HOMELAND SECURITY ADVISORY COUNCIL

REPORT OF THE CRITICAL INFRASTRUCTURE TASK FORCE

JANUARY 2006

Executive Summary

The objective of this report by the Critical Infrastructure Task Force (CITF) is to advance national policies and strategies that will foster the development of more resilient critical infrastructures. The recommendations contained herein leverage the foundation built by prior and ongoing Critical Infrastructure Protection programs, but assert that a future focus on resilience would establish a more appropriate basis for risk-based decisionmaking.

Our Nation's critical infrastructures—cyber and physical—empower and enable every aspect of our society and economy. From a homeland security perspective, fully functioning infrastructures are fundamental to all preparedness efforts. Consequently, our critical infrastructures represent attractive targets to adversaries. At the same time, critical infrastructures are inherently vulnerable to natural disasters, accidents, and other hazards that are a part of daily life. Given this diverse spectrum of potential threats, coupled with the reality that resources are limited, the CITF concluded that policies and strategies focusing on achieving resilience would be more robust than current guidance, which focuses primarily on protection. Specifically, the CITF observes that while protection is a necessary component of building resilience, resilience is not an inevitable outcome of strategies that focus on protection.

This report does not provide organizational recommendations. The CITF fully supports Secretary of Homeland Security Michael Chertoff's direction as stated in his March 16, 2005, speech at George Washington University: "Bureaucratic structures and categories exist to serve our mission, not to drive it."

This report also does not address the draft National Infrastructure Protection Plan that was disseminated for comment in November 2005; task force members provided feedback on that document within the designated comment period.

CITF members (see Appendix A) conductedmeetings in Charlotte, NC; Monterey, CA; and Washington, DC. Summaries of the meetings are included in Appendix B. CITF efforts were supported and informed by public and private-sector subject-matter experts, as noted in Appendix C. Throughout its deliberations, the CITF shared its observations and conclusions with the Homeland Security Advisory Council's State and Local Information Sharing Working Group, Private Sector Information Sharing Task Force, and the Weapons of Mass Effect Task Force.

The CITF chose to focus on strategic issues relating to the task at hand, distilling its conclusions to provide six high-impact recommendations. In developing these recommendations, task force members made an effort to integrate the perspectives of diverse stakeholder groups, both internal and external to the U.S. Department of Homeland Security. Discussion participants included Federal mission owners, private-sector infrastructure owners/operators, State and local government representatives, and scientific researchers who are working on related issues. Additional background information on regional, State, and local resilience and supporting information-sharing initiatives already underway is provided in Appendices D–I. These materials were generated by the people and organizations noted, and were not edited by the CITF.

The CITF's recommendations and the rationale for each are summarized below.

Recommendation 1: ***Promulgate critical infrastructure resilience (CIR) as the top-level strategic objective—the desired outcome—to drive national policy and planning.***

The CITF believes that business cases for investments that enhance CIR are both compelling and well-aligned with private-sector interests, a necessary condition for progress given the private-sector ownership of the vast majority of our infrastructures.

Recommendation 2: ***Align policy and implement directives for risk-based decisionmaking with the CIR objective within the broad context of the homeland security mission.***

The CITF observed that the top-level guidance that drives critical infrastructure planning efforts remains focused on protection against the terrorist threat, and believes that the resulting strategies will not mitigate the risks from a holistic perspective. The CITF further observed that the recent assignment of the Infrastructure Protection organization to the Preparedness Directorate affords a new opportunity to align and integrate planning approaches.

Recommendation 3: ***Create a framework of cascading national goals flowing from the top-level CIR objective.***

The CITF identified the need for a set of interlocking goals to align the objectives and actions of key stakeholder groups that influence CIR.

Recommendation 4: ***Establish and institutionalize proactive mechanisms to ensure that critical infrastructure policy and planning guidance continually evolves.***

The CITF observed that significant policy changes over the past decade tended to be event-driven (reactive), and believes that the complexity of the critical infrastructure planning challenge, coupled with the relative immaturity of current plans, warrants a proactive approach that fully engages the disparate stakeholder communities.

Recommendation 5: ***Establish a governance structure that supports the diversity of stakeholders within and among sectors, as well as the realities of infrastructure placement and operation within communities.***

The CITF noted that fostering the development of more resilient critical infrastructures will demand unprecedented cooperation and collaboration within and among disparate stakeholder communities. They identified the need for a governance structure that protects the equities of the various stakeholders.

Recommendation 6: ***Establish an information-sharing regime explicitly linked to critical infrastructure resiliency goals and governance—but integrated within an enterprise-wide information architecture.***

The CITF identified the need for information-related policies and systems to facilitate the actions necessary to achieve resilience—to encourage the necessary collaboration among private-sector entities as well as between the public and private sectors.

The CITF believes that the time for major investment in our Nation's critical infrastructures is long overdue. Responsibilities for critical infrastructure investments are, however, shared by the public and private sectors. Thus a common and empowering objective is needed if the Nation is to realize the full benefits of such investments. The CITF believes that CIR is that common objective.

Table of Contents

1. Critical Infrastructure Task Force Charter 1
2. Introduction 1
2.1 Retrospective 1
2.2 Common Threads 3
2.3 Current Environment 4
3. Resilience versus Protection 4
3.1 Lexicon 4
3.2 Business Case 5
3.3 Psychological Resilience 5
4. Strategic Guidance 6
4.1 Resilience versus Protection 6
4.2 Terrorism versus All-Hazards 6
4.3 Preparedness 6
5. National Goal 7
5.1 Relationship to National Preparedness Goal 7
5.2 Framework of Cascading Goals 7
5.3 Measuring Outcomes 7
5.4 Interdependencies 8
6. Planned Evolution of CIR Policy and Planning Guidance 8
6.1 Threat Diversity 8
6.2 Critical Infrastructure Exercises 9
6.3 Lessons-Learned Opportunities 9
7. Governance 9
7.1 Sector Diversity 10
7.2 Stakeholder Diversity 11
8. Information Sharing 11
8.1 Enable CIR 12
8.2 Leverage Emerging Initiatives 12
8.3 Use an Enterprise-wide Information Architecture 12
8.4 Maintain Operational Security 12
9. Conclusion 12

Appendices

Appendix A: CITF Members and Homeland Security Advisory Council Staff 13
Appendix B: Task Force Meeting Summaries 15
Appendix C: Government and Private-Sector Subject-Matter Experts 21
Appendix D: A Methodology for Critical Infrastructure Resiliency 23
Appendix E: Critical Infrastructure Resilience in Danville, VA 37
Appendix F: The Great Lakes Partnership: An Integrated Approach to Resilience and Recovery 39
Appendix G: Mission Assurance Governance Committee (MAG-C) Charter 41
Appendix H: St. Clair, Michigan Regional Critical Infrastructure Resilience Initiative 43
Appendix I: Community: U.S. Private and Public Partnership 47

Report of the Critical Infrastructure Task Force

1. CRITICAL INFRASTRUCTURE TASK FORCE CHARTER

"Review current and provide recommendations on advancing National Critical Infrastructure Policy & Planning to ensure the reliable delivery of critical infrastructure services while simultaneously reducing the consequences of the exploitation, destruction, or disruption of critical infrastructure products, services, and/or operations."

2. INTRODUCTION

Critical infrastructures—cyber and physical—provide the foundation for and enable the functioning of every facet of American society. As was demonstrated by the widespread impact of the infrastructure failures that followed Hurricane Katrina, resilient infrastructures—i.e., infrastructures that recover readily from adversity—are essential to continuity of business operations; to the successful execution of emergency response operations; to the maintenance of social stability; to the functioning of our economy; and to the advancement of our Nation's freedoms and quality of life.

2.1 Retrospective

National policy relating to critical infrastructures predates establishment of the U.S. Department of Homeland Security (USDHS) by more than two decades. Early guidance focused on ensuring the survival of a constitutional form of government and the continuity of essential Federal functions; plans dealt primarily with the threat of a nuclear attack.[1] Given the reduced threat from the former Soviet Union and its successor nations, most continuity of operations (COOP)/continuity of government (COG) programs were scaled back in the early 1990s. By the mid-1990s, the growing dependence on information technologies, together with emergence of malicious cyber attacks, gave rise to new concerns about the vulnerabilities of our Nation's infrastructures.

For the last decade, the policy and strategy framework relating to critical infrastructures has continued to evolve; major milestones are shown on the timeline in Figure 1.

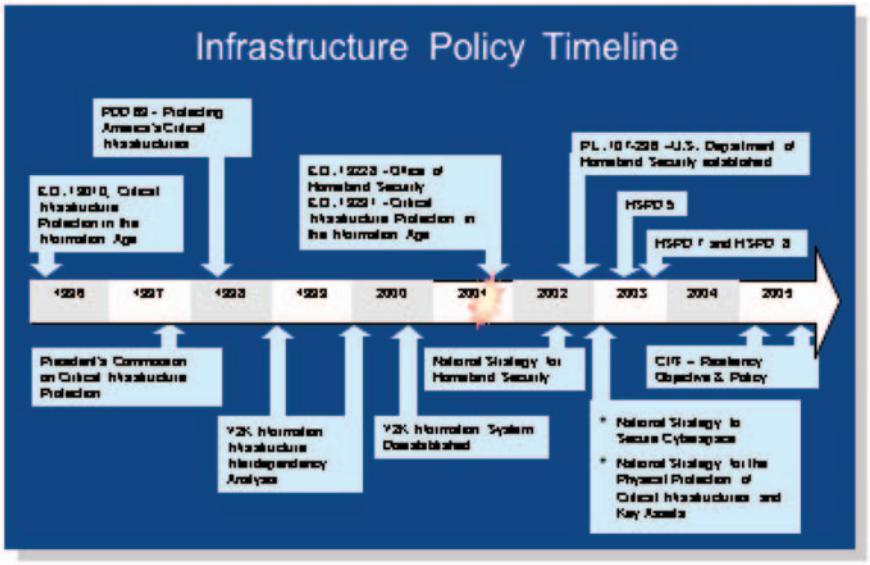


Figure 1. Evolution of critical infrastructure policy over the last decade

[1]NSDD 55, "Enduring National Leadership," dated September 14, 1982; NSD 37, "Enduring Constitutional Government," dated April 18, 1990; NSD 69, "Enduring Constitutional Government," dated June 2, 1992; PDD-67, "Enduring Constitutional Government and Continuity of Government Operations," dated October 21, 1998.

Executive Order (E.O.) 13010[2], issued in 1996, acknowledged that "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States;" continuity of government was included among a broader set of critical infrastructures. E.O. 13010 established the President's Commission on Critical Infrastructure Protection to analyze the situation and provide recommendations for government action. Among other tasks, the commission was to "recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation." The E.O. also identified the need for the government and the private sector to work together to develop such a strategy, and tasked the commission to "identify and consult with: (i) elements of the public and private sectors that conduct, support, or contribute to infrastructure assurance; (ii) owners and operators of the critical infrastructures; and (iii) other elements of the public and private sectors, including the Congress, that have an interest in critical infrastructure assurance issues and that may have differing perspectives on these issues."

Following the recommendations of the President's Commission on Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD-63)[3] restated in the President's Intent the longstanding national policy to "assure the continuity and viability of critical infrastructures." Although the National Goal established in PDD-63 (see Figure 2) was relatively comprehensive, specific guidance focused on elimination of significant vulnerabilities to physical and cyber attacks on critical infrastructures, with particular emphasis on protection of cyber systems.

As a result, the Federal Government proceeded to implement guidelines and programs that emphasized elimination of vulnerabilities, particularly those related to information networks, over the continuity and viability of critical infrastructures overall.

Despite years of effort, broad-based support was not obtained for the National Goal established in PDD-63. Numerous national councils, committees, offices, task forces, and working groups debated what should be done and by whom. Although the private sector comprised the principal infrastructure asset owners, operators, and ultimate source of expertise, they were not part of the discussion.[4]

A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- ***The Federal Government to perform essential national security missions and to ensure the general public health and safety;***
- ***State and local governments to maintain order and to deliver minimum essential public services;***
- ***The private sector to ensure the orderly functioning of the economy and the delivery of essential elecommunications, energy, financial and transportation services.***

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

Figure 2. National Goal established in 1998 by PDD-63.

[2]Executive Order 13010, "Critical Infrastructure Protection," dated July 15, 1996.

[3]Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," dated May 22, 1998.

[4]A notable exception is provided by the National Security Telecommunications Advisory Committee (NSTAC), which was created by E.O. 12382 in September 1982 to advise the President on matters regarding national security and emergency preparedness (NS/EP) telecommunications. The NSTAC is composed of up to 30 presidentially appointed industry leaders representing various elements of the telecommunications industry, and provides industry-based analyses and recommendations on a wide range of policy and technical issues related to telecommunications, information systems, information assurance, infrastructure protection, and other NS/EP concerns. For more information, see fact sheet at www.ncs.gov/nstac/nstac.html.

During this timeframe, private-sector planning continued to mature; infrastructure owners/operators increasingly focused on ensuring continuity of business in order to meet customer obligations as well as shareholder expectations.

The Year 2000 (Y2K) software glitch was the first significant test of public and private sector collaboration to resolve a problem that had the potential to severely disrupt economic activity in the developed world, as well as to jeopardize the health and safety of the public—a problem that stemmed from critical infrastructure dependence on information technology and the interdependence of information networks. Significant resources were expended to assure continuity of infrastructure operations—to build resilience in the face of a potentially catastrophic flaw.

The feared crippling of critical information networks did not materialize at the stroke of midnight on December 31, 1999, and the Federal Government promptly declared success and moved on to other priorities. Unfortunately, the institutional knowledge and public-private partnerships that might have formed the foundation for achievement of the National Goal established in PDD-63 were not sustained, and lessons from Y2K efforts had minimal long-term impact on critical infrastructure policy and planning.

Following the terrorist attacks on September 11, 2001, the Federal Government redoubled its efforts on critical infrastructure protection (CIP)—but the pendulum swung toward physical protection in contrast to the earlier focus on cyber threats. CIP-related programs focused on generating lists of critical assets and assessing the vulnerability of those assets—often without defensible criteria for evaluating criticality and/or a rigorous methodology for vulnerability assessment. Cyber-security programs evolved on a parallel path and, in February 2003, two separate national strategies were released—one for physical protection of critical infrastructures and key assets, and one to "secure cyberspace."[5] The National Strategy for Homeland Security called for a comprehensive national infrastructure protection plan that would build on the foundation of these two separate documents and establish standards and benchmarks for infrastructure protection.[6]

Guidance and focus continued to evolve with the establishment of the USDHS and subsequent Presidential Directives. The founding legislation for the USDHS identified primary responsibilities for the Under Secretary for Information Analysis and Infrastructure Protection[7] to include: (2) comprehensively assessing the vulnerabilities of the key resources and critical infrastructures in the United States; and (4) developing a comprehensive national plan for securing the key resources and critical infrastructures in the United States. Homeland Security Presidential Directive (HSPD)-7[8] established the corresponding national policy guidance and tasked the Secretary to produce "a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive."

2.2 Common Threads

While details of the national guidance—including definitions of the critical infrastructure sectors—have evolved over the past decade, some parameters have remained constant. Key policy documents have consistently identified protection—i.e., reducing vulnerabilities—as the key action driver. Despite the warning provided by the power blackout in the northeastern states in August 2003, as well as more recent natural disasters, strategic guidance relating to critical infrastructures has continued to focus on mitigation of the terrorist threat. And despite routine acknowledgment of the interdependencies within and among critical infrastructure sectors, sector-focused planning approaches have prevailed.

[5]"The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" and "The National Strategy to Secure Cyberspace," White House, February 2003.

[6]"The National Strategy for Homeland Security," Office of Homeland Security, White House, July 2002, p. 33.

[7]Homeland Security Act of 2002, Section 201, Under Secretary for Information Analysis and Infrastructure Protection.

[8]HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," dated December 17, 2003.

2.3 Current Environment

Secretary Chertoff established risk management as the top-level homeland security strategy, and consistently articulates the need to implement lower-level strategies to mitigate the three components of risk: threat, vulnerability, and consequence. CITF members agree with this emphasis on risk management, but believe that current policy and strategic guidance biases the actions of CIP mission owners toward reducing vulnerabilities, rather than encouraging the development of systems-level strategies that mitigate risks from a holistic perspective

The spectrum of adversities that threaten our critical infrastructures is diverse—ranging from terrorists and other enemies with malevolent intent to catastrophic accidents and natural disasters. The spectrum of vulnerabilities is immense—particularly given the geographic distribution and inherent interdependencies that exist both within and among infrastructure sectors. The spectrum of potential consequences is vast—ranging from economic impacts that accrue from destruction of property and disruption of vital services to loss of life.

The CITF members therefore believe that making **resilience** the top-level objective—the desired outcome—would foster development of subordinate risk management strategies that more effectively address the complexities inherent in the critical infrastructure mission.

3. RESILIENCE VERSUS PROTECTION

Although it may be argued that current planning for CIP encompasses the full risk equation, which considers threats and consequences as a by-product of identifying critical vulnerabilities, the focus for action remains on protection through emphasis on reduction or elimination of vulnerabilities. The CITF concluded that making resilience the overarching strategic objective would stimulate synergistic actions that are balanced across all three components of risk.

Recommendation 1: ***Promulgate critical infrastructure resilience as the top-level strategic objective—the desired outcome—to drive national policy and planning.***

3.1 Lexicon

It was acknowledged from the start that "homeland security is a shared responsibility"[9] and, as such, requires effective communication and collaboration within and across disparate stakeholder communities. An earlier recommendation by the Homeland Security Advisory Council (HSAC) stimulated initiation of a USDHS lexicon project to promote consistent use of key words and phrases, thereby enhancing communication among the Department's vast community of stakeholders. The HSAC also observed that ambiguity is introduced when words are defined or used in government documents in ways that are inconsistent with dictionary definitions.

