified critical assets in terms of risk.

Long-Term

6. Develop a tool set with which to assess damage in terms of economic, environmental, health and public safety, national security, and public confidence impacts.

7. Develop a regional risk-assessment approach that takes into account vulnerabilities, including interdependencies, the nature of the threat (multihazards), and the consequences of disruptions.

V. Cooperation and Coordination

A. Needs

1. Public and private-sector partnerships or similar collaborative mechanisms that include defense installations and facilities focused on regional preparedness, the goal being to share information, gain greater understanding of regional interdependencies, build trust, and effect mutual preparedness planning and project implementation.

2. Coordination of local emergency response and business continuity plans of key stakeholders, including nonprofits and community institutions.

3. Virtual integration of local emergency operations centers in a region or the creation of a regional emergency operations center that includes key stakeholder representatives.

4. Updating and testing of existing formal and informal cooperative agreements or mutual understandings for response and recovery activities, particularly for extreme disasters.

5. Dedicated channels for stakeholders to use to report to government agencies during regional emergencies to prevent inundation by requests for status reports.

6. Facilitation of regional information sharing while protecting data from public release.

7. Provision of threat information to significant utilities and other key organizations prior to an incident or disaster and during response and restoration, including cyber attacks, physical attacks, or those related to weapons of mass destruction.

8. Ways to deal with legal and proprietary barriers to sharing information among public and private-sector organizations.

9. Criteria to be used by commercial organizations in determining when to inform law enforcement agencies of a threat or security incident.

10. Mechanisms and procedures to enable commercial enterprises beyond existing infrastructure sector information sharing and analysis centers (ISACs) to provide threat-related information to the Federal Bureau of Investigation and other relevant agencies.

11. A regional information sharing and analysis center with an alert and warning capability.

12. A resource directory of disaster response/recovery points of contact, including "who does what," that should include logistics and supply components for such crucial items as fuel supply and distribution.

13. Protocols for secure information sharing and nondisclosure agreements.

14. Contingency communication plans.

15. Exercises and targeted drills to test communications systems under emergency conditions.

16. Tabletop and field exercises to test evacuation and sheltering procedures.

17. Development of a regional nuclear/radiological preparedness program that takes interdependencies into account.

18. Development of common terminology to bridge the gap between security, emergency management, and cyber communities.

19. Routine inclusion of private-sector entities with government entities in preparedness-planning activities.

20. Development of Good Samaritan laws and workman's compensation and death benefit laws to facilitate private-sector entities' coordination of and participation with public sector entities in disaster planning, drilling, response, and recovery.

21. Training of first responders and other essential personnel in federal, state/provincial, and local plans and procedures and in the use of such equipment as satellite phones.

22. Inclusion of and training for private-sector entities in government incident-management plans.

23. Involvement of private-sector entities in mutual assistance agreements, including model mechanisms that can protect proprietary information—for example, the creation of a nonprofit organization to shield data from state and local public disclosure laws.

24. Procedures to provide credentials for appropriate private-sector responders, health care workers, and essential personnel who need to travel and gain access to sites during emergencies.

25. The development of sample emergency response contracts for key activities that state/local governments can prenegotiate and set in place in advance of an incident.

26. Inclusion in preparedness plans of communities, institutions, and individuals with special needs—for example, nursing homes, prisons, and people needing respirators or medications.

B. Recommended Actions

Short-Term

1. Create regional public-private partnerships (the scope may be a municipality, other region within, or a single state

[province], multi-state, or cross-national border). Partnerships may focus on infrastructure security, homeland security, or disaster resilience and may serve as a collaboration mechanism and an umbrella for other associations and groups focused on similar missions.

2. Develop prolonged power emergencies workshops that are customized for key stakeholder personnel, the media, and the general public.

3. Conduct a regionwide inventory and assessment of existing physical and cyber disaster/attack preparedness capabilities—for example, mechanisms, plans, procedures, methodologies, approaches, communications systems, sensors, and tools to provide a baseline of what has been done and avoid reinventing the wheel.

4. Adopt nondisclosure agreements to facilitate the sharing of information.

5. Establish procedures for the sharing of information between key stakeholders and local and regional federal law enforcement agencies on threats and other security matters.

6. Develop public disclosure exemptions for use at the regional level.

7. Establish a regional emergency operations center (it may be virtual) staffed with governmental response agencies and commercial service providers.

8. Establish a mechanism—for example, a committee within a regional partnership—to enable emergency management and security personnel to meet with their counterparts in customer service and service provider organizations to share information in a secure environment on continuity of operations and business continuity plans.

9. Establish mutual assistance agreements among jurisdictions, private-sector and public sector organizations, or among civilian and regional defense facilities.

10. Create sector-specific cooperative associations to facilitate coordination for disaster response and provide a focal point for receiving and disseminating information to state and regional emergency operations centers.

11. Include key private-sector stakeholders, nonprofits, and community organizations in exercises and other preparedness-planning activities.

12. Develop, maintain, and share a current list of key stakeholder primary contacts responsible for disaster preparedness and management and state and local emergency operations centers .

13. Develop a list of federal, state, and local agency names to assist in providing points of contact for government resources.

Medium-Term

14. Develop a model charter and governance structure for a regional public-private partnership centered within a nonprofit organization to enable sharing of information with appropriate safeguards.

15. Assess the needs of community institutions and facilities—for example, schools and nursing homes—and of disabled and disadvantaged populations during a large-scale disaster.

16. Government and private-sector organizations develop critical information requirements to determine what information to provide federal and local law enforcement and responder agencies on threats, security incidents, and significant operational interruptions.

Long-Term

17. Develop a multi-year exercise strategy of tabletop and field exercises to test procedures and cooperation and identify gaps and potential corrective actions.

VI. Roles and Responsibilities

A. Needs

1. Improved coordination of command-and-control-related issues in a regional disaster (federal, civilian, defense, state, local agencies, private-sector, and nonprofits).

2. Collective stakeholder review of federal, state/provincial, and local preparedness plans, including incident management procedures to provide awareness and additional clarity on regional roles and responsibilities of government (civilian and defense) and private-sector entities during a regional disaster.