Dictionary[10] definitions for "protection" and "protect" are:

> **Protection—1**: the act of protecting : the state of being protected . . .
> **Protect—1**: to cover or shield from exposure, injury, or destruction . . .

The use of "protect" in HSPD-7 is aligned with the dictionary definition in that it maintains the defensive focus; HSPD-7 provides the following:[11]

> *The terms "protect" and "secure" mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.*

The CITF believes that protection, in isolation, is a brittle strategy. We cannot protect every potential target against every conceivable attack; we will never eliminate all vulnerabilities. Furthermore, it is virtually impossible to define a desired endstate—to quantify how much protection is enough—when the goal is to reduce vulnerabilities.

In contrast, a dictionary definition[12] for "resilience" is:

> **Resilience—2:** an ability to recover from or adjust easily to misfortune or change.

Strategies based on resilience accept that efforts to prevent attacks (reduce threats) and to defend against those attacks (reduce vulnerabilities), albeit necessary, will

[9]Ibid. Introductory letter signed by George W. Bush, dated July 16, 2002.
[10]Merriam-Webster Online Dictionary: http://www.m-w.com/dictionary.
[11]HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," dated December 17, 2003, definitions (6)(h).
[12]Merriam-Webster Online Dictionary: http://www.m-w.com/dictionary.

inevitably prove insufficient. Strategies based on resilience address all three components of the risk equation in an integrated fashion. The author of Beyond Fear[13] observes that:

> *Because security systems fail so often, the nature of their failure is important. Systems that fail badly are brittle, and systems that fail well are resilient. A resilient system is dynamic; it might be designed to fail only partially, or degrade gracefully; it might adjust to changing circumstances.*

With the intent of contributing to the homeland security lexicon, we offer the following definition, which was taken from a recent article in Science:[14]

> *Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.*

Critical Infrastructure Resilience (CIR) is not a replacement for CIP, but rather an integrating objective designed to foster systems-level investment strategies. Adoption of CIR as the goal provides a readily quantifiable objective—identifying the time required to restore full functionality.

3.2 Business Case

Given that the vast majority of our Nation's critical infrastructures are owned and operated by the private sector, relevant national objectives and strategies must be designed to motivate implementation within inherently competitive business environments. That is, there must be a quantifiable business case that justifies the investment of resources.

A business case assesses the value of a particular investment in terms of meeting an organization's objectives; it includes a cost-benefit analysis and clear articulation of expected outcomes. Business cases consider a wide range of factors, generally analyzing the social, technical, financial, and legal/policy implications of a proposed investment. The immutable rule, however, is that the analysis is performed from the perspective of the entity that will bear the cost of the investment.

The CITF concluded, after numerous discussions with private-sector stakeholders, that it is extremely difficult to build a business case for protection as a purely defensive strategy. This is due in part to the "how much is enough" dilemma, and in part because businesses typically do not own or control all of the resources on which they depend, and therefore have limited ability to protect those resources. These realities are leading the private sector to emphasize continuity of business planning, which integrates security planning (focusing on protection) with disaster recovery planning, and requires enterprise-wide risk analysis.

More recently, businesses have begun to adopt resilience as their over-arching objective, which implies a general ability to adapt to changing environmental conditions—not only to the direct impacts of a disaster. According to a 2002 paper published by Gartner[15], "enterprises are taking on the new challenge of deliberately designing resilience into their management of people, places, infrastructure, and work processes.… Business resilience emerges through business, corporate and IT leaders deliberately working together across geographical, functional, business and decision-making boundaries to build an organization that rebounds, adjusts quickly and resumes operations."

Whereas it is difficult to define a business case for CIP, the CITF believes that business cases for investments that enhance CIR are both compelling and well-aligned with private-sector interests. Such alignment is a necessary condition for progress, given that the vast majority of our critical infrastructures are owned and/or operated by the private sector. Without regulatory requirements, which are largely viewed as undesirable, a solid business case is necessary to motivate business owners to make investments that improve their business continuity, thus contributing to the overall resiliency of our critical infrastructures. The white paper provided in Appendix D describes a methodology for quantifying the resiliency of tightly coupled networks.

3.3 Psychological Resilience

Businesses and governments must retain the trust and confidence of their customers (citizens) if they are to remain viable. In the aftermath of September 11, 2001, the Travel Industry Association of America projected a 39-percent drop in total airline passenger miles in the fourth quarter of 2001.[16] The sharp drop in travel impacted not only the aviation industry, but

[13] Beyond Fear, Bruce Schneier, Copernicus Books: ISBN 0-387-02620-7, © 2003, p. 119.

[14] "Toward Inherently Secure and Resilient Societies," Brad Allenby and Jonathan Fink, Science, August 12, 2005, Vol. 309, p. 1034.

[15] "The Blueprint for the Resilient Virtual Organization," Gartner, 2002, ID Number: AV-15-0894.

[16] "States Take Action to Bolster Travel Industry," National Conference of State Legislatures, http://www.ncsl.org/programs/press/2002/issues/tourism.htm.

the tourism industry as well. The total economic impact extended well beyond the direct "ground zero effects," and was exacerbated by citizens' choices based on their altered perceptions of risk.

Ultimately, the ability of critical infrastructures to fully recover from a catastrophe depends on the actions of their customers. Thus educational initiatives designed to build "psychological resilience"—i.e., to help customers/citizens adapt to the changing security climate—should be key components of a national strategy for CIR.

4. STRATEGIC GUIDANCE

The organizational realignments that resulted from Secretary Chertoff's Second Stage Review of the USDHS provide a near-term opportunity to establish more integrated planning approaches for the critical infrastructure mission area, but issues nevertheless remain with top-level strategic guidance.

Recommendation 2: ***Align policy and implement directives for risk-based decisionmaking with the critical infrastructure resilience objective within the broad context of the homeland security mission.***

4.1 Resilience versus Protection

In Section 2 we observed that virtually all top-level guidance for critical infrastructure planning focuses on protection; in Section 3 we said that resilience is a more robust objective for risk-based decisionmaking.

Current actions of the Infrastructure Protection (IP) organization are driven by HSPD-7, which identifies mandatory elements for the National Plan for Critical Infrastructure and Key Resources Protection.[17] Without a change to the policy directive, the USDHS has the latitude to include "other Homeland Security-related elements as the Secretary deems appropriate." The CITF believes the Secretary should exercise this option and expand the current National Infrastructure Protection Plan (NIPP) planning process to encompass the broader resilience objective, while retaining the required elements that focus more narrowly on protection.

Ultimately, however, the CITF believes that HSPD-7 should be modified to establish a more consistent framework of policy guidance across all homeland security mission areas.

4.2 Terrorism versus All-Hazards

In Section 2 we observed that virtually all top-level guidance for critical infrastructure planning focuses on threats from terrorist attacks. Specifically, HSPD-7[18] defines as its purpose:

> "This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."

Although terrorist threats are obviously acknowledged, this guidance establishes for critical infrastructure mission owners a planning environment that is not aligned with the broader homeland security mission objectives, which incorporate the all-hazards perspective.

In particular, HSPD-8 requires "all-hazards preparedness" to connote "preparedness for domestic terrorist attacks, major disasters, and other emergencies."[19] Given that HSPD-8 establishes policies to strengthen our ability to prevent as well as to respond to all hazards, and that critical infrastructures play a vital role in all related activities, the CITF believes that critical infrastructure planning must also incorporate the all-hazards perspective. The CITF also believes that HSPD-7 should be modified to establish a more consistent framework of policy guidance.

The CITF observes that the private sector already employs an all-hazards perspective in assessing risks to their enterprises, so extension of the Federal Government's critical infrastructure planning in this regard is likely to be well-received—particularly in the aftermath of the infrastructure failure that greatly amplified the consequences of Hurricane Katrina.

4.3 Preparedness

The recent organizational alignment of the IP organization as a key component of the newly established Preparedness Directorate affords new opportunities to integrate USDHS planning efforts and foster the development of strategies that enhance CIR within the all-hazards context. Although the USDHS Secretary was assigned the responsibility for coordinating the overall national effort for infrastructure protection planning, additional guidance will likely be required to extend this more holistic

[17] HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," dated December 17, 2003, Implementation (27).
[18] Ibid. Purpose (1).
[19] HSPD-8, "National Preparedness," dated December 17, 2003, definitions (2)(a).

planning environment to other Federal departments and agencies that are designated to lead specific sector planning activities.

As previously observed, functioning critical infrastructures are vital to response and recovery efforts and therefore should be explicitly included in preparedness planning. The CITF therefore believes that additional rationalization is needed between HSPD-7, which delineates the Secretary's responsibilities with regard to all critical infrastructures, andHSPD-8, which establishes preparedness-related policies and guidance.

The CITF believes that articulation of CIR as the top-level objective establishes a framework that will facilitate integration of planning activities and yield more effective allocation of limited resources. In addition, we believe this objective is better aligned with both current private-sector practices and the needs of local communities to enhance their preparedness across the all-hazards spectrum.

5. NATIONAL GOAL

The National Goal established by PDD-63 (see Section 2.1) in 1998 failed to gain momentum for a variety of reasons, but the CITF believes it is worth reviewing as a starting point. The goal as written emphasizes protection against intentional acts and thus would need to be modified to be consistent with our recommended objective of resilience to all hazards. We observe, however, that the goal already addresses three key stakeholder communities, the Federal Government, State and local governments, and the private sector, and implies the need for resilient critical infrastructures:

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

Recommendation 3: ***Create a framework of cascading national goals flowing from the top-level Critical Infrastructure Resilience objective.***

5.1 Relationship to National Preparedness Goal

The approach described in the "Interim National Preparedness Goal" includes CIP on the Target Capabilities List, and identifies implementation of the Interim National Infrastructure Protection Plan as an overarching national priority.[20] It is not, however, apparent that the approach will yield the resilient critical infrastructures vital to the delivery of other target capabilities. In fact, it is not clear how such interdependencies are addressed within the preparedness planning framework.

The CITF believes that preparedness, like protection, is necessary but insufficient for achieving resilience. We therefore recommend that an overall framework be established with resilience as the top-level objective.

5.2 Framework of Cascading Goals

As we noted early in this report, critical infrastructures—cyber and physical—provide the foundation and enable the functioning of every facet of American society. Key stakeholder communities exist at every level of government and throughout the private sector. In the context of a business case analysis, individual stakeholders can be expected to make choices based on the value of a particular investment to the achievement of their objectives. Perhaps the greatest challenge we face in enhancing the resilience of critical infrastructures is the need to align the objectives of these disparate stakeholder communities and achieve the unity of effort needed to enhance resilience.

During its meetings, the CITF heard several examples wherein consolidation of infrastructure elements, although attractive from a right-of-way allocation perspective, led to traffic chokepoints and single points of failure. The white paper provided in Appendix D offers additional background information on this issue.

The CITF therefore sees the need for a hierarchical decomposition framework of cascading, interlocking, and increasingly specific goals that are designed to align the objectives—and therefore the actions—of the key stakeholder groups (at Federal, regional, State, local, tribal, and private-sector levels) that influence critical infrastructure resilience.

5.3 Measuring Outcomes

To be of value, the framework of cascading goals must define measurable outcomes. Then targets must be established for each, and resources allocated accordingly. This is standard business practice; the one caveat that must be added, however, is the adage: "Be careful what you measure, because what

[20] "Interim National Preparedness Goal," U.S. Department of Homeland Security, March 31, 2005.

you measure will improve—perhaps at the expense of something more important." Measures are important but must be selected carefully to ensure the alignment of actions necessary to enhance resilience.

An effective top-level measure of infrastructure resilience is the time required to restore full functionality in the event of a disruption. A corollary measure suggested by the National Goal defined in PDD-63 is the geographic scope of the disruption.

For tightly coupled networks, additional subordinate metrics are suggested in the white paper in Appendix D. The dilemma with many of these measures is that very often no single stakeholder "owns" all of the actions necessary to achieve success. Thus the goals must be designed to motivate the stakeholders to work collaboratively and to adopt best practices within this highly interdependent environment.

If a hierarchical decomposition technique is used to create the framework of interlocking goals, it should be performed with a focus on accountability/ownership at each level.

5.4 Interdependencies

Although most planning guidance relating to critical infrastructures acknowledges the interdependencies both within and among sectors, robust plans for dealing with those interdependencies have yet to emerge. Perhaps the most urgent need is to integrate planning activities across the physical and cyber threat spectrums, but other critical interdependencies exist.

The National Strategy to Secure Cyberspace identifies cyberspace as the nervous system for our Nation's critical infrastructures—the control system of the country.[21] At the same time, it acknowledges that "cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work"—physical assets. Enhancing the resilience of our critical infrastructures will require integrated planning that addresses both physical and cyber threats.

Recent disasters have provided ample demonstration that interdependencies among infrastructure sectors tend to amplify the overall impact (e.g., disruption of the telecommunications infrastructure severely impacts delivery of emergency services). The CITF therefore concluded that Federal strategic planning should shift its emphasis in the near term to identification and evaluation of such interdependencies. While nascent modeling and simulation tools are of some value in this area, it is not clear that the Federally funded tool development efforts are well-integrated with either Federal planning activities or the modeling and simulation capabilities used by the private sector for their own planning purposes. Here again, work performed by the NSTAC may provide valuable examples for the broader planning efforts.

6. PLANNED EVOLUTION OF CIR POLICY AND PLANNING GUIDANCE

In Section 2.1 of this report, we described the evolution of critical infrastructure policy and planning guidance. Most of the significant changes were threat-driven—reactions to perceived changes in the external threat environment. The collapse of the Soviet Union decreased our emphasis on planning for continuity of government in the event of a nuclear attack, although the NSTAC continued to provide focus on national security and emergency preparedness telecommunications as a key enabler of COOP/COG efforts. Growing dependence on information networks, together with the emergence of cyber threats, led us to focus on cybersecurity. The September 11, 2001, attacks, however, shifted our attention back to physical security. The increasing global access to the materials and expertise required to fabricate weapons of mass destruction (WMD) has led to increased investment in corresponding countermeasures. The CITF believes a proactive planning approach is long overdue.

Recommendation 4: ***Establish and institutionalize proactive mechanisms to ensure that critical infrastructure policy and planning guidance continually evolves.***

6.1 Threat Diversity

Terrorist capabilities will continue to evolve over the coming years as the forces of globalization spread both sophisticated technologies and the related expertise for weaponization. Although natural disasters are, in a sense, more predictable,

[21] "The National Strategy to Secure Cyberspace," White House, February 2003.

their impacts may be amplified by societal choices (e.g., erosion of natural flood barriers). Given the age, fragility, capacity limitations, and growing interdependencies of our Nation's critical infrastructures, accidents and errors are increasingly likely to cause disproportionate impacts. The bottom line is that critical infrastructure planning must consider a diverse, uncertain, and evolving spectrum of threats. The scenario-based methodology underway in preparedness planning provides a useful model for considering a wide spectrum of potential threats.

However, the critical infrastructure mission area is unique. Critical infrastructures may be directly targeted for destruction/disruption, and may serve as delivery systems for terrorist weapons (e.g., the U.S. Postal Service delivered the anthrax-laced letters). They may suffer collateral damage because of interdependencies (e.g., supply chain disruptions due to port closure, as occurred during the west coast management lock-out, and again in the aftermath of Hurricane Katrina).

The CITF therefore sees the need for scenarios that test the resilience of critical infrastructures in the face of both direct and indirect effects of an event; also assess their ability to thwart attempts to exploit our infrastructure for weapon delivery; and, perhaps most importantly, fully engage the disparate stakeholder communities.

6.2 Critical Infrastructure Exercises

Critical infrastructure planning is highly complex because of interdependencies among sectors, diversity within and among sectors, disparate stakeholder communities, and fragmented governance structures; the challenge is exacerbated by the evolving and diverse spectrum of threats to our infrastructures. The CITF therefore recommends the creation of a critical infrastructure exercise program—an ongoing series of scenario-driven tabletop events that bring together different stakeholder communities and emphasize learning versus demonstration. The program should be designed to educate participants while identifying capability gaps, thereby advancing the planning process.

The exercise program should bring together private-sector executives, security and emergency managers who are responsible for the provision of infrastructure services, representatives from State and local governments/communities who depend on those services, and Federal Government stakeholders. Scenarios should be designed to simultaneously engage all relevant sectors, rather than be held on a sector-by-sector basis. The program should be structured to identify strategic issues (e.g., right-of-way allocation in a geographic region) in addition to more tactical capability gaps. The overall goal of the exercise program should be the ongoing evolution of critical infrastructure policy and planning guidance to continually enhance CIR as systems are upgraded or replaced over time. Creation of a resilient critical infrastructure is not a task that will be completed—it is a journey, not a destination.

6.3 Lessons-Learned Opportunities

Natural disasters and accidents provide additional opportunities to advance critical infrastructure policy and planning guidance. The CITF recommends the creation of a robust lessons-learned process to be employed in the immediate aftermath of any event that significantly impacts critical infrastructure functionality. As with the outcomes of the recommended exercise program, the lessons should feed directly into the policy and planning processes, helping to advance strategic guidance while identifying problems that require immediate remedial action.

The CITF noted that Hurricane Katrina created a near-term opportunity for infrastructure-related lessons, and recommendsthat the event be used to establish a baseline methodology that is tailored to identify issues that relate specifically to CIR.

7. GOVERNANCE

Fostering the development of more resilient critical infrastructures will demand unprecedented cooperation and collaboration among disparate stakeholder communities; such cooperation will not occur without trust within and among those communities. During its session, the CITF heard repeatedly from private-sector and State/local government representatives that they had not been adequately engaged in critical infrastructure planning. The CITF concluded that at least part of the problem is because of the sheer diversity of the critical infrastructure sectors. In addition, it appears that the sector-based planning approach may not effectively integrate the perspectives of the communities and regions in which the infrastructures operate.

Recommendation 5: ***Establish a governance structure that supports the diversity of stakeholders within and among sectors, as well as the realities of infrastructure placement and operation within communities.***

7.1 Sector Diversity

As national policy and guidance have evolved over the past decade, so too have the definitions of our Nation's critical infrastructures. Figure 3 shows the responsibilities as assigned by PDD-63 in 1998 and the assignments established by HSPD-7 in 2003.

Although some changes resulted from creation of the USDHS and the associated transfer of responsibilities, other changes represent additions to the scope of our Nation's critical infrastructures.

The CITF observes that although most of the originally identified sectors operate as tightly coupled networks, some of the more recent additions (e.g., food, agriculture and Defense Industrial Base) lack that cohesion; this reality may contribute to some of the concerns raised during CITF discussions.

The CITF also observed that key resources and national icons are fundamentally different from the critical infrastructure sectors, and may require unique planning approaches; deliberations regarding these items were limited to a discussion of the need for psychological resilience as described in Section 3.3.

PDD-63 Assignments of Responsibility		HSPD-7 Designations	
Lead Agency	**Sector**	**Lead Agency**	**Sector**
Commerce	Information and Communication	USDHS	Information Technology; Telecommunications; Chemical; Transportation Systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; Emergency Services; and Postal and Shipping Key resources including dams, government facilities, and commercial facilities.
Transportation	Aviation; Highways, Mass Transit; Pipelines; Rail; Waterborne Commerce		
FEMA	Emergency Fire Service; Continuity of Government Services		
Department of Justice/FBI	Emergency Law Enforcement Services		
Treasury	Banking and Finance	Treasury	Banking & Finance
Environmental Protection Agency (EPA)	Water Supply	EPA	Drinking Water & Water Treatment Systems
Health and Human Services (HHS)	Public Health Services	HHS	Public Health, Healthcare, and Food (other than meat, poultry, egg products)
Department of Energy (DOE)	Electric Power; Oil & Gas Production and Storage	DOE	Energy, including the production, refining, storage and distribution of oil and gas; and electric power except for commercial nuclear power facilities
		Department of Agriculture	Agriculture, food (meat, poultry, egg products)
		Department of Defense	Defense Industrial Base
		Department of the Interior	National Monuments and Icons

Figure 3. Evolution of critical infrastructure sector definitions.

After discussions with representatives from several distinctly different sectors, the CITF concluded that proposed governance structures should be tailored to better accommodate the diverse characteristics of the individual critical infrastructure sectors, as well as theinterdependencies among sectors. Recent work by the National Infrastructure Advisory Council (NIAC) provides useful recommendations in this regard,[22] but additional refinement may be required to address the concerns expressed by some private-sector representatives.

7.2 Stakeholder Diversity

As noted earlier, critical infrastructures operate within communities, not sectors. Although some sector-specific planning is necessary, of equal importance is the need to engage the local communities to which services are delivered. Those communities are not only customers for infrastructure services; they also make decisions that impact infrastructure owners'/operators' ability to provide those services. Similarly, a single sector does not operate in isolation (e.g., the food sector depends on the transportation sector, which depends on the energy sector, etc.). The CITF therefore concluded that the equities of individual stakeholder groups must be identified before an effective governance structure can be defined. Figure 4 offers a perspective on how key stakeholder interests intersect around resilience.

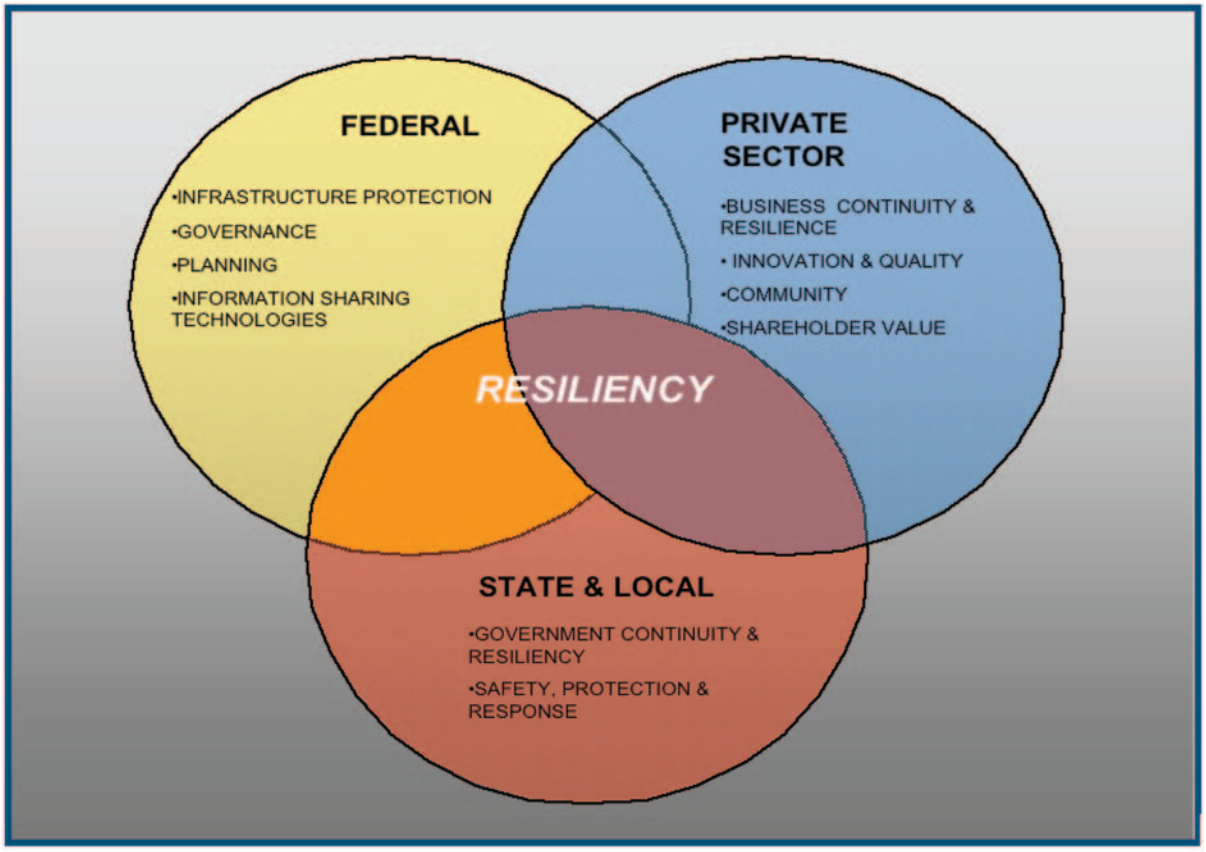


Figure 4. Intersecting stakeholder interests.

8. INFORMATION SHARING

As noted in the previous section, creation of more resilient critical infrastructures will require unprecedented collaboration and cooperation between disparate stakeholder communities. Based on anecdotal feedback to the CITF, the trust required to foster such cooperation does not yet exist. While some issues relate to policy, other concerns stem from the lack of efficient communication channels. Several participants observed that the numbers of channels and systems continue to expand, whereas the unique information content does not.

Recommendation 6: ***Establish an information-sharing regime explicitly linked to critical infrastructure resiliency goals and governance—but integrated within an enterprise-wide information architecture.***

[22] "Initial Report and Findings," Sector Partnership Model Working Group, NIAC, dated October 11, 2005.

8.1 Enable CIR

Strategies to enhance resiliency cannot be implemented in isolation; they must be integrated to address all components of the risk equation. The requisite information-sharing regime must support collaboration—i.e., much more than a one-way dissemination channel is needed. Information-related policies and systems must be designed to facilitate the actions necessary to achieve resilience—to encourage the necessary collaboration among private-sector entities, as well as between the public and private sectors.

The framework of cascading goals described in Section 3 will provide a basis for identification of the required collaborative relationships, and the lessons-learned processes described in Section 6 can help refine the requirements and guide policy evolution.

8.2 Leverage Emerging Initiatives

During its session, the CITF learned of several initiatives designed to foster CIR and improve collaboration between the public and private sectors. These initiatives are included in alphabetical order in Appendices E–I. The CITF suggests that progress toward achieving effective information sharing and CIR could be accelerated through aggressive identification and sharing of lessons learned from such regional and local initiatives.

8.3 Use an Enterprise-wide Information Architecture

Other reports have identified the need for an enterprise-wide information architecture to support the homeland security mission; we endorse those recommendations. We further observe that effective architecture design requires clear articulation of what information is needed by whom and for what purpose. The CITF noted that many end users at the local level are accountable for multiple mission areas within the overall homeland security mission. A core element of the critical infrastructure planning process should be identification of the information requirements of key private-sector and regional/State/local stakeholders; those requirements should influence a unified enterprise architecture design, however, rather than create additional critical infrastructure-specific communication channels.

8.4 Maintain Operational Security

History provides ample evidence that our adversaries are adept at gaining access to unprotected information. Although the Internet is an invaluable resource for many purposes, we must accept that our adversaries mine that resource and exploit publicly available information to aid their operational planning. Risk management strategies must support the design and implementation of the necessary information-sharing regime.

9. CONCLUSION

America's interdependent critical infrastructures are efficient but aging, overstressed, often geographically concentrated, and potentially consequence-amplifying. In spite of a decade of national policy, guidance, and investment relating specifically to CIP, little progress is discernible. And during the same period, societal dependencies and sector interdependencies continued to expand.

There are technologies that could mitigate some concerns through the replacement of obsolete equipment. Other modern technologies could be used to enable operators to rapidly detect or anticipate impending failures. Current and emerging modeling and simulation tools are available to help analyze interdependencies and their consequences, as well as to investigate risk mitigation options. But all of these technologies, tools, and techniques are of value only if applied within the context of a clear objective—a desired outcome that is measurable.

The time for major investment in our Nation's critical infrastructures is long overdue. But such investment is necessarily a shared responsibility, and therefore requires the full support of the private sector, as well as public-sector stakeholders. Such support will not be obtained without a shared objective that is aligned with the interests of all stakeholder communities. The CITF believes that the national pursuit of CIR is that shared objective.

Appendix A

CITF MEMBERS

Dr. Ruth David (Chair), President and Chief Executive Officer of ANSER – Member, Homeland Security Advisory Council (HSAC) and Vice Chair, Academe and Policy Research Senior Advisory Committee, HSAC.

Erle Nye (Vice-Chair), Chairman of the Board and chief executive for TXU Corp. and Chair of the National Infrastructure Assurance Council – Member, HSAC.

Duane Ackerman, Chairman and Chief Executive Officer, BellSouth Corporation – Member, HSAC and Member, National Infrastructure Assurance Council.

Dr. Richard Andrews, Former Homeland Security Advisor to Governor Schwartzenegger, Senior Director, Homeland Security Projects, for NC4 – Member, HSAC and Chair, Emergency Response Senior Advisory Committee, HSAC.

Frank Cilluffo, Associate Vice President for Homeland Security at The George Washington University – Member, HSAC.

Frank Cruthers, Deputy Commissioner, New York Fire Department – Member, Emergency Response Senior Advisory Committee, HSAC.

Robert Eckels, Judge, Harris County, TX – Member, State and Local Officials Senior Advisory Committee, HSAC.

Don Knabe, Supervisor, Los Angeles County Board of Supervisors – Member, State and Local Officials Senior Advisory Committee, HSAC.

MG (Ret.) Bruce Lawlor, Chairman and CEO of CRA, Inc. – Member, HSAC.

Peggy Merriss, City Manager, Decatur, GA – Member, State and Local Officials Senior Advisory Committee, HSAC.

Judith Mueller, Director of Public Works, Charlottesville, VA, and Former President, American Public Works Association – Member, Emergency Response Senior Advisory Committee, HSAC.

Mitt Romney, Governor of Massachusetts – Member, HSAC and Chair, State and Local Officials Senior Advisory Committee, HSAC.

Gary Scott, Chief, Campbell County, WY, Fire Department – Member, Emergency Response Senior Advisory Committee, HSAC.

Bill Whitmore, President and CEO, Allied Security – Member, Private Sector Senior Advisory Committee, HSAC.

Houston Williams, CEO and Chairman, Pacific Network Supply, Inc. – Member, Private Sector Senior Advisory Committee, HSAC.

Dr. John "Skip" Williams, Provost and Vice President for Health Affairs and Bloedorn Professor of Administrative Medicine, The George Washington University – Member, Emergency Response Senior Advisory Committee, HSAC.

BG (Ret) Allan Zenowitz, Retired FEMA Official – Member, Academe and Policy Research Senior Advisory Committee, HSAC.

HSAC STAFF

Dan Ostergaard, Executive Director, HSAC.

Jeff Gaynor, Director, Emergency Response Senior Advisory Committee and Director, Critical Infrastructure Task Force, HSAC.

Mike Fullerton, Director, Academe and Policy Research Senior Advisory Committee, HSAC.

Mike Miron, Director, State and Local Officials Senior Advisory Committee, HSAC.

Carnes Eiserhardt, Executive Assistant, HSAC.

Appendix B

Task Force Meeting Summaries

The Task Force conducted meetings and discussed, at length, national critical infrastructure policy objectives, governance, and operations with Federal, State, and local government officials and corporate and private subject-matter experts.

February 21, 2005—Omni Hotel: Charlotte, NC

Objective: After studying Presidential Decision Directive (PDD)-63, Homeland Security Presidential Directive (HSPD)-7, HSPD-8, the Interim National Infrastructure Protection Plan (INIPP), Unrestricted Warfare, and the Sarbanes-Oxley Act of 2002, members of the Critical Infrastructure Task Force (CITF) should focus on its charter to:

> *"Review current and provide recommendations on advancing national critical infrastructure policy and planning to ensure the reliable delivery of critical infrastructure services while simultaneously reducing the consequences of the exploitation, destruction, or disruption of critical infrastructure products, services, and/or operations."*

Meeting Summary: To these ends, the CITF attended presentations and engaged speakers on:

- Ongoing and projected U.S. Department of Homeland Security (USDHS) critical infrastructure protection (CIP) and INIPP efforts.
- Operations security (OPSEC).
- Private-sector information sharing.
- The organization and operations of the Homeland Security Information Network—Critical Infrastructure (HSIN-CI).
- Critical infrastructure resiliency (CIR) modeling and business case.
- Private sector/business and Federal mission assurance initiatives.
- International infrastructure resilience initiatives.

Task Force Observations:

- Critical infrastructure(s) (CI) operation powers the Nation and provides the foundation for individual, government, and national activities:
  - — CI are targets that can provide attackers with high-consequence effects—potentially inflicting long-term human suffering, social disorder, and physical and economic damage.
- USDHS infrastructure protection initiatives provide a foundation for ensuring the reliable delivery of infrastructure services. After September 11, 2001, and with more attacks throughout the world, however, protection is not an adequate or objectively measurable and sustainable national objective:
  - — Previous, current, and projected CIP efforts are largely remnants and iterations of mid-1990s cyber/network protection philosophies, and to an attacker these represent static, defensive, predictable, and easily defeatable approaches.
  - — Protection is inconsistent with the lessons of history and war, with the operational continuity focus of the private-sector/business communities, and with emerging initiatives by regional and local groups and parts of the international community.
  - — Protection instills a defender's view (i.e., from the inside out) and lessens the ability to see and effectively anticipate what the enemy may see looking from the outside in—what has been termed the "predator's view."
- There is far too much CI targeting information publicly available. Increased emphasis on OPSEC is vital. Infrastructure and business owners must learn to view and value information more as our adversaries—i.e., information as targeting data—in order to make responsible decisions on the public release of information.
- HSIN-CI is a USDHS-sponsored, regionally based, trust-building, and information-sharing portal. With more than 40,000 business/private-sector and State and local government members, HSIN-CI should be replicated throughout the Nation.
- Critical infrastructure information sharing is key to ensuring the reliable delivery of infrastructure services:

— Many questions linger regarding the security of private-sector critical infrastructure information, its use by the USDHS, and the overall implementation of the Department's Protected Critical Infrastructure Information (PCII) program.
— The Government's Year 2000 information-sharing efforts provide a proven, secure, and trust-building model for exchanging critical infrastructure information.

- The ability to accurately model infrastructure operation and to provide a foundation for sound investments in CIR was demonstrated. Data derived from publicly available sources were mapped and, in addition to providing targeting data, provided cost-effective measures for eliminating choke and single points of infrastructure and commercial failure:
  — Current and emerging technologies can provide for comprehensive, multisector infrastructure instrumentation, real-time performance visualization, and automated decision enhance to support the reliable delivery of critical infrastructure services.
- Infrastructure and business resiliency efforts are growing both domestically and internationally. Numerous American businesses make the business case for and are engaged in business continuity and resiliency efforts.
- The United Kingdom, Italy, Singapore, and France have either ongoing or emerging Cabinet-level national resiliency programs.

April 25–26, 2005—Naval Postgraduate School: Monterey, CA

Objective: Because private-sector critical infrastructure representatives own and operate 85% of the Nation's critical infrastructure, meet with them to determine business methodologies that support CIP and business continuity-related operations. Additionally, receive an update on the U.S. Department of Defense's (DoD's) mission assurance initiative and its critical infrastructure education efforts.