3. Clarification and information on how federal agencies will interact with regional and local authorities and private-sector organizations and how decisions will be made.

4. Integration of federal defense assets in regional preparedness planning, both pre- and post-event.

5. Information on how federal defense assets will support and interact with civilian government and private-sector organizations in a catastrophic situation in which these assets could be required.

6. Better understanding of lines of authority among federal and local government law enforcement entities.

B. Recommended Actions

Short-Term

1. Conduct workshops on regional incident management (physical and cyber).

2. Create a working group of key stakeholder representatives to delineate roles and responsibilities of government authorities at all levels and also of private-sector stakeholders.

3. Provide guidelines for law enforcement and private-sector interaction on crisis and consequence management.

Medium-Term

4. Develop, where necessary, memorandums of understanding, mutual assistance pacts, and other cooperative agreements that involve both public and private organizations to address roles and responsibilities issues.

5. Incorporate drills to explore roles, responsibilities, and challenges and include all key public and private-sector stakeholders, including relevant federal agencies, components of those agencies, and federal defense agencies—for example, the U.S. Northern Command—into a regional exercise program.

6. Incorporate information and procedures that address roles and responsibilities into preparedness plans.

Long-Term

7. Continue regional and targeted exercises and drills (including field exercises) and incorporate lessons learned into incident management planning.

VII. Response Challenges

A. Needs

1. Procedures on how and when a virtual emergency operations center would be established that would call upon the resources of local federal agencies and also include Department of Defense installations, state and county entities, major municipalities, and the command centers and emergency operations centers of other key public and private organizations.

2. Realistic evacuation procedures that take interdependencies into account. Such plans should provide for housing large numbers of displaced persons as well as people with special needs, including tribal, nursing home, and prison populations.

3. Plans for dealing with large numbers of abandoned vehicles and debris removal to enable emergency response.

4. A strategy for dealing with a large number of casualties that exceeds the surge capacity of hospitals.

5. Means to ensure that utilities and other essential service providers (banks and other financial institutions, hospitals, etc.) can bring in staff or use incentives to discourage personnel from abandoning their jobs to be with their families, including provisions to shelter individuals who could not return to their homes.

6. Determination of what role media should play in response.

7. A certification process to enable emergency medical, utility maintenance, and key stakeholder essential personnel to have access to buildings and pass through roadblocks.

8. The need to ensure the delivery of products, social security checks, customer payments, etc., particularly for small businesses and individuals.

9. The need for schools to provide safe shelter during a disaster response.

10. Mortuary facilities for casualties.

11. Means of dealing with civil unrest when law enforcement is stretched thin or unavailable.

B. Recommended Actions

Short-Term

1. Develop a practical and effective credentialing process that includes input from county and municipal officials, private-sector organizations, and other key stakeholder organizations. This process must also be coordinated with neighboring states and, if appropriate, across national borders.

2. Work with local media to determine how to best utilize their resources for disaster response. Include local media in exercises.

3. Work with the U.S. Postal Service and private-sector logistics, shipping, and delivery services to ensure uninterrupted delivery of products, social security checks, customer payments, etc. and to train their employees to help ascertain the presence and welfare of residents.

Medium-Term

4. Identify the resources local businesses have available to sustain first responders (food, restroom facilities, and such equipment as blankets, tools, and flashlights).

5. Coordinate with local federal agencies—including Department of Defense installations and their mobilization personnel—to identify resources and the availability of materials and supplies that could be accessed through the appropriate tasking authorities.

6. Identify the location of ports and marine/naval services and investigate their ability to assist in response efforts.

7. Identify staging areas and transportation routes for disaster management and assess them for potential interdependencies-related vulnerabilities.

8. Develop a plan to ensure that schools are operational as quickly as possible, and designate them in advance as potential shelters with stockpiled supplies.

9. Develop with local law enforcement, the Federal Bureau of Investigation, and the National Guard a contingency plan to deal with civil unrest when police resources are limited.

Long-Term

10. Develop and conduct regional exercises and targeted drills with a range of stakeholders—including the media and community groups—to test and further improve response plans.

VIII. Recovery and Restoration

A. Needs

1. An integrated regional resource management plan for recovery and restoration in large-scale disasters—including significant cyber incidents—that explains how essential government (civilian and defense) and private-sector and nonprofit personnel, equipment, and other resources could be accessed and secured quickly without significant impediments caused by interdependent infrastructures.

2. A database of available resources that includes means for effective communication among all key stakeholder organizations to enable expeditious coordination, prioritization, and reallocation of resources to meet changing circumstances.

3. Memorandums of understanding between regional stakeholders and with and between states on resources to be supplied, under what conditions, and how reimbursement will be handled.

4. Methods of raising awareness of the availability of federal, state, and local government resources as well as resources within the private-sector and nonprofit arenas that would be available in the event of a regional disaster.

5. A means to promote understanding by private-sector organizations as to how disaster response resources and/or reimbursements are requested and allocated.

6. Ways to circumvent procedural, bureaucratic, and political impediments to achieve expeditious availability of adequate critical resources and procedures for prioritized access to emergency backup equipment and critical components.

7. Assurance of adequate stockpiles of fuel, generators, medical supplies, and sustenance, as well as waste management procedures for hospitals, elder care facilities, schools, etc., to meet needs in an unexpected regional disruption lasting more than a few days.

8. Plans for temporary and longer-term housing and other provisions for displaced persons. These plans should take into account the impact on cities and localities that must accommodate a large influx of displaced individuals.

9. Integration of charitable and other nonprofit institutions providing essential services and supplies in resource management plans.

10. Strategies and procedures to deal with volunteers and unsolicited donations.

B. Recommended Actions

Short-Term

1. Conduct an inventory of federal, state, and local government, private-sector, and nonprofit resources that could be utilized in different types of disasters/disruptions.

2. Study pre- and postevent needs, including restoration/recovery from potential extreme disaster scenarios.

3. Assess the resources and capabilities of research organizations to provide information and training on threats and vulnerabilities (including supervisory control and data acquisition and process control system vulnerabilities), weapons of mass destruction, and resources required to deal with various types of natural and man-made disasters.