Meeting Summary: There were presentations from and discussions with representatives of critical infrastructure sectors, including:

- Banking/finance
- Transportation
- Food
- Petroleum
- Energy
- Aerospace manufacturing
- Soft targets (e.g., hotels, shopping centers, cruise lines, and high-population density events

Presentations covered:

- CIR modeling
- Naval Postgraduate School (NPG) Defense and Civil Critical Infrastructure Programs
- DoD critical infrastructure initiatives

Task Force Observations:

- All of the sector representatives supported CIP efforts, but noted that protection was the foundation of larger business continuity and disaster planning efforts.
- Prevention is the priority. "Paying for prevention is better than paying for recovery."
- Businesses must be proactive, and not wait for government mandates. "Business has only two homeland security colors—open and closed."
- Exercising disaster recovery and business resiliency plans is vital.
- Standards for business continuity include National Fire Prevention Association 1600, ASIS International, and Best Current Practices (BCP) Guidelines.
- The business case for investments in operational continuity (of which protection is a part) is made each day by companies that are in business to provide quality services while making a profit, expanding their businesses, and increasing shareholder value:
  — No business should want to be considered as having critical components.
  — The focus is to ensure that there are no critical nodes, which will better support business continuity and resiliency objectives.
- Managers of soft targets want to test breakthrough technologies to stop 13 types of terrorist attacks:
  — There are many offers of technology from companies claiming strong accomplishments. The following is a good 3-question test:
    ▸ How many have been sold to Israel?
    ▸ How many are being used to protect troops in Iraq?
    ▸ "If I shoot a suspect based on an indication from a product—will the company stand behind it?"
- Resiliency modeling involves:
  — CIR modeling data derived from publicly available sources.
  — Identification and assessment of bottlenecks, points of maximum consequence, and tolerance of loss.
  — Time—the objective measure for investing in, achieving, and maintaining business, operational, and infrastructure resilience.

- The NPG offers State, local, and private-sector officials free (or at least partially USDHS-funded) critical infrastructure information and assessment courses:
  - — NPG officials acknowledged the need for CIR.
- DoD has always been focused on operational continuity and mission accomplishment:
  - — DoD critical infrastructure programs are moving their focus from protection to mission assurance.
  - — Critical infrastructure operation is essential to all defense operations. Protection is fundamental, but not sufficient to ensure the reliable provision of interdependent critical infrastructure services on which DoD relies (but does not own).
  - — The NPG Defense and Civil Critical Infrastructure Programs are looking to build resiliency in infrastructure systems. They are working with the USDHS Office of State and Local Government Preparedness and Coordination and providing free infrastructure network analysis tools to support critical infrastructure investment decisions.

June 21, 2005—The Federal Reserve: Washington, DC

Objective: Investigate USDHS and other Federal, regional, State, local, and private-sector critical infrastructure-related policies, efforts, and objectives.

Meeting Summary: Discussions with the USDHS Assistant Secretary for Infrastructure Protection were held. Presentations by Federal, regional, and business resiliency representatives were given on topics that included:

- Strategic direction of USDHS critical infrastructure efforts.
- Regional assessment methodologies.
- State economic growth and business resiliency initiatives.
- International infrastructure and economic resiliency requirements.
- Federal Reserve initiatives.
- Department of Energy electrical transmission research and development (R&D).
- Enabling legislation—review of Sarbanes-Oxley Act.
- USDHS Critical Infrastructure Protection Decision Support System (CIPDSS).

Task Force Observations:

- There is recognition of past organizational problems, and a fundamental and strategic redirection of infrastructure protection is underway. However, the organization is still focused on and struggling with an important national objective—protection:
  - — "What is enough to maintain a steady state of protection?"
  - — Resilience provides that which has eluded CIP efforts since their inception—time.
- USDHS/CITF representatives recognized that there is a lot of work to be done to make the National Infrastructure Protection Plan a viable/executable document, including the incorporation of:
  - — Robust private-sector engagement
  - — A risk-based approach (threat/vulnerability/consequence) to infrastructure programming
  - — The need to fully integrate cyber and physical infrastructure planning
  - — Integration with Homeland Security Presidential Directives and strategic plans
- The various sectors of an infrastructure rely on each other for successful operation:
  - — Federal governance mechanisms need to be established that recognize the reality of infrastructure ownership and operation, as well as their geographic concentrations and national economic consequences.
  - — Traditional sector-based, node-centric assessments are constructive but not sufficient.
  - — Regional assessments recognized "submerged risks" (e.g., the common use of exploitable infrastructure nodes and multiple companies relying on the same facilities/support).
  - — Regional assessments support business resilience and "adaptive capacity building" (e.g., hotel space used as hospital rooms).
- The Federal Reserve provides a model for sector-specific efforts, and has accomplished the following:
  - — Led the financial sector through the Year 2000 transition:
    - ▸ An information-sharing and national trust-building effort whose success has not been fully recognized or leveraged.

- Continuous "Contingency in Depth" planning and no-notice exercises are conducted throughout the Federal Reserve system, resulting in continuous improvement within the sector and, by extension, the Nation's economic resilience.

- There is an immediate need for investment in critical infrastructure R&D:
  - The electrical grid is overtaxed, consequence-amplifying, and increasingly vandalized.
  - The Nation is spending $25 million per year on electrical transmission R&D. Approximately the same amount is spent on dog food research and advertising.
  - New technologies (e.g., carbon fiber lines and large battery backup) are available, or can be made available, to ensure reliable delivery of electricity.
  - China is undercutting the price of coal. America is becoming dependent on Chinese coal, which is a threat to the U.S. coal industry and potentially the Nation.
- Sarbanes-Oxley legislation:
  - Business judgment, due care provisions, and specifically Section 409 are fostering increased Chief Executive Officer knowledge about corporate dependencies and enterprise risks.
- Convergence of Federal, regional, State, local, and private-sector infrastructure efforts is essential:
  - Continuing the security-by-sector approach is insufficient.
- CIPDSS is a Federal/national lab effort:
  - There is no objective measurement of how much protection is enough.
  - There are questions regarding CIPDSS relationships with existing assessments (e.g., DoD's Balanced Survivability Assessment) and other USDHS assessment development efforts (e.g., Risk Analysis and Management for Critical Asset Protection), as well as the assumptions made in creating CIPDSS models.

August 25, 2005—The Federal Reserve: Washington, DC

Objective: Continue investigation into USDHS and other Federal, regional, State, local, and private-sector critical infrastructure-related policies, efforts, and objectives; continue CITF deliberations.

Meeting Summary: There were presentations for and discussions with Federal, regional, and local officials, and a State Homeland Security Advisor on topics that included:

- A national infrastructure resiliency initiative
- State and county CIR resiliency initiatives
- The Joint Staff perspective on critical infrastructure
- U.S. Navy Year 2000 (Y2K) lessons learned
- Regional transportation resilience

Task Force Observations:

- There is clear financial sector recognition of the need for resilience, the realities of interdependency, and the consequences of infrastructure service loss (regardless of the cause):
  - Some things just have to work."
  - It is possible to create "Critical Infrastructure Resiliency Zones" throughout the Nation.
- Critical infrastructure operations are often highly concentrated in low-population regions of the Nation:
  - There are many significant, high-consequence-producing, single points of infrastructure failure whose cascading consequences will be national in impact.
  - Consequences of loss must be measured in economic as well as human costs.
  - Infrastructure operation is regional, State, local, and in many cases international.
  - In addition to traditional sector issues, infrastructure assessments must include geographic and political realities.
- The Navy's Y2K transition experience demonstrated the need for (in some cases) the utter reliability of critical infrastructure operation:
  - Y2K was not about fixing anything, but rather about the continuity of Navy and DoD operations during a period of combat operations, and the potential for the diversion of significant operational resources to deal with the potential human and national effects of Y2K.
  - Recognizing that infrastructures are targets, the Navy created and is currently employing a planning tool called "Mission Dependence on Infrastructure" (MDI).
  - MDI supports DoD's mission assurance focus and requires the integration of critical infrastructure knowledge, including threats, vulnerabilities, and consequences of loss, into Navy operational planning.

- Regional transportation resilience is essential to the rapid response to and recovery from any catastrophic event:
    - In a crisis, local transportation assets can be easily overwhelmed.
    - Regional transportation operational resilience is dependent on the operational resilience of regional infrastructure(s).
    - Information sharing is vital. Years have passed since September 11, 2001, and there is still no fully integrated, reliable means of passing timely, unclassified, and actionable homeland security information to transportation authorities.
    - Continued evaluation and testing of critical infrastructure regional capabilities (not only the local and critical infrastructure sectors) is mandatory.
    - Federal help is needed to accelerate the coherent development, testing, integration, and execution of regional assessment methodologies.
- Analysis of the London bombings showed that even in the United Kingdom, a large amount of information was available to assist terrorist planning:
    - There are indications that the information was exploited.
    - Experience with the Irish Republican Army, the population's historic resilience, and highly trained and frequently tested first responders minimized the consequences of the attack.
- Modeling data are constantly improving and can be used to proactively identify and help prevent or respond to an attack or infrastructure failure.

Appendix C

SUBJECT-MATTER EXPERTS—GOVERNMENT

Robert Stephan, Assistant Secretary, Infrastructure Protection, USDHS

COL Bruce Beebe, Joint Staff

William Bryan, Director, Critical Infrastructure, Office of the Secretary of Defense

James Caverly, Infrastructure Coordination Division, USDHS

Tom Dinnano, Acting Deputy IP, USDHS

SSA Art Fierro, FBI/USDHS, Director, HSIN-CI

Dr. Mary Ellen Hynes, CIP Portfolio Manager, S&T Organization, USDHS

Steve Malphrus, Staff Director, Board of Directors, Federal Reserve Bank

Colonel Mike McDaniel, Michigan Assistant Adjutant General for Homeland Security

William Parks, Transmission Reliability Office, Department of Energy

SUBJECT-MATTER EXPERTS—PRIVATE SECTOR

Richard Arns, CEO, The Security Board

David Barron, BellSouth Corporation

Tom Bozek, Former Director, DoD Critical Infrastructure Protection, Office of the Secretary of Defense, and President, Bozek Consulting, LLC

Hank Chase, Director, Smart Business Consulting, Smart and Associates, LLP

Dennis Dorsey, Director of Security, Northpark Mall, Dallas, TX

Jeff Friedland, Director of Emergency Services, St. Clair County, MI

Shawn Gorden, County Executive, St. Clair County, MI

Dr. Sean Gorman, Infrastructure Mapping Project, George Mason University, VA

Robert Greenberg, G&H International Services, Inc.

Stephen Iannucci, Vice President, Crisis Management, Citigroup

Leo McCann, Business Continuity Manager, American Electric Power

Melinda Metzger, Deputy Executive Director, PACE Suburban Bus, Chicago

Bill Ramsey, McCormick & Company

Jeff Reed, City of Danville, VA

James Savage, Chief of Security Operations, Hunt Oil Co.

Joe King, Assistant City Manager for Utilities, City of Danville, VA

David Shepherd, Director of Security, The Venetian Hotel, Las Vegas, NV

Rick Stephens, Sr. Vice President, Boeing Corp.

Mr. Steve Trevino, President, Global Resiliency Inc.

Dr. Penny Turnbull, Sr. Director Business Continuity, Marriott International

Jack Williams, President and CEO, Royal Caribbean & Celebrity Cruises

Appendix D

A Methodology for Critical Infrastructure Resiliency

Dr. Sean Gorman, Infrastructure Mapping Project,
George Mason University

The first step in any comprehensive plan for ensuring the resilient operation and reliable delivery of services is the establishment of a methodology by which standards and metrics can be set. There needs to be a common methodology by which stakeholders can objectively quantify investment in business continuity by measuring resiliency. What follows are proposed initial steps towards establishing such a methodology.

Infrastructure Resiliency Assessment

One of the significant obstacles in dealing with critical infrastructure is assessing and setting baselines for large and com plex networks. Further, the most critical of infrastructure assets are often interdependent on one another. Fortunately there has been considerable work accomplished on methods for assessing and quantifying critical infrastructure. Infrastructures can be assessed based on several factors, a few of which include:

- Density – how much infrastructure is there in any discrete location – i.e. 15 fiber optic conduits, 3 electric transmission lines, 2 gas pipelines.
- Capacity – how much volume, flow, or traffic are the infrastructures in any discrete location able to handle – i.e. the fiber lines have a 10 Gbps[1] capacity, the electric transmission lines are 720 Kv, and the gas pipeline are 42 inches in diameter.
- Bottleneck identification – algorithmic approaches to identify areas with high amounts of capacity but little diversity to route it.
- Structural analysis – another algorithmic approach that calculates all possible paths across an infrastructure and finds those discrete locations that are most frequently used in routing.
- Weighted structural analysis – expands the all possible path analysis to include to identify those locations are frequently used in routing and have low levels of capacity, or alternative routing paths in the event of failures that could be under capacitated.
- Interdependency:
  - Collocation – two or more infrastructures are located in the same discrete location.
  - Structural – the most frequently utilized routing paths of two or more infrastructures are located in the same discrete location.
  - Functional – the loss of one infrastructure will cause failures in a dependent infrastructure – i.e. the loss of electric power causes traffic light failures resulting in cascading traffic congestion, further infuriating commuters and hampering emergency response.
- Cost – creating a baseline figure of cost for the infrastructure in its current configuration – i.e. the cost of leasing fiber per month from a network provider.

While these are but a few of the possible approaches to assessing infrastructure(s), they provide the basic aspects of infrastructure components that are important to understand. Each separate assessment provides a list of locations and assets that could be critical to the operation of one or multiple infrastructures.

Verification

There a multitude of ways to assess infrastructure and identify potential vulnerabilities, a few of which were identified in the preceding section. There needs to be a means to identify which approach works best in each environment through a verification process. One means of verification is failure simulation. Once an infrastructure has been assessed and the most critical components identified and ranked, a failure of each component can be simulated. After the failure impact can be charted and subsequently compared to other components to verify their criticality. Would the failure of a location with the highest density of infrastructure cause more impact than an area with the highest capacity, or would a failure at a bottleneck cause the greatest repercussions? Failure simulation provides a means to verify the criticality of any of these scenarios to the continuity of the infrastructure. Once baseline verification has been performed, a combination of assessment methods can be investigated. For instance, the greatest impact to continuity could

[1] Gigabyte per second (OC-192)

come from the most frequently used routing path that contains a high density of three different infrastructures.

A second aspect that needs to be considered in a verification process is after an initial failure the structure of the network changes. What was once the second most critical asset in the network may now be different. To determine if it has or not a combinatorial optimization needs to be run where after the first failure has occurred all possible second most critical assets are tested to determine the second most significant asset. In the best case scenario, real time analysis can be performed to react to failures and determine how to best allocate resources in the network, but proactive analysis is still critical to ensure continuity.

Consequence

Since the Nation's enemies are actively seeking to inflict maximum and lasting psychological, physical, and economic consequences, an integral part of both assessment and verification is determining what the consequences of a failure are. Consequences can be calculated through a variety of methods and ultimately are specific to an individual scenario, the infrastructure involved and the users dependent on it. That said, there are some broad areas into which consequence can be categorized:

- Population affected – how many people will be affected by a failure or lack on continuity in an infrastructure – i.e. after a transmission line failure and subsequent blackout how many people will be without power.
- Businesses affected – how many business locations will be affected in a failure scenario for aggregation purposes these consequences can be grouped by Standard Industrial Classification (SIC) or North American Industrial (NAIC) codes.
- Traffic affected – whether it is packets, power, commodities, dollars, oil or electricity, each physical infrastructure has traffic that flows across it. The loss of a physical infrastructure component can cause cascading loss across multiple operational realities.
- Interdependent infrastructures affected – what infrastructures with dependencies to a failed infrastructure will be impacted by an event – i.e. a transmission line failure causes the failure of a transportation node, or the closure of shopping centers, schools and businesses.

These are just four broad categories under which consequence could be grouped. For specific critical sectors, consequence can be more narrowly defined and quantified. Operation traffic needs to be mapped to physical infrastructure allowing detailed calculation of consequence to both populations and businesses. Once consequence has been measured it is possible to attach a dollar figure and a probability of that consequence, which can in turn establish a justified level of investment in resiliency.

Fiscal Evaluation

Establishing cost metrics to determine the optimal level of investment into resiliency is a two-step process. The first step is determining the warranted level of investment into resiliency and the second step is maximizing the return on that investment. Each step follows the metric guidelines discussed above, conducting a resiliency-based infrastructure assessment to determine vulnerabilities and quantifying the potential impact of their successful exploitation. An important missing step is determining the probability of a vulnerability exploit. Determining probability gets out of the main scope of this methodology requiring resiliency-focused intelligence gathering, threat assessment, and prediction, but it is critical to making an accurate assessment of warranted investment. In its simplest form the investment calculation would be:

$$\sum_{ij} cve \times \left[\sum_{ij} pve \Big/ \sum_{ij} ve \right]$$

cve – cost of vulnerability exploit
pve – probability of vulnerability exploit
ve – vulnerability exploit

As an example, a fiber network operator discovers ten vulnerabilities in the network that meet their threshold as critical. For each vulnerability in the network, the operator determines the number of lit buildings that would be affected and the subsequent financial loss of the service outage—for this example a total of $20,000,000 for all ten scenarios.

For each vulnerability, a probability of an exploit is then gauged. Investment to mitigate each vulnerability can be accomplished on an individual basis or aggregated on average. In the averaging scenario seen in the equation above the average

probability of all exploits is 5.2% for all ten scenarios. When these numbers are included in the equation an investment of $1,040,000 is warranted to mitigate the vulnerabilities. Further analysis can be made as to how much money of that figure to spend on each vulnerability through dis-aggregation of the analysis. This is the most rudimentary form of a possible analysis and there is considerable room to create more sophisticated equations and approach to quantification

Scare Resource Allocation and Maximization

The second part of analysis is calculating the return on investment from the money allocated and determining how best to maximize it. To accomplish this task the resiliency of the network must be quantified. There are several possible approaches to quantifying resiliency, but for the sake of simplicity the structural analysis approach outlined earlier is implemented. In a structural analysis all possible routes across an infrastructure are calculated, then the number of times a discrete location is used in all possible routes across the network is analysis for a regional infrastructure is illustrated in Figure 1.