4. Create a template for local governments to use to inventory available critical resources necessary during a major disaster and create a resources database for use in preparedness planning and emergencies.

Medium-Term

5. Create a disaster management resource inventory/database with analytic capabilities of public and private-sector resources available for response and recovery, including technical subject matter experts, manpower, vehicles, food, water/ice, pharmaceutical supplies, temporary housing, equipment, services, and points of contact information.

6. Establish and implement a plan to identify and stockpile—or provide procedures for access to—electric power generators, other emergency backup equipment, and supplies.

7. Call for assessments by local jurisdictions and organizations of established inventories of supplies in schools, hospitals, nursing homes, other community facilities, and prisons to ascertain what additional resources would be needed for regional disasters.

8. Create a list of federal civilian and federal defense resources that are accessible to public and private-sector organizations for response and recovery.

9. Assess the capacity of nonprofits and other groups to provide assistance in a major disaster.

10. Create a template for a regional disaster restoration plan for use by businesses, nonprofits, and public sector organizations.

11. Survey local government agencies, regional utilities, other key service providers, and commercial enterprises to determine expected equipment and personnel availability and needs in a significant prolonged regional disruption.

Long-Term

12. Establish a regional mechanism to act as the focal point for coordinating response to regional disasters that is empowered to direct actions associated with resource allocation and management.

13. Undertake an assessment of federal, state, and local laws, rules, regulations, and procedures that impede recovery and restoration, including a cost-benefit analysis of how these constraints could be reduced and, if warranted, eliminated.

IX. Business Continuity and Continuity of Operations

A. Needs

1. Vulnerability assessments (physical and cyber).

2. Model continuity of operations and business continuity plans for small- and medium-sized organizations.

3. Exercises and drills.

4. Understanding of supply chain vulnerabilities.

5. Model plans for small and medium enterprises and organizations.

6. Cost-effective backup and redundant systems and remote data storage.

B. Recommended Actions

Short-Term

1. Conduct a continuity of operations workshop for small and medium-sized organizations that includes interdependencies and links interdependent organizations.

2. Create templates for in-house exercises—including interdependencies tabletops—and for participation in external exercises with other organizations.

Medium-Term

3. Establish methodologies and approaches for vulnerability assessments.

4. Create model business continuity and continuity of operations plans.

Long-Term

5. Incorporate interdependencies—including those of supply chains and customers' supply chains—into existing preparedness plans.

X. Logistics and Supply Chain Management

A. Needs

1. Means to better understand and analyze supply chain vulnerabilities and disruption impacts and how interdependencies and supply chain gaps relate to sustainable resiliency for organizations and citizens in a major disaster.

2. Cost-effective security and mitigation measures.

3. Methods to ensure supply chains and just-in-time deliveries.

4. A model contingency plan for supply chain disruptions. Organizations should identify critical suppliers, products, and materials.

5. Cooperative arrangements for use with key suppliers and customers that enable assessment of cost-effective security and resiliency needs for supply chains.

6. A management strategy to ensure the availability of and access to critical equipment, materials, components, and products, including those from offshore sources.

B. Recommended Actions

Short-Term

1. Create a template to use to identify critical suppliers, products, and materials.

2. Devise methods by which to identify organizational risks and analyze gaps.

Medium-Term

3. Develop a management strategy to ensure the availability of and access to critical equipment, materials, components, and products, including those from off-shore sources.

4. Develop contingency plans for commercial organizations addressing supply chain disruptions.

5. Create a benchmark standard based on risk and gap analysis for "lean" security and resilience that would be employed by other organizations in the supply chain system.

6. Share information on confidentiality and legal constraints on collaboration with other supply chain organizations and on ways to address these issues to foster necessary cooperation.

7. Establish means to educate key suppliers on interdependencies and to conduct on-site "total system" assessments that include particular focus on critical services (water, energy, etc.) and that establish high-order priorities for risk reduction and overall security.

Long-Term

8. Establish processes and tools to identify and assess supply chain vulnerabilities/interdependencies and disruption impacts.

9. Develop risk assessment and decision support systems to determine optimal mitigation measures.

10. Establish a model process to establish continuous improvement through benchmarking and economic valuation metrics.

XI. Public Information/Risk Communications

A. Needs

1. A public information and education strategy that enables the general public and the media to receive necessary, accurate, and coordinated information during a major regional disaster, (including major cyber incidents) and provides the public with timely and accurate information without inciting panic.

2. Recognition of the media as critical infrastructure and as first responders.

3. Inclusion of the media as well as public and private-sector public information officers in regional preparedness planning in a way that enables key stakeholders to achieve a comfort level in dealing with the media on regional emergencies.

4. A vulnerability assessment of the emergency warning and communications systems to ensure that they are fully reliable in the event of a regional disaster.

5. A public regional risk communication plan that involves key stakeholders within both the public and private-sectors and establishes a central coordination and information dissemination point of contact.

6. A strategy to encourage and maintain civil order if critical infrastructure services are disrupted and the risk of civil disorder escalates.

7. Risk education at K–12 grade levels.

B. Recommended Actions

Short-Term

1. Develop a public information strategy to coordinate dissemination of information during a regional crisis.

2. Develop, with selected media, a set of guidelines on how to best utilize the media in large-scale disasters.

3. Include selected media representatives in regional preparedness planning, exercises, and training, as necessary.

4. Create a guide for media on critical infrastructure interdependencies, cyber security challenges, and attacks involving weapons of mass destruction (nuclear, radiological, biological, and chemical attacks) to help them understand the issues.

5. Refine procedures to provide public service announcements and develop alternate and redundant ways to inform the public during a regional disaster.

6. Create a short list of trusted experts to provide expertise to the media.

7. Provide training for key stakeholder employees on dealing with the media.

8. Provide training for law enforcement personnel on how to deal with civil unrest and panic situations.

Medium-Term

9. Create a risk communication toolbox that includes guidelines, procedures, a glossary of common terms, and other information to facilitate the effective communication of pertinent, multihazards disaster-related information to the public and the media.

10. Create a regional joint information center associated with a regional emergency operations center that includes public affairs officers of all major public and private-sector stakeholder organizations.