In each geographic segment of the network the criticality of the network is analyzed using the structural assessment, then indicated by a color code. In the visualization above the most critical segments of the network are indicated by white, then red, orange, yellow, green, and tan. The analysis clearly illustrates the large bottleneck between the top and bottom halves of the infrastructure. A baseline can also be calculated of infrastructures, the current resiliency based on the calculated. An example of such an number of routes available to infrastructure. After a failure the average route length can increase, the number of available routes can decrease, and parts of the network can be disconnected. It is also critical to understand how multiple infrastructures can interact with each other from both a geographic and functional perspective. The figure below depicts a second infrastructure overlaid on the first infrastructure analysis, so that a spatial interdependency analysis can be performed.

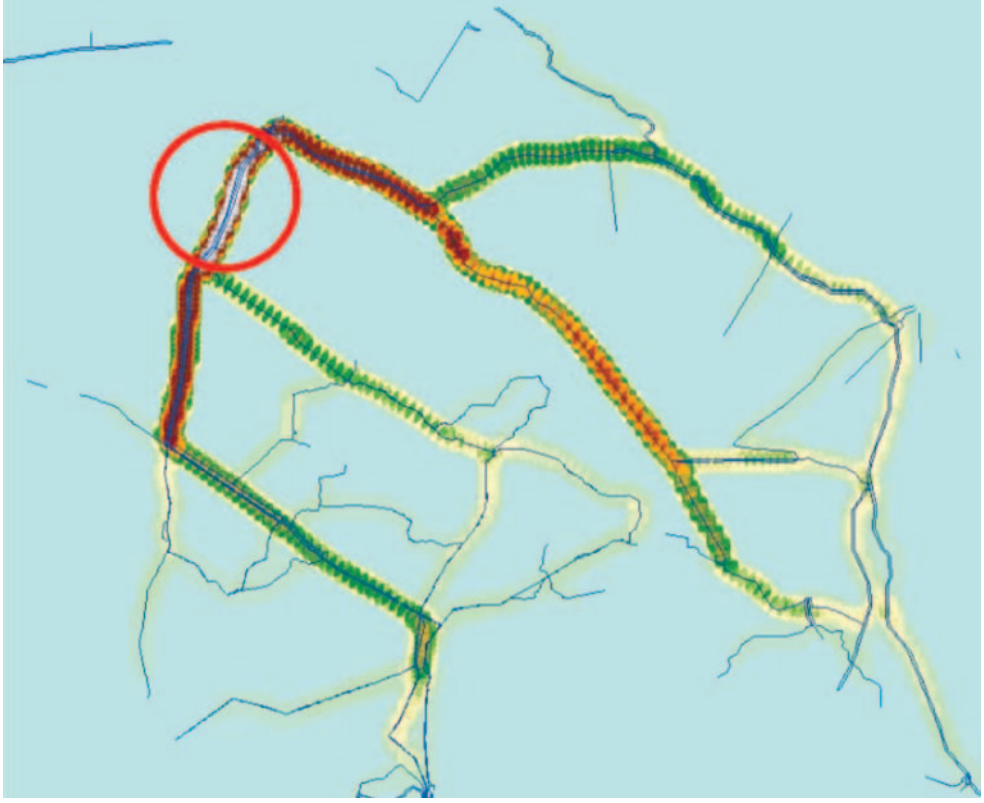


Figure 1: A Structural Analysis of Regional Infrastructure.

[2]Functional interdependencies are not covered in this brief overview, but failure probability surfaces can be utilized to determine when assets of interdependent infrastructures will be affected by a failure. This does require an ontology of functional relationships between infrastructures along with temporal parameters. The national labs and several universities have done significant work in this area.

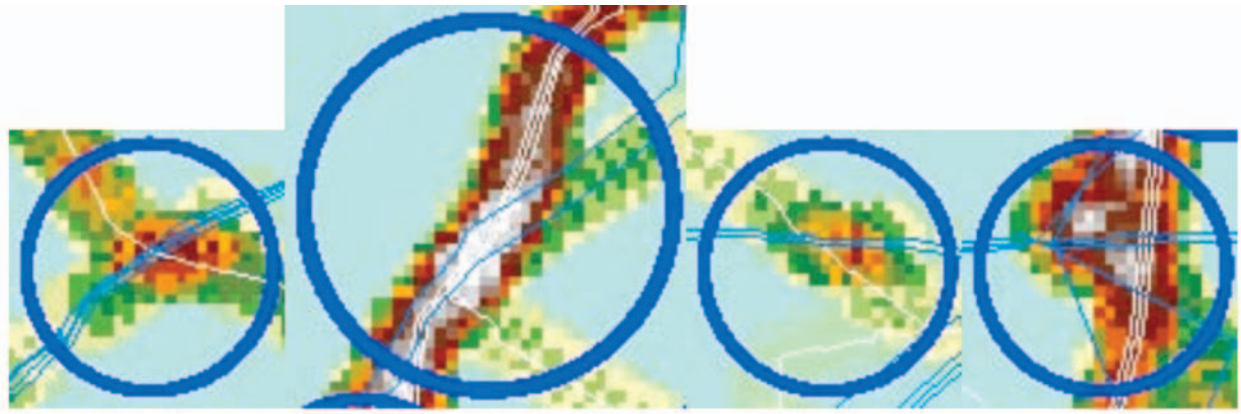


Figure 2: Structural Interdependencies of Two Networks.

In the spatial interdependency analysis the structural criticality of both networks is calculated, then areas are identified where there are both high levels of criticality and physical collocation. While there are four areas of high criticality there are also several areas of collocation that are not significant. This allows a straightforward method to illustrate interdependencies and identifying which are most critical. The technique also provides the opportunity to identify possible alternative routes for increased resiliency and diversity. Right-of-way collocation can sometimes cause infrastructure vulnerabilities, but often they can also be used to diffuse them. The blue network provides a second route to connect the upper and lower half of the white network. Figure 3 illustrates the addition of this route to the network and a recalculation of the network's structural criticality.

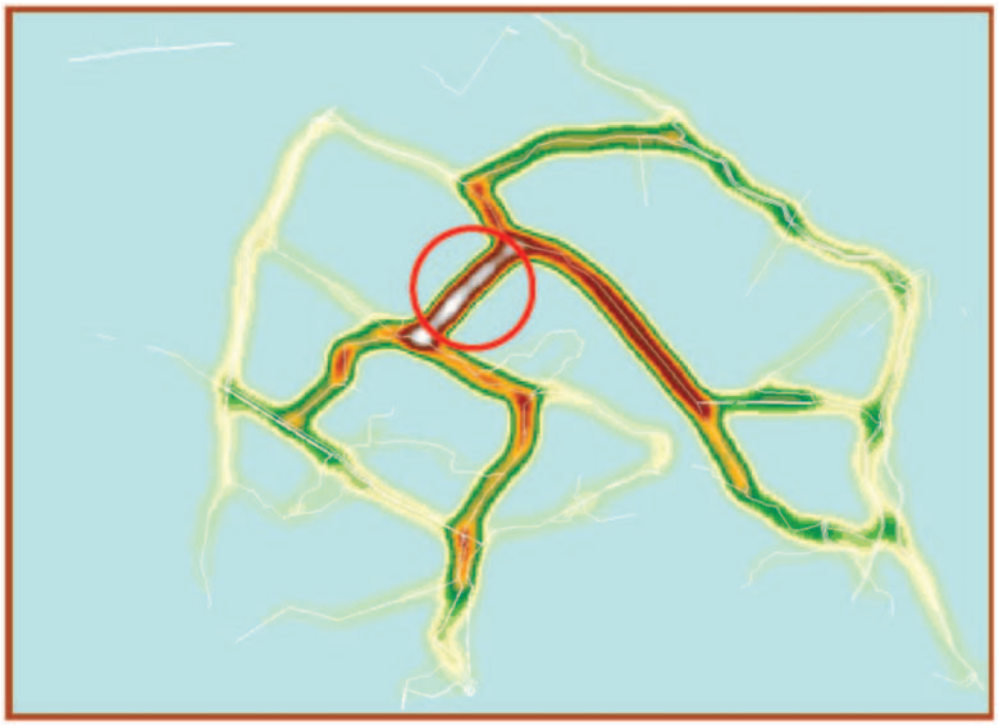


Figure 3: Route Mitigation and Analysis.

The red circle identifies the additional route added, which now provides a method to route around the previous bottleneck. The mitigation increases the resiliency of the network 14.96% through the additional route diversity added to the infrastructure. The mitigation also increases the efficiency of the network by decreasing the average route length in the network.

Trenching and building an additional route varies in cost by the environment and infrastructure, using a proxy of soft earth builds the average cost is around $50,000 per kilometer. The mitigation in the scenario above was 15.6 km, and would cost roughly $780,000. Thus from a cost perspective it could be estimated that there was a 1% increase in resiliency per $52,139 spent. This baseline can then be used to compare other possible mitigation strategies to determine which provides the greatest return on investment. If multiple mitigation possibilities are available, a portfolio analysis can be used to find the optimal combination within a specified budget.

The structural analysis also illustrates a reduction in the criticality of the old route, but also a heavy emphasis on the criticality of the new route. This can be clearly seen when the difference in connectivity is calculated before and after the addition of the new route as seen in Figure 4.

The greens and oranges illustrate areas that have lost criticality and the dark reds and maroons are areas that have gained in criticality. The mitigation has effectively diffused vulnerability in the old route and provided a second route to keep all the critical assets in the previous failure connected. These types of analyses can also be connected to public policy initiatives to help increase resiliency in critical infrastructures at the national, regional, and local levels. Structural analysis is just one approach to quantifying resiliency; several other approaches are available depending on the nature of the infrastructure involved. The model can also easily incorporate the mapping operational data for more refined and even real time analysis specific to any one or multiple interdependent infrastructures.

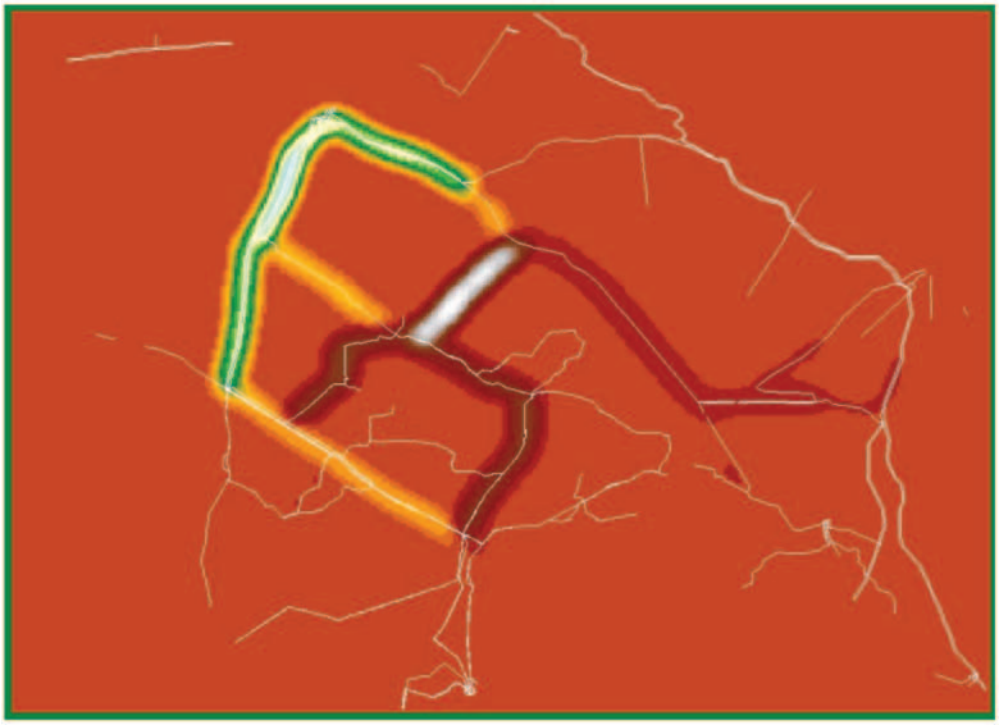


Figure 4: Visualization of the Impact of Network Mitigation.

Combining these approaches to infrastructure assessment provides a flexible methodology behind which to build metrics and set standards. The methodology can be broken into three areas: 1) operations 2) evaluation and 3) investment as seen in the following flow diagram.

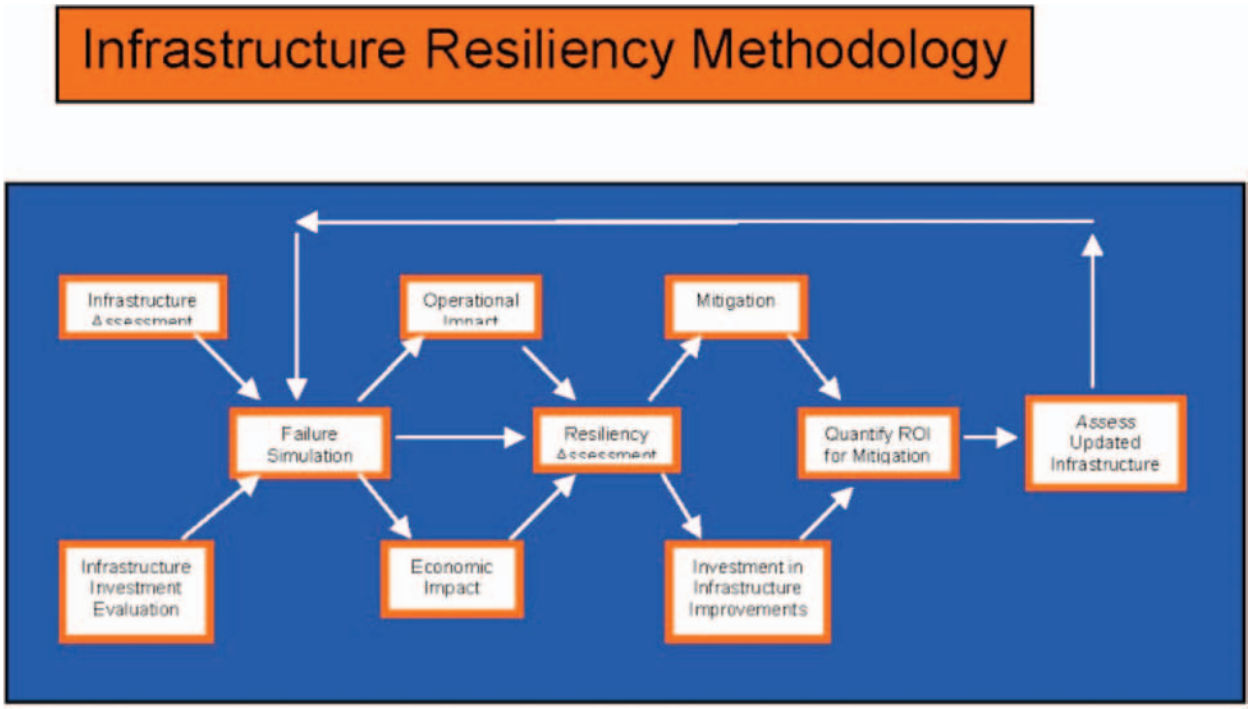


Figure 5: An Integrated Infrastructure Resiliency Methodology.

The diagram illustrates the flow of analysis discussed previously and illustrates how economic impact and investment assessment can be made at each step. This provides a means to quantify metrics in a common language all stakeholders can share. For any methodology to be successful it has to be flexible, adaptive and rapid enough to be utilized in crises as well as for strategic planning. What follows in the next section is an example implementation of the methodology in a simulated crisis of the Gulf Coast energy sector and the various interdependent infrastructures that constitute it.

INFRASTRUCTURE RESILIENCY METHODOLOGY

OPERATIONS
Infrastructure Assessment
Operational Impact
Mitigation

EVALUATION
Failure Simulation
Resiliency Assessment
Quantify ROI for Mitigation
Assess Updated Infrastructure

INVESTMENT
Infrastructure Investment Evaluation
Economic Impact
Investment in Infrastructure Improvements

Building Adaptive Real Time National Resiliency: A Case Study in Natural Disaster Preparedness

The Challenge

While there are several long-term challenges facing infrastructure security investment there is a pressing need to maximize the current resiliency of infrastructure. To take full advantage of the nation's current assets there is a need to be able to react in real time to crisis, disaster, and even day-to-day turbulence. The confluence of several technologies has created the possibility of real time adaptive decision-making abilities. To understand how new technologies can be utilized to solve real world problems a brief case study is useful.

Hurricanes Katrina and Rita were poignant reminders of not only the brittleness of the nation's infrastructure, but also the difficulty of adapting and reacting to failures of critical systems. The result was cascading failures that caused unprecedented human and economic loss. Many of the problems caused by the hurricanes revolved around the ability of the public and private sector to prepare and adapt to the damage caused by infrastructure failure. While the foundation of any solution to the problems, illustrated by Katrina and Rita, are rooted in changes in organizations, coordination, and communication, technology and approach can offer critical assistance for better preparedness and response.

The Scenario

Another Category Five hurricane enters the Gulf of Mexico this coming fall and appears to have a trajectory headed again for the coasts of Louisiana, Mississippi and Texas. Large swaths of human population lie in the storm's path along with critical energy assets that fuel the nation's economy. What follows is a description of how a combination of geo-spatial, distributed computing, and service-oriented architectures could be combined to minimize the impact of the storm and optimize recovery after impact.