Long-Term

11. Develop a dynamic web-based system to enable key stakeholder personnel to obtain accurate information from experts on infrastructure security and general preparedness issues.

XII. Exercises, Training, and Education

A. Needs

1. An effective multi-year program of tabletop and field exercises that has a regional focus, involves all key stakeholders and selected media, and does not overburden local organizations.

2. Education for stakeholders, the media, and legislators on the following:
   - Awareness of impacts of long-term power outages and rolling blackouts;
   - Regional infrastructure interdependencies and their impacts on regional disasters;
   - Cyber threats and disruptions;
   - Pandemic and other biosecurity threats;
   - The impacts of, response to, and recovery from attacks involving weapons of mass destruction; and
   - Other extreme disaster preparedness/response/recovery issues.

B. Recommended Actions:

Short-Term

1. Develop tools for educating public officials and citizens on local disaster preparedness and management plans and challenges—for example, specialized publications, exhibit booths set up outside public meetings to disseminate public information, etc.

2. Create a public-private exercise planning committee to develop a coordinated multiyear plan of tabletop and field exercises that avoids duplication of effort.

3. Develop training courses for the public, the media, and interested staff of key stakeholders on the impacts of long-term power outages and rolling blackouts; regional infrastructure interdependencies and their impacts on regional disasters; and cyber threats and disruptions.

4. Develop training courses for the public, the media, and interested staff of key stakeholders on the impacts of, response to, and recovery from weapons of mass destruction.

5. Produce a web-based calendar of disaster resilience/homeland security-related events to provide a heads-up to stakeholders on training opportunities and to coordinate event schedules.

Medium-Term

6. Develop a program of public-private regional and targeted exercises to further illuminate interdependencies and related preparedness shortfalls and other challenges, demonstrate new procedures, and test progress made on the implementation of an action plan for regional disaster resilience.

Long-Term

7. Continue the disaster resilience "life-cycle" of improvements, exercises, lessons learned, etc.

Using the Guide to Develop A Regional Action Plan

The overall framework, projects, and activities identified in this guide are designed to enable public and private stakeholders to develop an action plan that provides a general, dynamic strategy customized to specific regional and organizational needs. This process involves prioritizing selected projects and activities, determining the requirements for each, and devising means to best accomplish their cost-effective implementation within the shortest time frame.

The prerequisite is for interested local, state, and private-sector leaders to jointly reach out to key stakeholders to work together toward regional disaster resilience. Some municipalities, counties, and states have already set up such cross-sector collaborative mechanisms and are starting down the road toward a comprehensive regional preparedness strategy. Several of these regions have already developed official partnerships, and many others have various collaborative mechanisms in place that were created by private-sector or nonprofit organizations. The important requirement is that there be an umbrella partnership that can encompass the wide range of key stakeholders to provide the level of coordination and cooperation necessary to focus regional disaster resilience efforts.

One model for creating such an umbrella regional partnership is outlined below. This process, which can be accomplished within 7 to 12 months, may be customized to suit specific stakeholder needs. It is designed to enable regions to include existing collaborative arrangements and initiatives and leverage already existing best practices and solutions. Once completed, it also provides a test bed to use to undertake activities with support from federal agencies and other sources.

Seven-Step Action Plan Process

Step 1 ***Create a formal or informal regional cooperative initiative or partnership composed of key stakeholders, ideally including the leadership of senior local/state and private-sector organizations.*** This core group, typically 30 to 45 organizations that will become the de facto steering committee of the partnership, should represent major utilities; key local, state, and regional government organizations, including defense installations; businesses; nonprofits; and such academic and community institutions as schools and hospitals. Associations that represent broad organizational memberships should also be invited to participate. For those regions with existing collaborative mechanisms, it is important to ensure that all key stakeholders are represented.

Step 2 ***Develop and conduct an interactive, educational workshop to provide necessary information to key stakeholders on regional infrastructure interdependencies and disaster preparedness and security challenges.*** The number of attendees may range from 100 to 200 representatives of regional public/private-sector organizations. A primary goal of this workshop is to develop an understanding of regional interdependencies and establish a framework of trust and collaboration to advance regional preparedness and response as well as an understanding of regional hazards and threats.

Step 3 ***Develop and conduct a regional infrastructure interdependencies exercise that includes a scenario designed by members of the core stakeholder group and other interested organizations to reflect their interests and concerns regarding a major disaster.*** The objectives of the exercise are not to test plans or procedures but to provide stakeholders with an awareness of baseline regional interdependencies and associated physical and cyber vulnerabilities, to identify preparedness gaps, and to devise useful solutions. Participants in the exercise will include attendees from the workshop described above in step two as well as representatives of federal departments (civilian and defense) who are involved in disaster response and recovery.

Step 4 ***Produce a report based on the lessons learned from the exercise that includes findings and recommendations that have been coordinated with/validated by the key stakeholders.***

Step 5 ***Develop and conduct an action planning workshop with the exercise participants to prioritize and build upon the recommended activities in the exercise report and identify specific projects.***

Step 6 ***Produce an action plan composed of these prioritized projects, using the framework provided in this guide, and coordinate it with the key stakeholders.*** These action plan activities should be incorporated into regional and organizational preparedness strategies and plans.

Step 7 ***Create working groups within the regional partnership—including lead government agencies and private-sector organizations—to undertake those short-, medium-, and long-term activities in the action plan that require a cross-sector cooperative approach.*** These working groups will be responsible for developing requirements to address project oversight, management, and funding issues.

Implementation Challenges

The action plan developed should be envisioned as an ongoing process toward regional disaster resilience. The plan will evolve as regional stakeholders' general knowledge of how to better approach comprehensive disaster preparedness also evolves.

It is important that this guide be considered just that—a roadmap for state and local governments and other regional stakeholders to customize for their use and not a mandatory standard. Stakeholders will determine how they want to approach public/private-sector collaboration and—on the basis of perceived risk, available resources, and incentives—which activities are desirable for their respective action plans. Citizens will need to determine to what extent they are willing to underwrite improvements through utility rate hikes or increased local taxes.

Maintaining the Momentum: The Essential Role of Regional Partnerships.
Developing a disaster-resilient region is a difficult task, made all the more daunting by limited understanding of infrastructure interdependencies and the current dearth of analytic capabilities to assess associated vulnerabilities and disruption impacts and perform necessary risk assessment. The absence of hard data on risk and where to direct resources, however, should not impede localities, states, private enterprises, and other organizations from cooperatively undertaking the activities in this plan, many of which fall into the "low-hanging fruit" category.

What is most important is establishing working regional public-private partnerships to assist in identifying preparedness shortfalls, validating and prioritizing the activities selected for implementation, and undertaking individual and collaborative solutions to address these gaps. Also essential is the need to create, within regional partnerships, governance structures that can enable the secure sharing of information and methods to engage multiple organizations in project development and to pool resources from various organizations while avoiding conflicts of interest. This will require the flexibility and willingness of local and state governments to give partnership members a say in regional planning, implementation, and funding decisions.

Importance of Top Down/Bottom Up Leadership

Critical to the success of efforts to achieve disaster resilience is the federal government, which will need to provide the encouragement, technical expertise, seed money, and in certain cases, substantial investment through new and existing mechanisms for many of the activities in the action plan. One challenge will be determining how to best develop the organizational structures and programs to do this that can supplement traditional state and local funding mechanisms. Few models exist that enable federal dollars to be provided to regional entities—hence the importance of establishing nonprofit status for regional partnerships to allow for the provision of grants for regional preparedness enhancements.

The greatest challenge at the grassroots level will be maintaining the momentum needed to move forward with the action plan toward regional disaster resilience. Local governments and other organizations will need to take a leadership role in implementing the action plan activities and make a vigorous effort to retain and expand stakeholder interest and involvement.

Maintaining momentum will require ongoing effort. Most public and private stakeholders hold professionally demanding positions and for the most part engage in preparedness activities on a volunteer basis. This means that progress toward disaster resilience will ultimately depend on the willingness of key regional stakeholders to move forward on cooperative planning and implementation and to set up the collaborative mechanisms required to ensure disaster resilience.

List of Acronyms

ASCE	American Society of Civil Engineers
CISO	Chief Information Security Officers
CONOPS	Concept of Operations
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
EMP	Electromagnetic Pulse
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telephone System
ISAC	Information Sharing and Analysis Center
ISBE	Infrastructure Security for the Built Environment
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCRCG	National Cyber Response Coordination Group
NORTHCOM	U.S. Northern Command
NRP	National Response Plan
POC	Point of Contact
SCADA	Supervisory Control and Data Acquisition
TISP	The Infrastructure Security Partnership
TSP	Telecommunications Service Priority Program
WMD	Weapons of Mass Destruction
WPS	Wireless Priority Service

APPENDIX A

SUMMARY OF RECOMMENDATIONS

SHORT-TERM

1. Develop an infrastructure interdependencies template for use by stakeholder organizations to enable mapping physical and cyber linkages on a regional basis.

2. Develop a secure database for high-level information provided by stakeholders that includes mutually agreed upon security and information protection safeguards.

3. Compile a list—including point of contact (POC) information—of public and private organizations in the region that have similar interdependencies programs under way.

4. Conduct a regional infrastructure interdependencies tabletop exercise to provide initial baseline knowledge for regional stakeholders, explore particular interconnections in more depth, and test preparedness improvements.

5. Develop a web-based lessons-learned database to capture and share interdependencies-related knowledge from exercises and training conducted in various regions.

6. Develop cyber incident threshold criteria for emergency operations center stand-up.

7. Create cyber security and incident response awareness workshops customized for stakeholder personnel, the media, and the general public.

8. Produce a cyber security first aid handbook for government and private-sector organizations that includes information on such basics as data recovery, backup, and systems restoration.

9. Incorporate cyber security challenges into regional and other exercises.

10. Incorporate cyber incident management into collaborative federal, state, and regional incident management procedures.

11. Create a regional cyber security coordination group of key stakeholder chief information security officers (CISOs) and other interested managers to raise awareness of threats, incidents, and challenges; share information; and focus on activities to improve regional cyber resilience.

12. Establish regional and national cyber centers of excellence to share best practices and offer low-cost or no-cost penetration testing, application threat modeling, and security assessments of cyber solutions.

13. Enlist volunteers drawn from or sponsored by cyber security-focused entities who offer their time and expertise to help small organizations or businesses increase their information security operations and awareness.

14. Determine sources for cyber security-related intelligence that can be shared with stakeholders.

15. Establish data backup and off-site storage procedures to minimize issues with respect to cyber or other attacks and to assist in rapid restoration.

16. Develop an inventory and assessment of available backup and alternative communications systems and resources when phone, cell phone, and Internet services are disrupted.

17. Conduct an assessment of regional interoperable communications needs that includes key private-sector and nonprofit organizations.

18. Establish access for interested public and private-sector organizations to the Government Emergency Telephone System (GETS) priority communication system and any other government emergency network, the Wireless Priority Service (WPS), and the Telecommunications Service Priority (TSP) Program.

19. Establish emergency communications contingency plans for public and private-sector organizations that include backup systems to ensure redundancy to deal with outages of phone, cell phone, and Internet service.

20. Develop a structure to reestablish command and control when there is disruption or destruction of communications capabilities.

21. Develop alternative methods of communication, including mobile capabilities and information technology systems that provide greater use of high-speed Internet voice transmissions and data, customer contact, hotline numbers, satellite phones, and text messaging.

22. Identify sources of emergency power generators, investigate extended-life batteries, batteries that are standardized and can be easily changed, and standardized charger connections.

23. Create a mechanism by which to identify and provide low-cost or no-cost technical expertise for telecom/critical information technology infrastructure assessment, disaster preparedness, and management.

24. Devise methods for shipping and transporting essential information technology and communications equipment and supplies during a regional crisis.

25. Develop a plan and procedures for integrating Department of Defense capabilities into communications/critical information technology disaster preparedness/response.

26. Create greater public awareness of interdependencies-related communications and critical information technology vulnerabilities and of what this means for creating the level and extent and duration of self-sufficiency necessary for organizations and communities in a major disaster.