As the storm enters the Gulf, weather feeds from NOAA are pulled over a service oriented architecture that allows a wide variety of disparate information sources to be pulled over the Internet in a common easily integrated format. The weather feed is pulled into a context sensitive common operating picture that identifies the current position of the hurricane, the area of likely landfall, and predicted wind speeds and storm surge.

From the federated national asset database a web services query is sent to pull in all the critical assets that could be impacted by the impending storm.

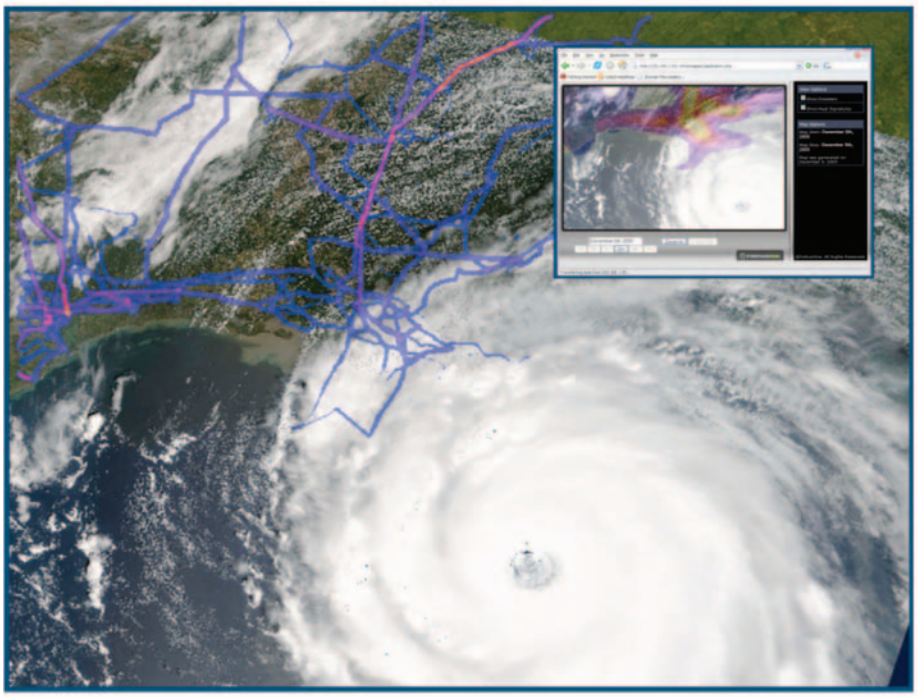


Figure 1. Interdependent analysis of energy infrastructure in the path of an approaching Hurricane delivered through a web browser. The areas in yellow (high) fading to blue (low) indicate critical junctures in the energy infrastructure vulnerable to the approaching hurricane.

A quick query is run to determine which sectors have the largest number of vulnerable assets based on the consequence of their loss in the possibly affected areas. The results illustrate that there is a potentially devastating loss to the energy sector based on exposure of oil and gas platforms in the Gulf as well as the pipelines on and offshore connecting production to refineries and storage facilities onshore.

The Analysis

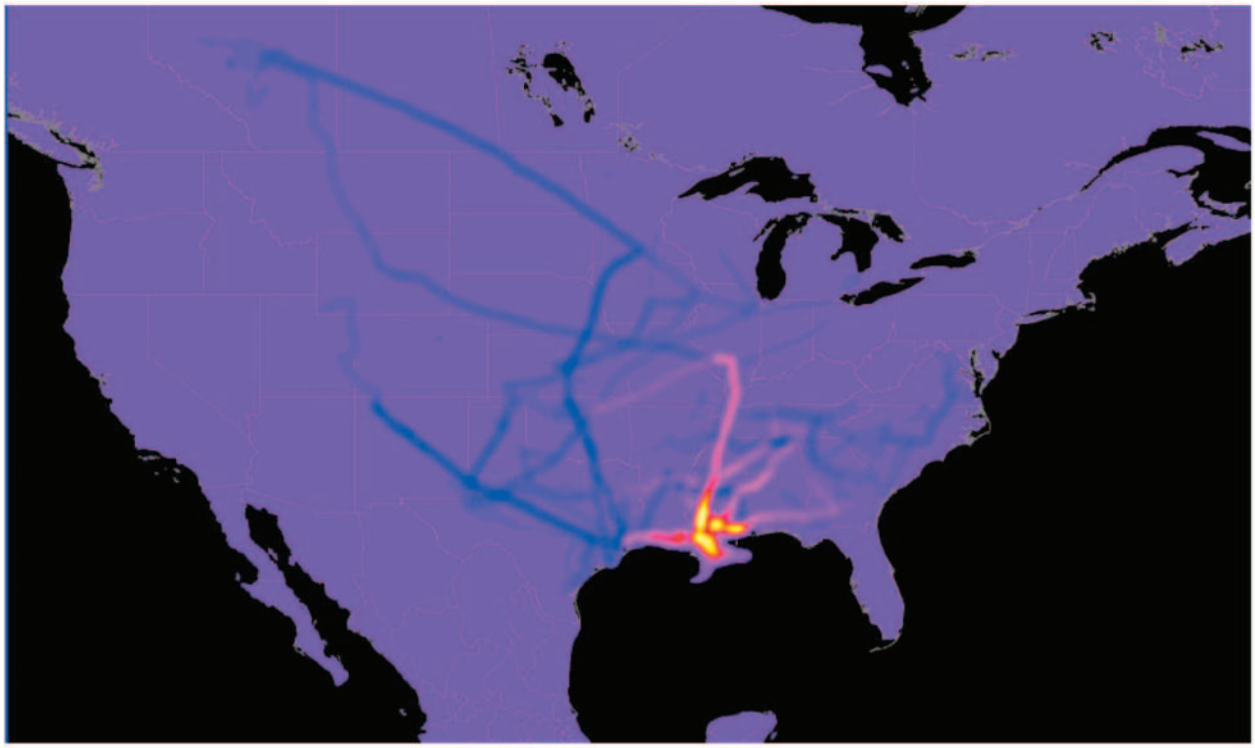
Having identified a high consequence sector a predictive failure simulation is run to determine how the interdependent energy infrastructures could be affected by the storm's impact. The system sends a simulation query to a distributed computing cluster that runs failure analysis on the nation's crude oil, refined product, LPNG, natural gas, and electric power transmission infrastructures. Analysis of the impact on each individual-infrastructure is returned in seconds along with the interdependent impacts of the failures.

In addition to maps indicating the areas of infrastructure loss and congestion reports are delivered indicating the specific assets impacted directly and indirectly through interdependent failures. The operational impact is predicted based on heuristics to determine the amount of energy capacity lost and time delay to move product because of the storm. The statistical analysis of the simulations provides a quantification of the impact at both the regional and national level.

Figure 2. Interdependent analysis of energy infrastructure simulating the impact of the approaching hurricane. The areas fading from purple (low) to yellow (high) indicate areas that have lost connectivity because of predicted damage by the storm. The areas in blue have become congested and caused delays because of rerouting around failed infrastructure assets.

New Orleans, LA MSA and Baton Rouge, LA

	Total Frequencies Before (in thousands)	Total Frequencies After (in thousands)	Change in Frequencies (in thousands)	Percent Change in Frequencies	Percent Change in Volume Transported
Crude Oil	13,373.3	4,507.2	-8866.1	-66%	-52%
LNPG	2,005.0	0	-2,005.0	-100%	-100%
Refined Products	10.0	0.042	-9.9	-99.5%	-99%



National

Infrastructure	Total Frequencies Before (in thousands)	Total Frequencies After (in thousands)	Change in Frequencies (in thousands)	Percent Change in Frequencies	Percent Change in Volume Transported
Crude Oil	536,678.7	483,653.6	-53,025.1	-10%	-6.5%
LNPG	173,767.7	151,226.3	-22,536.5	-13%	-12%
Refined Products	108,602.7	108,426.0	-176.7	-0.16%	-14%

Table 1. Regional and National Impacts of an Approaching Category Five Hurricane.

This analysis is further supplemented by functional interdependency analysis to identify assets that could fail because of their dependency on an infrastructure vulnerable to the oncoming storm. The map and table below illustrate functional interdependencies of critical energy assets with electrical power, but similar analysis could be done for telecommunications and variety of other critical services.

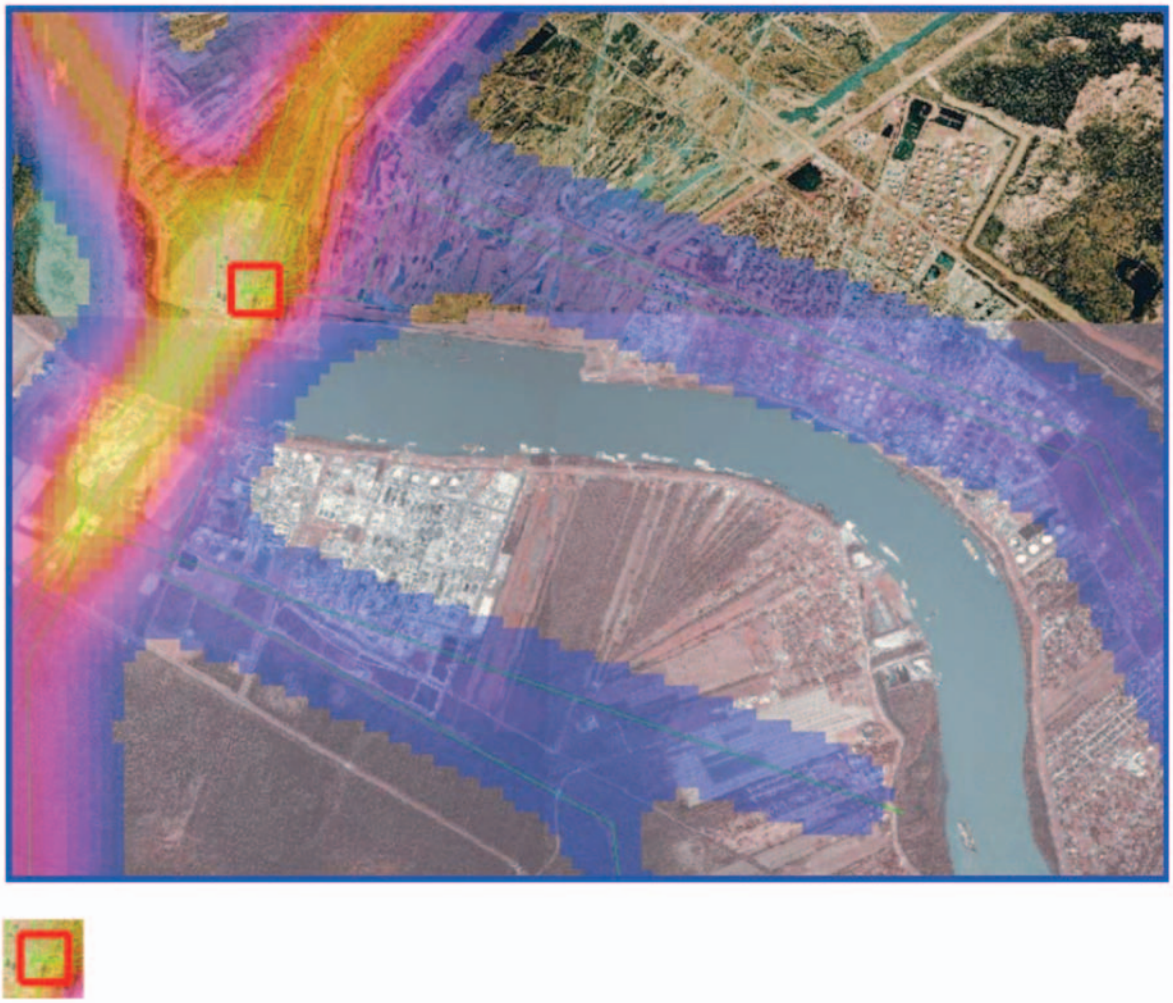


Figure 3. This image illustrates a large number of energy facilities that have a high risk of loosing electrical power because of their functional and spatial dependency on the highlighted power substation.

In addition to mapping the geographic effects of the power infrastructure failures key assets can be identified that are at high risk for failure because of their dependency on electric power.

FACILITY TYPE	COMMODITY
Delivery point to power plant	Natural Gas
Meter station	Natural Gas
Delivery point to power plant	Natural Gas
Meter station	Natural Gas
Meter station	Natural Gas
Industrial plant	Natural Gas
Compressor station or pump station	Natural Gas
Meter station	Natural Gas
Meter station	Natural Gas
Industrial plant	Natural Gas
Meter station	Natural Gas
Industrial plant	Natural Gas
Meter station	Natural Gas
Meter station	Natural Gas
Compressor station or pump station	Natural Gas
Compressor station or pump station	Natural Gas
Storage/tank farm/terminal	Refined Products
Storage/tank farm/terminal	Refined Products
Storage/tank farm/terminal	Crude, Refined Products
Refinery	Crude, Refined Products
Refinery	Petrochemical
Chemical plant	Natural Gas, Petrochemical
Industrial plant	Natural Gas, Petrochemical
Chemical plant	Natural Gas, Petrochemical
LPG fractionator	LPG/NGL
Gas processing plant with NGL	Natural Gas, LPG/NGL
Meter station	Miscellaneous
Meter station	Miscellaneous
Compressor station or pump station	Miscellaneous
Industrial plant	Miscellaneous
Storage/tank farm/terminal	Crude, Refined Products, Miscellaneous
Chemical plant	Petrochemical, Miscellaneous
Chemical plant	Petrochemical, Miscellaneous
Chemical plant	Natural Gas, Petrochemical, Miscellaneous
Chemical plant	Natural Gas, Petrochemical, Miscellaneous
Refinery	Crude, Refined Products, LPG/NGL, Miscellaneous
Chemical plant	Petrochemical, LPG/NGL, Miscellaneous
Refinery	Crude, Refined Products, Petrochemical, LPG/NGL

Table 2. A list of assets that have a high likelihood of losing power because of the failure of the substation in the previous image.

From this analysis a handful of key energy providers are identified that will both be hard hit by the storm and if not prepared could have a significant impact on the nation's economy. Once these firms have been identified, the system sends a request to the critical energy providers to help coordinate mitigation strategies along with access to simulation results to quantify the threat to their business. With the permission and cooperation of the impacted private sector firms' real time queries can be made by the system to determine where there is possible available storage capacity and line-packing outside the impact of the storm. Since the analysis and information sharing can be done in minutes there is enough lead-time to coordinate resources for a better evacuation of slow moving reserves and product out of the impacted region to avoid fuel shortages and outages across the nation. The approach can also be used to determine multi-modal means to move product using alternative transportation like road, rail, and waterways.

Resilient Recovery

The pre-positioning assets can also improve recovery from the storm. An analysis of areas likely to suffer power outages from the storm's impact can be used to determine where to locate diesel generators and fuel to allow operations to continue until power is restored. In the case of the energy sector diesel generators and back-up fuel can be pre-positioned at the refineries and pumping stations likely to suffer power failures. This allows production and distribution to be resumed quickly with facilities and assets that are still operational. Building on the previous example critical facilities in need of pre-positioned generators are identified.

Similar analysis could be used for the pre-positioning of mobile telecommunications assets, emergency supplies, construction material, and a variety of other key recovery assets.

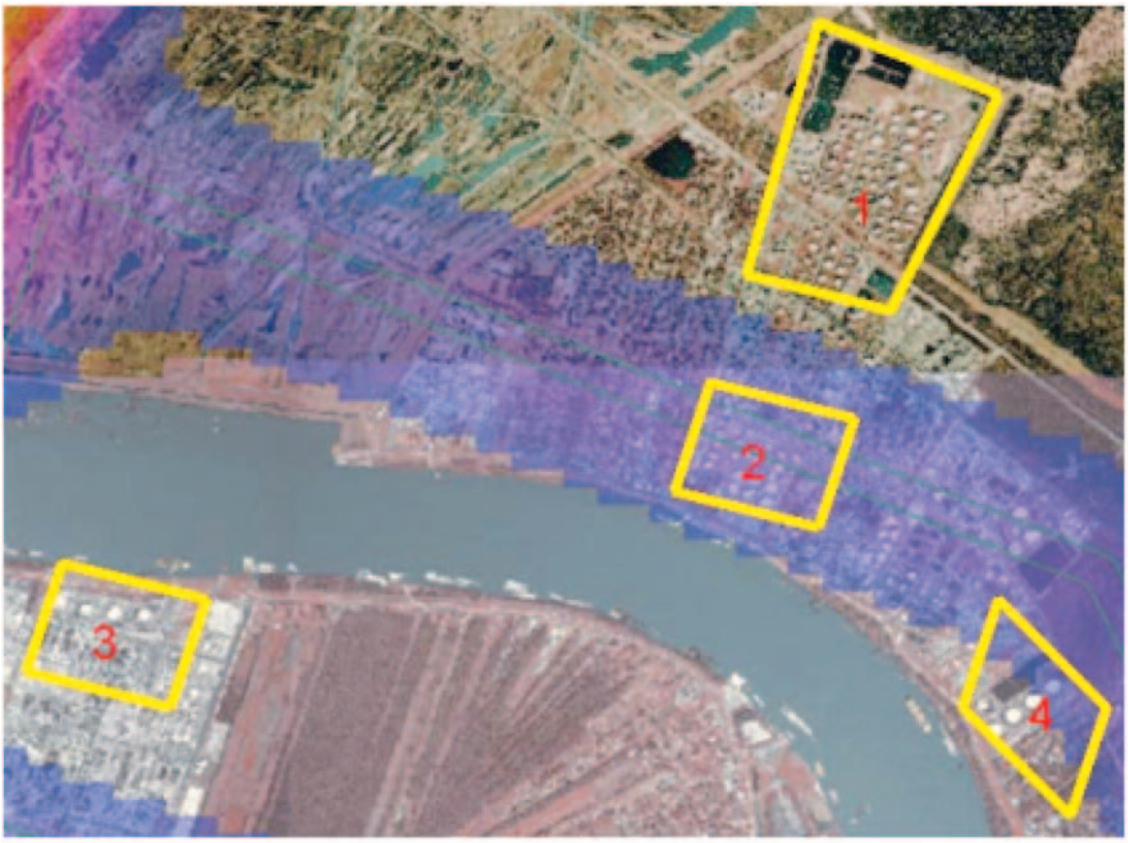


Figure 4. The yellow squares indicate facilities that have a high risk of power failures and the prioritization of diesel generator allocation to ensure a minimization of downtown and rapid recovery of key critical energy assets.