27. Bring together government, private-sector, and other key stakeholders to identify what incentives and liability protection would be most useful to encourage organizations to undertake vulnerability and risk assessments.

28. Establish criteria by which to identify critical assets and facilities within the context of regional needs.

29. Undertake a regional threat assessment.

30. Create regional centers of expertise to provide low-cost or no-cost technical expertise and tie them together virtually to reinforce the sharing of lessons learned and best practices.

31. Create regional public-private partnerships (the scope may be a municipality, other region within, or a single state [province], multi-state, or cross-national border). Partnerships may focus on infrastructure security, homeland security, or disaster resilience and may serve as a collaboration mechanism and an umbrella for other associations and groups focused on similar missions.

32. Develop prolonged power emergencies workshops that are customized for key stakeholder personnel, the media, and the general public.

33. Conduct a regionwide inventory and assessment of existing physical and cyber disaster/attack preparedness capabilities—for example, mechanisms, plans, procedures, methodologies, approaches, communications systems, sensors, and tools to provide a baseline of what has been done and avoid reinventing the wheel.

34. Adopt nondisclosure agreements to facilitate the sharing of information.

35. Establish procedures for the sharing of information between key stakeholders and local and regional federal law enforcement agencies on threats and other security matters.

36. Develop public disclosure exemptions for use at the regional level.

37. Establish a regional emergency operations center (it may be virtual) staffed with governmental response agencies and commercial service providers.

38. Establish a mechanism—for example, a committee within a regional partnership—to enable emergency management and security personnel to meet with their counterparts in customer service and service provider organizations to share information in a secure environment on continuity of operations and business continuity plans.

39. Establish mutual assistance agreements among jurisdictions, private-sector and public sector organizations, or among civilian and regional defense facilities.

40. Create sector-specific cooperative associations to facilitate coordination for disaster response and provide a focal point for receiving and disseminating information to state and regional emergency operations centers.

41. Include key private-sector stakeholders, nonprofits, and community organizations in exercises and other preparedness-planning activities.

42. Develop, maintain, and share a current list of key stakeholder primary contacts responsible for disaster preparedness and management and state and local emergency operations centers .

43. Develop a list of federal, state, and local agency names to assist in providing points of contact for government resources.

44. Conduct workshops on regional incident management (physical and cyber).

45. Create a working group of key stakeholder representatives to delineate roles and responsibilities of government authorities at all levels and also of private-sector stakeholders.

46. Provide guidelines for law enforcement and private-sector interaction on crisis and consequence management.

47. Develop a practical and effective credentialing process that includes input from county and municipal officials, private-sector organizations, and other key stakeholder organizations. This process must also be coordinated with neighboring states and, if appropriate, across national borders.

48. Work with local media to determine how to best utilize their resources for disaster response. Include local media in exercises.

49. Work with the U.S. Postal Service and private-sector logistics, shipping, and delivery services to ensure uninterrupted delivery of products, social security checks, customer payments, etc. and to train their employees to help ascertain the presence and welfare of residents.

50. Conduct an inventory of federal, state, and local government, private-sector, and nonprofit resources that could be utilized in different types of disasters/disruptions.

51. Study pre- and post-event needs, including restoration/recovery from potential extreme disaster scenarios.

52. Assess the resources and capabilities of research organizations to provide information and training on threats and vulnerabilities (including supervisory control and data acquisition and process control system vulnerabilities), weapons of mass destruction, and resources required to deal with various types of natural and man-made disasters.

53. Create a template for local governments to use to inventory available critical resources necessary during a major disaster and create a resources database for use in preparedness planning and emergencies.

54. Conduct a continuity of operations workshop for small and medium-sized organizations that includes interdependencies and links interdependent organizations.

55. Create templates for in-house exercises—including interdependencies tabletops—and for participation in external exercises with other organizations.

56. Create a template to use to identify critical suppliers, products, and materials.

57. Devise methods by which to identify organizational risks and analyze gaps.

58. Develop a public information strategy to coordinate dissemination of information during a regional crisis.

59. Develop, with selected media, a set of guidelines on how to best utilize the media in large-scale disasters.

60. Include selected media representatives in regional preparedness planning, exercises, and training, as necessary.

61. Create a guide for media on critical infrastructure interdependencies, cyber security challenges, and attacks involving weapons of mass destruction (nuclear, radiological, biological, and chemical attacks) to help them understand the issues.

62. Refine procedures to provide public service announcements and develop alternate and redundant ways to inform the public during a regional disaster.

63. Create a short list of trusted experts to provide expertise to the media.

64. Provide training for key stakeholder employees on dealing with the media.

65. Provide training for law enforcement personnel on how to deal with civil unrest and panic situations.

66. Develop tools for educating public officials and citizens on local disaster preparedness and management plans and challenges—for example, specialized publications, exhibit booths set up outside public meetings to disseminate public information, etc.

67. Create a public-private exercise planning committee to develop a coordinated multiyear plan of tabletop and field exercises that avoids duplication of effort.

68. Develop training courses for the public, the media, and interested staff of key stakeholders on the impacts of long-term power outages and rolling blackouts; regional infrastructure interdependencies and their impacts on regional disasters; and cyber threats and disruptions.

69. Develop training courses for the public, the media, and interested staff of key stakeholders on the impacts of, response to, and recovery from weapons of mass destruction.

70. Produce a web-based calendar of disaster resilience/homeland security-related events to provide a heads-up to stakeholders on training opportunities and to coordinate event schedules.

MEDIUM-TERM

1. Revise and improve existing preparedness and disaster management plans to address interdependencies, including those focused on nuclear/radiological, biological, and chemical incidents. Provide a strong focus on concepts of operations (CONOPS).

2. Examine evacuation and sheltering or shelter-in-place plans to ensure that they are realistic, taking into account facilities' limitations and regional interdependencies and using extreme disaster scenarios as baselines; revise plans to meet existing realities; and identify and implement preparedness activities, mitigation measures, and resource strategies necessary to achieve optimal evacuation and shelter procedures, revising plans accordingly.

3. Identify the economic and health and human safety ramifications of various security measures that may be put in place during a disruption or attack—for example, closing ports, interstates, tunnels, airports, bridges, or borders—to assess how these activities could complicate or facilitate response and recovery activities.

4. Develop a program addressing ongoing regional and targeted infrastructure interdependencies tabletop and field exercises to explore particular interconnections in greater depth and to test preparedness improvements.

5. Create incentives for academic studies to assess and understand worldwide interdependencies and vulnerabilities inherent in the ongoing use of the Internet for financial transactions and communications. Develop alternatives and redundancies that would increase resilience in times of deterioration or destruction of Internet-based systems.

6. Create a cyber regional incident management system that includes means for key stakeholders to communicate electronically during significant disruptions.

7. Develop automated and user-friendly threat modeling and application information security assessment tools.

8. Engage relevant public and private stakeholders to define requirements and develop a regionwide interoperable communications capability for threat, response, and recovery information that includes technical requirements, identifies which organizations should be included and what type of information should be conveyed, and establishes appropriate security procedures governing access and data storage for sensitive information.

9. Undertake a regional needs assessment that includes an inventory of government, private-sector, and other essential primary communication systems—including those used for emergencies—their general vulnerabilities under certain disaster scenarios, mitigation alternatives to address these vulnerabilities, and alternative communications links if disrupted.

10. Establish criteria to be used to identify and prioritize communications/critical information technology infrastructure assets and facilities.

11. Develop a plan for providing situational awareness of regional telecom and critical information technology capabilities during a disaster.

12. Establish procedures for determining flexible prioritization of service restoration, taking interdependencies into account.

13. Establish an automatic emergency response network to access regional residents and community organizations and businesses to alert them via phone or cell phone to major emergency situations.

14. Link key stakeholder emergency operations centers and command centers in a region—including utility emergency operations centers—through a regional, interoperable communications network based on radio and satellite phone systems.

15. Investigate methods to link first responders and local and private-sector emergency operations centers to local radio stations to provide notification of outages, threat information, and general public information when phone lines, networks, and/or e-mail are not available.

16. Establish a schedule to ensure routine testing of existing communications systems and incorporate it into regional and in-house organization exercises.

17. Develop a system for quantitatively and qualitatively ranking identified critical assets in terms of risk.

18. Develop a model charter and governance structure for a regional public-private partnership centered within a nonprofit organization to enable sharing of information with appropriate safeguards.

19. Assess the needs of community institutions and facilities—for example, schools and nursing homes—and of disabled and disadvantaged populations during a large-scale disaster.

20. Government and private-sector organizations develop critical information requirements to determine what information to provide federal and local law enforcement and responder agencies on threats, security incidents, and significant operational interruptions.

21. Develop, where necessary, memorandums of understanding, mutual assistance pacts, and other cooperative agreements that involve both public and private organizations to address roles and responsibilities issues.

22. Incorporate drills to explore roles, responsibilities, and challenges and include all key public and private-sector stakeholders, including relevant federal agencies, components of those agencies, and federal defense agencies—for example, the U.S. Northern Command—into a regional exercise program.

23. Incorporate information and procedures that address roles and responsibilities into preparedness plans.

24. Identify the resources local businesses have available to sustain first responders (food, restroom facilities, and such equipment as blankets, tools, and flashlights).

25. Coordinate with local federal agencies—including Department of Defense installations and their mobilization personnel—to identify resources and the availability of materials and supplies that could be accessed through the appropriate tasking authorities.

26. Identify the location of ports and marine/naval services and investigate their ability to assist in response efforts.

27. Identify staging areas and transportation routes for disaster management and assess them for potential interdependencies-related vulnerabilities.

28. Develop a plan to ensure that schools are operational as quickly as possible, and designate them in advance as potential shelters with stockpiled supplies.

29. Develop with local law enforcement, the Federal Bureau of Investigation, and the National Guard a contingency plan to deal with civil unrest when police resources are limited.

30. Create a disaster management resource inventory/database with analytic capabilities of public and private-sector resources available for response and recovery, including technical subject matter experts, manpower, vehicles, food, water/ice, pharmaceutical supplies, temporary housing, equipment, services, and points of contact information.

31. Establish and implement a plan to identify and stockpile—or provide procedures for access to—electric power generators, other emergency backup equipment, and supplies.

32. Call for assessments by local jurisdictions and organizations of established inventories of supplies in schools, hospitals, nursing homes, other community facilities, and prisons to ascertain what additional resources would be needed for regional disasters.

33. Create a list of federal civilian and federal defense resources that are accessible to public and private-sector organizations for response and recovery.

34. Assess the capacity of nonprofits and other groups to provide assistance in a major disaster.

35. Create a template for a regional disaster restoration plan for use by businesses, nonprofits, and public sector organizations.

36. Survey local government agencies, regional utilities, other key service providers, and commercial enterprises to determine expected equipment and personnel availability and needs in a significant prolonged regional disruption.

37. Establish methodologies and approaches for vulnerability assessments.

38. Create model business continuity and continuity of operations plans.

39. Develop a management strategy to ensure the availability of and access to critical equipment, materials, components, and products, including those from off-shore sources.

40. Develop contingency plans for commercial organizations addressing supply chain disruptions.

41. Create a benchmark standard based on risk and gap analysis for "lean" security and resilience that would be employed by other organizations in the supply chain system.

42. Share information on confidentiality and legal constraints on collaboration with other supply chain organizations and on ways to address these issues to foster necessary cooperation.

43. Establish means to educate key suppliers on interdependencies and to conduct on-site "total system" assessments that include particular focus on critical services (water, energy, etc.) and that establish high-order priorities for risk reduction and overall security.

44. Create a risk communication toolbox that includes guidelines, procedures, a glossary of common terms, and other information to facilitate the effective communication of pertinent, multihazards disaster-related information to the public and the media.

45. Create a regional joint information center associated with a regional emergency operations center that includes public affairs officers of all major public and private-sector stakeholder organizations.

46. Develop a program of public-private regional and targeted exercises to further illuminate interdependencies and related preparedness shortfalls and other challenges, demonstrate new procedures, and test progress made on the implementation of an action plan for regional disaster resilience.