Conclusion

The examples provided are just one example of how available technology can be used to maximize the resiliency of current infrastructure systems and assets. While long term investments are needed to further enhance and build resilient infrastructures for the future, it is imperative that the nation become better prepared to leverage current capabilities to minimize the impact of catastrophes and crises. While the example provided for this scenario was the energy sector, the same approach could be used for all critical infrastructure sectors. A similar approach could be utilized to determine optimal paths for evacuation routing, determining the best paths for emergency vehicles, the best allocation of resources for rebuilding bridges and the optimal order for bringing key infrastructure assets back online. Once the capabilities and tools have been put in place decision makers and operational entities have the power to make rapid and adaptive decisions to maximize the use of their scarce resources. The ability to make key informed decisions in an agile real time environment is a critical function to effectively instill national resiliency and preparedness in the future.

Appendix E

Critical Infrastructure Resilience in Danville, VA

Danville, VA is taking the initiative not simply to prepare for catastrophes, but also to develop critical infrastructure sufficiently resilient to minimize, if not altogether avoid, service disruptions that commonly result from large scale natural and man-made disasters.

Danville, VA

Danville is a city of 46,000 in a metropolitan area of 107,000 inhabitants located in south-central Virginia, along the North Carolina border. Established in 1793 as a tobacco trading post, Danville grew to become the center of Virginia's large textile and tobacco industries. As those traditional industries declined, Danville has transitioned to a leading location for new businesses and industries. The city not only offers the typical array of municipal services, but is unique in additionally providing water, wastewater, natural gas, electricity, and telecommunications services.

The Project

Community resilience refers to the capacity to resist disaster damage and to recover rapidly from whatever damage has occurred. Traditional emergency management has focused primarily on preparation for and manage-ment of post-disaster response. With funding from the U.S. Department of Homeland Security (USDHS), the City of Danville and the Virginia Governor's Office of Commonwealth Preparedness have cooperated with Virginia Tech's Disaster Risk Reduction Program (DRR)* to go beyond this traditional approach and also assess the interdependencies and resilience of the City's four principal infrastructure sectors: communication, energy, transportation, and water/wastewater. The study used an all-hazards approach in examining infrastructure systems resilience and included: 1) an evaluation of current threats, vulnerabilities, and consequences of manmade or natural disasters affecting the four sectors, 2) an identification of key geographic, physical, electronic, and functional cross-sector interdependencies, and 3) a review of the city's needs for future system investments and management capabilities necessary to achieve and maintain a high level of infrastructure resiliency.

Assessment Approach

The DRR team relied on direct interactions with the personnel who know the systems best, using directed questions and discussions. DRR has evolved this approach over the past six years through a number of projects in which infrastructure personnel were interviewed regarding system security and system performance before, during, and after natural disasters.

The methodology employed by the DRR team to conduct the Danville assessment involved a 3-tier collaborative approach involving interviews and meetings with mid- and upper-level managers, engineers, and operations personnel. First, the DRR team met with representatives from individual infrastructure sectors to identify critical facilities and examine their characteristics, and to ascertain infrastructure interconnections and interdependencies. The integration of emergency management priorities in each sector's planning, operation, and budget was also examined. The DRR teams then met in a series of paired-sector meetings with personnel from two sectors at a time to further explore infrastructure interdependencies. Lastly, the DRR team convened a meeting of all sector representatives for a final review of collected information and findings. In all of three meeting tiers, discussions were guided by

*DRR is a multi-disciplinary applied research and implementation disaster risk manage-ment center at Virginia Tech's Advanced Research Institute in Arlington, Virginia. It includes natural scientists, engineers, architects, urban planners, economists, sociolo-gists, and policy analysts. DRR takes a systems approach to disaster management, including the identifi-cation of risks, reduction of risk through development of physical and operational mitigation measures, and risk transfer through the mechanisms of insurance and relief policy.

central topics and previously prepared questions. Discussions and analysis by the DRR team benefited greatly from in-depth access to the city's infrastructure information database. Geographic information system (GIS)-based maps, facility system diagrams, system capabilities drawings, and aerial photographs were used to facilitate cross-sector discussions during each meeting.

Products

The study produced three reports for local government executives and managers at the Governor's Office of Commonwealth Emergency Preparedness:

- A summary of the study methodology used in Danville, which will provide guidance to other local governments interested in assessing and improving their critical infrastructure resiliency (CIR).
- A report on further mitigation actions the City of Danville can take to enhance resilience and decrease system vulnerabilities in its four principal infrastructures.
- A report on Danville's capabilities to serve as a regional disaster recovery and back-up data security site for businesses, governments, and institutions located in identified threat zones of Washington, DC; the Richmond and Tidewater areas of Virginia; and the Piedmont area of North Carolina.

Follow-on Activities

At the completion of the study, the City of Danville intends to build on its existing partnership with the Commonwealth of Virginia and the USDHS to design and develop a specialized industrial and office park to accommodate firms within a half-day's travel from Danville that require a Resiliency Zone—a safe, highly reliable off-site location for parallel, redundant, back-up, and/or recovery and reconstitution facilities. The city will also propose development of a Community Certification Program to assist local governments exposed to a wide variety of man-made or natural disasters and vulnerabilities to maximize the resiliency of their critical infrastructure systems.

Additional Information

For further information on the project, contact

Dr. Fred Krimgold
Director, Disaster Risk Reduction Program
Virginia Tech
Advanced Research Institute
4300 Wilson Blvd., Ste. 750
Arlington, VA. 22203
(703) 387-6033
krimgold@vt.edu

Bob Newman
Deputy Assistant to the Governor for
Commonwealth Preparedness
Executive Office Building
1111 East Broad Street
P.O. Box 1475
Richmond, VA. 23218
(804) 692-2595
robert.newman@governor.virginia.gov

Ron Bunch
Economic Development Director
City of Danville
427 Patton Street
P.O. Box 3300
Danville, VA. 24543
(434) 793-1753
rbunch@discoverdanville.com

Joe King
Assistant City Manager for Utilities
City of Danville
1040 Monument Street
Danville, VA. 24541
(434) 797-8963
kingjc@ci.danville.va.us

Web Sites

The Disaster Risk Reduction Program at Virginia Tech
www.ari.vt.edu/drr

State of Virginia,
Office of Commonwealth Preparedness
www.commonwealthpreparedness.virginia.gov

Discover Danville
www.discoverdanville.com

City of Danville, VA
www.danville-va.gov

Appendix F

The Great Lakes Partnership: An Integrated Approach to Resilience and Recovery

In the four years since 9-11, public-private collaboration has been identified and endorsed by business and political leaders as essential to restoring continuity of operations in the wake of catastrophic incidents. This agreement on the "why" is now being strengthened by a growing consensus on the "how" of bringing key stakeholders together to plan for and act on disaster readiness and recovery. The Great Lakes Partnership, Ltd. (GLP) is one of several nascent organizations around the country that have formed to lead regional approaches to homeland security.

Founded in 2003, the vision of GLP is to ensure the economic vitality of the Great Lakes region through effective integration of security, sustainability and innovation. GLP's mission is to bring leaders together for cross-sector collaboration to assure the resilience of the region and test solutions for national, homeland and economic security challenges. GLP recognizes the need to advance our thinking from protection to resilience. Resilient infrastructures, communities, and businesses are a deterrent to attack because the consequences of attacking them are dramatically minimized. Resiliency also expedites recovery from natural disasters.

Why does GLP advocate a regional approach? The answer, in brief, is to foster a new culture between the public and private sectors, one that is grounded in deeper understanding of the impacts of global and regional interdependency. Disruptions, whether natural or man-made, bypass state and possibly national borders. The same is true of the critical infrastructures that support our economy and standard of living—transportation, communications and energy, to name a few. In the wake of Hurricanes Katrina and Rita and in the looming shadow of seemingly imminent pandemic flu, the need to act regionally and apply systems-based thinking to these challenges is even more compelling.

Among the benefits cited by advocates of regional public-private collaboration are:

- It enables the Department of Homeland Security and other federal, state and local agencies to readily reach the private sector that owns more than 80% of the nation's critical infrastructure. A network of regional partnerships would constitute a national system of leaders and experts at the ready when disruptions occur.
- Regional partnerships leverage public and private sector resources to more rapidly deploy best practices and minimize the potential for duplication and false starts.
- A regional approach expedites interaction among the emergency response community, NGOs and the private sector within and across the nation.
- Regional partnerships take into account the key sectoral dependencies--and attendant risks--unique to a region. While the complexity of key sector dependencies will vary across the nation's regional economies, the people we count on to manage them will be more effective when trust is built before crisis forces cooperation.

The Great Lakes region (defined as eight U.S. states and two Canadian provinces) illustrates the complexities. It is the third largest economy in the world. Its vast natural, capital and logistical resources make it the nation's most intense area of intra-regional commerce flow. Local communities across the United States depend on the goods and services that traverse the territory. The Great Lakes is uniquely defined by its environmental assets (e.g. 20% of the world's fresh water), financial markets, manufacturing and food distribution networks, energy grid and pipelines, transportation hubs, medical and research institutions and the world's largest internet exchange by volume.

For the past two years, volunteers from the public and private sector in Illinois and other Great Lakes states and Canada, have built the framework for a regional partnership. Earlier this year, GLP incorporated as a private not-for-profit organization, and is currently assembling its board of directors. Membership in GLP is open to government agencies, private companies and NGO leaders and experts representing the region's critical resources

and sectors. GLP is co-located with and managed by the Chicago Manufacturing Center (a member of the NIST MEP national network), which founded the group in collaboration with DHS-FEMA Region V and private sector leaders.

GLP will demonstrate its value to the nation's readiness, response and resilience infrastructure through pilot projects that test solutions and build a culture of resilience. For example, one project under consideration seeks to demonstrate an integrated global cargo security system that satisfies government's responsibility to regulate global shipping as well as industry's need to expedite transport. Another pilot in design will test a regional approach to the threat of a pandemic, encompassing not only public health and safety concerns, but also business issues around supply chain continuity, market incentives and cost. This approach seeks to expedite agreements on intellectual property to accelerate vaccine research and manufacturing capacity; address trans-jurisdictional health care and mutual aid concerns, and test the use of knowledge/information technology to support decision making and increase community based and business self sufficiency. A third pilot is focused on food supply chain security and resiliency.

In addition to these pilot projects, GLP is collaborating with the United States Business Council for Sustainable Development on issues surrounding the sustainability-security and lean resiliency nexus of business continuity. Also, GLP serves as a regional policy liaison and is sought as a voice in new policy review as well as a trusted intermediary between the public and private sector.

We are a nation at a pivotal stage in our history that is poised to either capture the full benefits of our open society and global economy or suffer greatly under the burden of inertia and a failure to change. Looking ahead to the likelihood of pandemics and reflecting on the Gulf Coast lessons, we are soberly reminded of the responsibility shared by all public and private sector leaders. That is, to ensure the resiliency of our infrastructure in all its dimensions, and, when catastrophe strikes, to reassure a more prepared public that their homes, workplaces and schools will be made safe and secure as quickly as possible. Regional public-private partnerships, with roots in local communities, can be trusted allies in fulfilling this mission.

For more information, contact:

Demetria Giannisis
President
Great Lakes Partnership
(312)542-0444
dgiannisis@cmcusa.org

Helen Gagel
Vice President
Chicago Manufacturing Center
(312)542-0446
hgagel@cmcusa.org

www.greatlakespartnership.com

Appendix G

Mission Assurance Governance Committee (MAG-C) Charter

Background

While often taken for granted, critical infrastructure operation – both cyber and physical – enable mission assurance and form the foundation, and the functioning of American society. Thus, the resilient performance of the Nation's interdependent Critical Infrastructure is essential to continuity of business and government operations, the success of military operations, the growth of the economy, social stability and the advancement of the Nation's freedoms and quality of life. Throughout history nations and all manner of armies have studied, and exploited their adversary's vulnerabilities and infrastructure failure points with the intention of inflicting harm by amplifying service disruption or destruction within and across their interdependent critical infrastructure(s). Accordingly, and especially in the wake of events before and since September 11, 2001, America must accept a dedicated enemy with global reach and in its midst is doing the same and views America's Critical Infrastructure components as accessible and "legitimate targets," and potentially a set of "Domestic Weapons of Mass Destruction" which it can exploit to inflict comprehensive, widespread, and lasting consequences on the Nation.

Despite these realities, America has continued to place its emphasis on iterations of a pre-9/11, defensive, unquantifiable, and largely static and highly stovepiped Critical Infrastructure Protection (CIP) structure and objective (protection) that is not aligned with historic business and government continuity of operations efforts; emerging global business and national resilience strategies, and the physical realities of critical infrastructure placement and operations. In the wake of 9/11 and in an interdependent environment, predictable efforts to physically protect critical assets are necessary but only a first step in preventing or minimizing the effects of attacks on or in dealing with a spectrum of critical infrastructure failure(s). In order to ensure the Nation is efficiently and effectively prepared to deal with the surprises the 21st Century has brought and will continue to bring, and to assure the success of business, government, and National Security operations, a pro-active, objectively measurable and sustainable national critical infrastructure objective based on equality of predator and defender perspectives, convergence with Private Sector business and Government preparedness and continuity objectives, and the realities of Critical Infrastructure operation is required.

Purpose

The MAG-C is forward-thinking interagency forum comprising critical infrastructure and mission assurance leaders from US Government organizations created for the purpose of improving agency practices, sharing information, and advancing a proactive approach to mission assurance and, by extension, national resilience. The MAG-C envisions cooperation and coordination among the myriad existing contingency and security programs, including, but not limited to:

- Critical Infrastructure
- Information Sharing
- Business Continuity
- Continuity of Government
- Continuity of Operations
- Counterterrorism
- Cyber Security
- Decision Support/Situational Awareness
- Crisis Management
- Emergency Management
- Enterprise Resilience
- Information Assurance
- Information Technology Disaster Recovery Planning
- Personnel Security
- Risk Management

MAG-C believes that these programs operate more effectively and efficiently to assure the mission of an organization when there is a collaborative, objectively measurable risk-based framework that provides for their coordination, planning, governance, and resource allocation.

MAG-C Mission
The MAG-C mission is to bring together the strengths and perspectives of its members to provide mutual support for developing mission assurance capabilities in their own organizations, and to support together the Federal Government's efforts to achieve sustained fulfillment of critical missions given the potential disruptions inherent in the 21st Century national security environment.

Membership
Members will be full-time employees of the Federal Government. Membership in the MAG-C is by invitation only. Any member of MAG-C can propose a new member; however, MAG-C Chairs must approve new members before invitations are extended.

Guest attendees may be invited to participate in meetings or activities at the consent of the members and Chairs.

Activities
The MAG-C shall be engaged in the following activities:

- Identify, share, and disseminate best practices, emerging technologies, and lessons learned to overcome the mission assurance challenges faced by member agencies.
- Develop a common perspective and approach among member agencies on the protection of shared critical assets to allow identification of shared vulnerabilities and support a coordinated response in the event of disruptions.
- Perform an awareness-raising function on behalf of practitioners and leaders seeking to implement change.
- Share information with related boards, councils, or governmental policy and standards entities, and nominate MAG-C members to serve in those groups.
- Solicit input from key groups of federal management and program officials, as well as industry, academia, and federal, tribal, and state and local governments, on matters of concern to the Committee.

Procedures
The MAG-C shall select from among its members, by majority vote, a Chairperson(s) who will lead committee activities. The Chairperson(s) will select a Vice-Chairperson to co-lead activities on behalf of the Committee Membership. Both the Chairperson(s) and Vice-Chairperson shall serve one-year terms.

The MAG-C Chairperson(s) will:

- Schedule meetings, develop the agenda, coordinate tasks and track completion of deliverables.
- Establish procedures for promulgating Committee decisions and resolutions.
- Select a recorder to take notes and develop meeting minutes, to be approved and distributed within 10 working days to all members.
- Appoint working groups as directed by the MAG-C to address issues. The working group leader will provide written reports addressed to the Chairperson to be included in the MAG-C meeting minutes.

Face-to-face meetings or conference calls will be held at least bimonthly, at times and locations agreed upon by MAG-C members. Special meetings, teleconferences and videoconferences may be called by the Chairperson(s) as necessary.

Sub-Committies
The MAG-C may establish standing sub-committees and working groups as necessary to consider items of interest or concern. Such sub-committees will investigate and resolve problems and will present solutions and options to the MAG-C within established timelines. Sub-committee leaders will be selected from among MAG-C membership.

Duration
This charter will be reviewed once annually and modifications must be approved by the Chairperson(s).

Mission Assurance Governance Committee (MAG-C) Co-Chairpersons

William Bryan
Director, Critical Infrastructure Protection
Office of the Assistant Secretary of Defense for Homeland Defense
Department of Defense

Curtis Bartell
Office of the Sergeant at Arms
U.S. Capitol

Appendix H

St. Clair, Michigan Regional Critical Infrastructure Resilience Initiative

Background

America's economic and national security and the welfare, opportunities and freedoms afforded its citizens are all highly dependent upon a vast network of highly complex, automated, largely privately owned and operated and inextricably interdependent national and global critical infrastructure systems and services. These critical cyber and physical infrastructures produce and distribute energy, enable communications, control transportation, ensure the availability of food, water, and emergency care, and moreover, provide every service and support every activity that defines and empowers America.

St. Clair County, Michigan, is unique for its combination of high concentration of critical infrastructure, relatively low tax base, and population. Sitting adjacent Ontario Canada's Chemical Valley, St. Clair County is the Nation's primary entry point for carriers of hazardous, radioactive, flammable materials between the United States and Canada. It is the second ranked entry point in the United States for hazardous materials imports, the second busiest northern border crossing in America and third-ranked commercial point of entry for the North American Continent crossing for 4,800 commercial trucks and 12,000 passenger vehicles daily and 5.8 million commercial and passenger vehicles annually. Thus St. Clair County is the Nation's principal gateway for international trade with Canada with 27% of total North American land-based international trade. Under the Blue Water Bridge carrying all commercial and passenger traffic pass 7,432 vessels carrying over 86,067,000 tons of product annually. Under the St. Clair River on which those freighters pass are approximately 30 pipelines that connect the U.S. and Canada. They carry a product value of greater than $2.1 billion (2004) and range in diameter from six to 48 inches.

Because of the above, publicly available information on the age of and both the isolation of some critical nodes and extreme density of others and the interdependencies among critical infrastructure operations, attacks, acts of nature (as the Nation witnessed in the aftermath of Hurricane Katrina), and even accidents can easily result in a cascading effect that can paralyze a city or region and produce consequences impacting the entire Nation.

Of particular concern and addressed by this initiative are infrastructure nodes and operations within the Michigan and Canadian border regions. These infrastructure operations constitute a major hub of and empower national security, industrial, economic and societal activities of enormous magnitude. Accordingly, a terrorist or "insider" attack, accidents, technological failure, or natural disaster(s) impacting critical infrastructure operation within this region have the distinct potential to inflict grave consequences on the region and the entire Nation.

Consistent with the Department of Homeland Security's emphasis on managing risk as a combination of threat, vulnerability and consequence, and in a concerted effort to ensure the security and economic viability of local, regional, national business and the maintenance of international trade that is essential to the Nation's economy and the quality of life of its people, leaders in St. Clair County took action.

Partnering with The Security Board, St. Clair County has initiated the conduct of a multi-year regional and international assessment to enhance the county's and the Nation's preparedness to directly address the "all-hazards environment" to ensure the operational resiliency Critical Infrastructure operations on the U.S./Canadian Border. While protection forms a sound foundation, in the post-September 11 environment and in the wake of the critical infrastructure failure that made Katrina a national tragedy, it has become obvious that critical infrastructure resiliency is a regional and national imperative.

Accordingly, St. Clair County will employ a Critical Infrastructure Resiliency Index (CIRI) to benchmark the state of the region's critical infrastructure resiliency.

The CIRI will provide an objective foundation for investment in and managing the effectiveness and efficiency of regional infrastructure resiliency efforts. The CIRI rating will be used as a metric for "before and after" comparisons of critical infrastructure resiliency and the effectiveness of related critical infrastructure and ongoing business resiliency investments. The index is adaptable and can be used to understand the resiliency of a region's critical infrastructure operation, and when combined with similar efforts can be used to understand the Nation's, and its principal overseas trading partners'/allies' infrastructure resiliency.

Phase 1
The critical infrastructure resiliency assessment will initially focus on telecommunications, natural gas, electric energy and transportation will have several objectives:

- Identify regional critical infrastructure concentrations and chokepoints whose operational disruption (regardless of cause) could adversely effect regional and national businesses and security.
- Establish desired infrastructure resiliency standards
- Establish a regional CIRI rating as a result of the region's identified standards, quantified threats, vulnerabilities and consequences.
- Raise awareness of critical infrastructure operational and interdependency issues and their potentially catastrophic consequences.
- Identify public information challenges and ways to improve dissemination of timely, actionable threat and warning information, and lessons-learned/best practices to support infrastructure resiliency efforts and foster trust and coordination between all levels of government, business partners and critical infrastructure owners and operators.
- Identify Critical Infrastructure technology development needs to provide for 21st Century infrastructure management. Specifically, the instrumentation and real-time visualization of multiple critical infrastructure performance, and analysis and decision support tools to identify multi-sector interdependencies and cascading intercept points to ensure the timely and effective restoration of critical infrastructure services regardless of the cause of their loss.

Phase 2
Conduct economic-probabilistic modeling of regional incidents, infrastructure failures, and resulting societal, business, and economic consequences on the critical infrastructure, business, and government operations and regions being studied. The magnitude and scope of this modeling will be dependent on the findings from phase 1 and will be incorporated into the established CIRI rating.

An economic assessment and Risk/Return Analysis of a critical infrastructure failure using the Business Economic Valuation (BEV) methodology will be used.

The probability of such events will be calculated dependent upon information gathered in collaboration with the U.S. Department of Homeland Security, other Government Agencies, public/private partnerships, regionally focused organizations and the development of other sources of information and infrastructure resiliency expertise. The uncertainty surrounding the means and parameters of the next attacks on the United States and whether an attack on telecommunications will be external, physical, or internal/web-based will be considered.

- The objective is to identify and build a general equation for the economic value/loss of a critical infrastructure failure including the cost and the loss of benefits, specifically:
  - Identify the key factors that determine the BEV of critical infrastructure to the business, region and potentially the Nation.
  - Identify the cost and loss of the services not delivered when there is a critical infrastructure failure, and as a result government and/or businesses failure.
  - Identify all of the external relationships affected by this failure and quantify the impact on important constituencies such as customers, suppliers, banks, business partners, and others.

Building a National Model
This initiative and the regional critical infrastructure resiliency approach provide a test-bed and pilot for similar national efforts that constitute "An investment in America." This initiative also demonstrates the imperative for rapidly developing public and private trust, information exchange based on requirements of local, state, regional and private sector stakeholders. Overall, a true partnership must be developed to solve the Critical Infrastructure challenges resulting from the 9/11 and Katrina environments, technological advancement and the accompanying creation of increasingly exploitable software and hardware, and to prevent the potentially catastrophic and lasting physical, economic and human consequences that can be inflicted on the Nation by their destruction or corruption.

Ultimately, the attainment and sustainment of resilient Critical Infrastructure operation for cities, states and regions -- and the Nation -- will require the identification and assessment and continuous testing of assets based on desired and objectively measurably resiliency goals (e.g., time to restoration of essential functions), trusted, timely, tailored, and reliable information exchange, and the

promulgation of national policies, standards, and procedures built from the "bottom-up" – i.e., in close cooperation with infrastructure owners and operators, key private sector and business leaders, and all levels of government. It is to that end that the St. Clair, Michigan, Regional Critical Infrastructure Resilience Initiative is dedicated

Acknowledgments

- **Senator Carl Levin**, D-MI
- **Senator Debbie Stabenow**, D-MI
- **Congresswoman Candice Miller**
  R-10th Congressional District, MI
- **Col. Michael McDaniel**,
  Homeland Security Policy Advisor to the Governor of Michigan
- **Shaun Groden**, County Administrator,
  St. Clair County Board of Commissioners

Contact Information

Jeffrey A. Friedland, Director
St. Clair County Homeland Security/
Emergency Management
jfriedland@stclaircounty.org
(810) 989-6965

Dick Arns, Executive Director
Security Board
dickarns@comcast.net
(630) 926-5040

Appendix I

Community: U.S. Private and Public Partnership

Community Overview
The U.S. Private and Public Partnership (US P3), formerly known as HSIN-CI, connects the Homeland Security Operations Center (HSOC), the Federal Bureau of Investigation's (FBI's) Field Intelligence Directorate, and representatives from the private sector, law enforcement, public safety, and critical infrastructure. US P3 enables these individuals and entities to disseminate information both vertically (among private and public, regions, and headquarters) and horizontally (among members operating within the same geographic location, infrastructure, or discipline).

US P3 has two main components: field operations and the technology to support them. The field operations are a joint U.S. Department of Homeland Security (USDHS) and FBI effort that involves the creation of private and public-sector regional governances (RGs) within the established Federal Emergency Management Agency (FEMA) regional boundaries. The RGs are coordinated by a US P3 Regional Manager (FBI Special Agent from the Field Intelligence Group); together they are responsible for promoting local private and public-sector participation within their regional sector. Participation involves providing their 24/7 point of contact (POC) for themselves and their company or organization.

The technology has three main features: a web portal that reflects the regional program equities for the members; a member database/repository; and robust search and communication features. This technology allows for horizontal and vertical routine information sharing and 24/7 alert and notification data by individual member, critical infrastructure, company, or geographic location. Specifically, 10,000 simultaneous outbound calls, 3,000 faxes, 30,000 inbound calls, text paging, and e-mail to desktops and mobile devices are a few of the technology features. Another feature, which is in partnership with the FBI, allows the members or the general public to submit suspicious reports via a web link on each regional web portal. These suspicious reports are transmitted in real time to the USDHS HSOC and FBI Strategic Information Operations Center (SIOC) for handling

The goal of US P3 is to leverage the network of personal relationships at the regional and local levels, among public and private decisionmakers, to facilitate the identification and prevention of natural or manmade disasters. The program is designed to provide the USDHS and the HSOC with access to a broad spectrum of industries, agencies, and critical infrastructure owners and operators across the public and private sectors. Members join US P3 as part of a group defined by industry, region, or area of interest. Examples include U.S. geographic region, critical infrastructure sector, security professionals, and general public interest.

Currently, the program has approximately 40,000 members, organized into four regions: Seattle (Northwest), Dallas (Southwest), Indiana, and Atlanta (Southeast). The future goal is to extend the program to 200,000 private and public decisionmakers over the next two years, encompassing 10 U.S. regions.

COMMUNITY FUNCTIONALITY AND USAGE

Technical Functionality
US P3 has the following capabilities:

- **Alert and Notification Capability** issues 24/7 emergency alerts and notifications (typically from the USDHS and the FBI) to individual members or groups through e-mail, telephone, broadcast, pager, fax, or mobile phone. The system enables the sending of alerts specific to a geographic or local area.
- **Information Sharing (E-mail) Capability** gathers and distributes critical and general information across the program or to specific members or groups.
- **Suspicious Reporting Capability** provides a suspicious-reporting portal on the Internet that can be used by members and the general public to report suspicious activity directly and simultaneously to the USDHS and the FBI.

- **Strategic Contact Management Capability** approves and categorizes contacts as either a public or a trusted source and maintains up-to-date 24-hour member contact information.
- **Resource Visibility Capability** maintains member-accessible resource databases for emergency planning and response.
- **Asset Visibility and Assignment Capability** coordinates and tracks posted needs and donations to expedite resource movement during emergencies and to inform after-action reports

The tool most widely used through the US P3 program is e-mail narrowcast and broadcast. US P3 has robust search capabilities that can specify the criteria for a targeted audience within the database and locate the specific individuals, such as by member name, subject-matter expertise, company, geographic location, critical infrastructure, or resources. Once the user has identified the target audience, the message can be disseminated via voice broadcast (10,000 simultaneous outbound calls per minute), faxes (3,000 simultaneous outbound per minute), e-mail to mobile and desktop computers and text messaging (10,000 simultaneous per minute). The message delivery method is determined by the priority of the information to be disseminated.

Usage

Community members use US P3 to send messages in the following ways:

- **Government to community.** The USDHS sends out daily reports through US P3, such as the IAIP Daily Report, and Global Snapshots highlighting briefs around the world that focus on terrorism, transport, national security, and other topics, which affect day-to-day issues of homeland security. The USDHS and the FBI use US P3 to submit general or targeted sector-specific notifications and alerts to US P3 members, at the national or regional level.
- **Intra/Inter-community**. The US P3 member community shares information, such as threats, suspicious activity, and requests for information. For example, if a person is seen snapping photographs at a nuclear plant, US P3 can be quickly implemented to notify all others in the area of that infrastructure, or in other COIs.
- **Community to Government.** The FBI Tips Suspicious Report feature enables both members and the general public to submit information on suspicious activities or events. These reports are shared in real time with the USDHS (HSOC) and the FBI Counter Terrorism Unit and passed on as required to relevant FBI field offices, multi-agency joint terrorism task forces (JTTFs) and State fusion centers.

US P3 tools are also used under special circumstances (following an incident) for members to log resources that could be used for restoration and recovery operations.

Case Studies

The HSOC delivers routine information daily to US P3 members—generally in the form of the IAIP Daily Reports.

During the Columbia shuttle disaster, NASA's Johnson Space Center used US P3 to deliver targeted information and instructions to public and private-sector members over the 200-square-mile area of the debris field. Broadcast instructions ranged from the handling of shuttle debris and human remains to organizing the personnel for the extended recovery mission.

Following the 2005 hurricanes, and at the request of the USDHS and FEMA, the National Program Office for US P3 created the National Emergency Resource Registry (NERR) as an added feature to critical infrastructure to support relief efforts for Hurricanes Katrina and Rita. When the NERR was activated, US P3 e-mailed the entire membership asking for any resources that could be made available for relief efforts. Within minutes, and into the weeks following, US P3 members began listing what would amount to almost 70,000 resources. These resources included housing, hazardous materials equipment, trained medical personnel, and other items.

COMMUNITY MEMBERSHIP AND GOVERNANCE

Membership

US P3 currently supports approximately 40,000 regular members nationwide. In addition, there were 76,000 individuals who signed up separately for the NERR program. Of the current membership, 90 percent are estimated to come from the private sector, which reflects the estimated 85 percent industry owner/operator status of the Nation's critical infrastructure.

In addition to the applicants, US P3 also imports entire databases of membership (several thousand) from companies and organizations across the country, such as BOMA, the Federal Executive Board, the Red Cross, ASIS, the National Retail Federation, InfraGard, and key Fortune 500 corporations. The program allows multiple organizations to use the US P3 technology platform at no cost, while DHS does not interfere with the organizations' operations. The value to the government and the various organizations is that they are enabling their members to participate in a program that has direct 24/7 information access to and from the USDHS HSOC. Equities in the program are also provided to these organizations/associations through regional or national governance seats/participation.

Governance

Governance of US P3 is organized by regions and directed by the US P3 National Governance (a non-profit corporation and thus a legal entity), composed of the officers from each of the RGs. The National Governance works in close coordination with the US P3 National Program Office (NPO) located in Dallas, TX. Currently there are four operational regions: Southwest (Texas), Southeast (Atlanta), Northwest (Seattle), and Indiana (19 states). The goal is to eventually expand the program to the 10 regional boundaries based on the FEMA State boundaries. This geographical structure was chosen because most States and some private corporations have mutual-aid agreements based on the existing FEMA geographical boundaries.

Each region supports a regional governance body, selected from the member pool for that particular geographic area, and is led by a USDHS Regional Manager (an FBI agent from the Field Intelligence Group (FIG). The RG identifies and solicits the participation of a vetted cross-sector community representing critical infrastructure owners and operators, subject-matter experts, and others from the private and public sectors.

Among the membership/governance bodies, various committees have been formed to identify sector-specific information requirements and reports. These committees allow the USDHS to work with the private sector/critical infrastructure to identify the existing information requirements for both partners.

Each US P3 region has one or more gatekeepers/moderators for each affiliated COI to authorize content postings. Each RG representative appoints the various gatekeepers/moderators per COI.

Implementation Status

Although officially still in "pilot" phase, US P3 is fully functional and operational since former Secretary Tom Ridge officially launched the program in June 2004. 40,000 members and dozens of Federal, State, and local government agencies are currently using it across the county. The widemajority of current members were gained within one year of the pilot program launch.

The US P3 National Deployment will include 10 regional programs (locally/regionally governed and administered) and one National Program, to serve as the Federal coordination point for the 10 regional programs.

The program will be coordinated through the National Program Office located in Dallas, TX. As the program moves toward a national scope, the goal for growth is 200,000 vetted cross-sector members by the end of FY07. The US P3 National Deployment is based on the strategy, success, and lessons learned of the US P3 Pilot Program.

In addition to the growth of membership, the metrics used to gauge the success of this program will include participation from private and public members, as well as regional and national governance and committee activity, which are key to the administration of this program. To date, there are approximately 200 persons in these roles, who serve as the program leadership in coordination with the USDHS and FBI Federal program managers for the 40,000+ national members.

Further implementation goals include formalizing procedures for sharing content/intelligence with State Fusion Centers, and putting in place a process to further integrate FBI intelligence at the Federal and regional levels. This includes bringing in the FBI FIG as a full partner in US P3. The objective is to deliver regionally relevant, timely, and actionable information to the US P3 members.

Training and Outreach

The primary channel for outreach to new members of US P3 is through the Regional Managers and RGs. The RG bodies identify and solicit additional participation from the cross-sector community of critical infrastructure owners and operators, subject-matter experts, and others from the private and public sector that have a "need to act," rather than the traditional "need to know" required for security clearances.

US P3 training is coordinated through the National Program Office and focused on the members with administrative roles in site operations. Training for Regional Managers and RGs consists of the detailed hands-on US P3 web portal (instructions), PowerPoint presentations highlighting the functionality and communication features of US P3, as well as the provision of additional system documentation and references for administrators, technicians, and members.

To date, all persons with gatekeeper roles have been trained. The ease of the system does not require the everyday user to be trained. As the program brings in more gatekeepers, they will need training.
The success of the program has mainly been due to member promotion. Limited resources have been allocated to the advertising. A formal joint USDHS and FBI US P3 announcement is scheduled for January 2006 and will serve to enhance publicity at the time of the program's launch.
The US P3 National Governance intends to reach the 76,000 NERR members when that program ends (expected at the end of 2005) and offers them the opportunity to apply for full membership in one of the regional US P3 programs.