LONG-TERM

1. Create an interdependencies analysis system for mapping, visualizing, and analyzing cyber and physical interdependencies. Organizations would provide agreed upon high-level information and legal and liability procedures would be in place. The system may be virtual and should be available to the broad range of key stakeholder organizations under secure access procedures.

2. Develop a secure high-level database to house contributing organizations' information with agreed upon security safeguards and legal provisions regarding unauthorized disclosure of information.

3. Establish an integrated analysis capability (a "tool set" of models and systems) that can be used to assess and provide cost-effective protection and mitigation decisions regarding interdependent infrastructures and organizations for use during preparedness planning, response, and restoration.

4. Develop a regional infrastructure security plan that is centered on interdependencies and comprehensive in focus, including all regional jurisdictions and covering multihazards. This regional plan would incorporate and be synergistic and compatible with existing local and state disaster preparedness and management plans.

5. Provide incentives for key private-sector stakeholders to undertake vulnerability assessments (physical, cyber, and interdependencies focused) and share information, as appropriate.

6. Undertake studies and develop assessment tools to measure the impacts of catastrophic disasters on cyber systems, including electromagnetic pulse attacks or attacks involving weapons of mass destruction.

7. Develop methods and technologies to harden systems to better withstand catastrophic events.

8. Develop tools and systems to better prevent and thwart cyber attacks.

9. Install, upgrade, and test resilient and interoperable regional communications systems on a regular basis.

10. Develop tools and technologies to foster better communications and critical information technology infrastructure resilience.

11. Develop a tool set with which to assess damage in terms of economic, environmental, health and public safety, national security, and public confidence impacts.

12. Develop a regional risk-assessment approach that takes into account vulnerabilities, including interdependencies, the nature of the threat (multihazards), and the consequences of disruptions.

13. Develop a multi-year exercise strategy of tabletop and field exercises to test procedures and cooperation and identify gaps and potential corrective actions.

14. Continue regional and targeted exercises and drills (including field exercises) and incorporate lessons learned into incident management planning.

15. Develop and conduct regional exercises and targeted drills with a range of stakeholders—including the media and community groups—to test and further improve response plans.

16. Establish a regional mechanism to act as the focal point for coordinating response to regional disasters that is empowered to direct actions associated with resource allocation and management.

17. Undertake an assessment of federal, state, and local laws, rules, regulations, and procedures that impede recovery and restoration, including a cost-benefit analysis of how these constraints could be reduced and, if warranted, eliminated.

18. Incorporate interdependencies—including those of supply chains and customers' supply chains—into existing preparedness plans.

19. Establish processes and tools to identify and assess supply chain vulnerabilities/interdependencies and disruption impacts.

20. Develop risk assessment and decision support systems to determine optimal mitigation measures.

21. Establish a model process to establish continuous improvement through benchmarking and economic valuation metrics.

22. Develop a dynamic web-based system to enable key stakeholder personnel to obtain accurate information from experts on infrastructure security and general preparedness issues.

23. Continue the disaster resilience "life-cycle" of improvements, exercises, lessons learned, etc.

APPENDIX B

TISP TASK FORCE FOR REGIONAL DISASTER RESILIENCE
Member Organizational Affiliations

A2Group, Inc.
Air National Guard
American Institute of Architects
American Society of Civil Engineers' Committee on Critical Infrastructure
Argonne National Laboratory
ASME Innovative Technologies Institute, LLC
Assessment, Strategy & Tactics, Inc.
Association of Metropolitan Water Agencies
BellSouth
Bonneville Power Administration
Building Diagnostics Research Institute, Inc.
Chicago Manufacturing Center
Chicago Metropolitan Mayor's Caucus
ChicagoFirst
Cingular
City of Seattle
Collins Engineers, Inc.
Contra Costa County, California
Cox Communications
CSA Southeast, Inc.
Dufresne-Henry
Earth Tech, Inc./Tyco International
Edwards and Kelcey
EYP Mission Critical Facilities
Federal Bureau of Investigation, New Orleans Field Office
Federal Facilities Council
Florida Department of Law Enforcement
Fuller, Mossbarger, Scott and May Engineers, Inc.
Great Lakes Partnership
Hagerty Consulting
Hunton & Williams LLP
Iowa Homeland Security and Emergency Management Division
ISO New England
King County, Washington Office of Emergency Management
Las Vegas Valley Water District
Lessons Learned Information Sharing
Maryland Governor's Office of Homeland Security
Metcalf & Eddy/AECOM
Microsoft Corporation

Mississippi Maritime Association
Mitretek Systems
National Academic Consortium for Homeland Security
National Capital Region Planning Commission
National Institute of Standards and Technology
National Partnership for Streamlining Government
National Research Council, Board on Infrastructure and the Constructed Environment
National Society of Professional Engineers
New Orleans Mayor's Office of Homeland Security
New York City Office of Emergency Management
Office of the Assistant Secretary for Homeland Defense
Pacific NorthWest Economic Region
Pittsburgh Regional Business Coalition for Homeland Security
PMC Group, LLC
Post, Buckley, Schuh, Jernigan (PBS&J) Incorporated
Principal Financial Group
Puget Sound Partnership for Regional Infrastructure Security
Rescobie Associates, Inc.
San Diego Regional Chamber of Commerce
Scripps Health San Diego
Shaw Group
South Carolina VOLTAG
State of Louisiana
State of Washington, Critical Infrastructure Protection Office
State University of New York at Stony Brook Forum on Global Security
The Scalingi Group, LLC
Transportation Security Administration
U.S. Army Corps of Engineers
U.S. Coast Guard
U.S. Department of Energy Office of Electricity Delivery and Energy Reliability
U.S. Department of Homeland Security
Union Pacific
United Parcel Service
University of Findlay School of Environmental & Emergency Management—Center for Terrorism Preparedness
University of New Orleans
University of Washington
Washington State Association of Sewer & Water Districts
Wells Fargo & Company
William H. Gordon Associates, Inc.

THE INFRASTRUCTURE SECURITY PARTNERSHIP

TISP
1801 Alexander Bell Drive
Reston, VA 20191
http://www.tisp.org