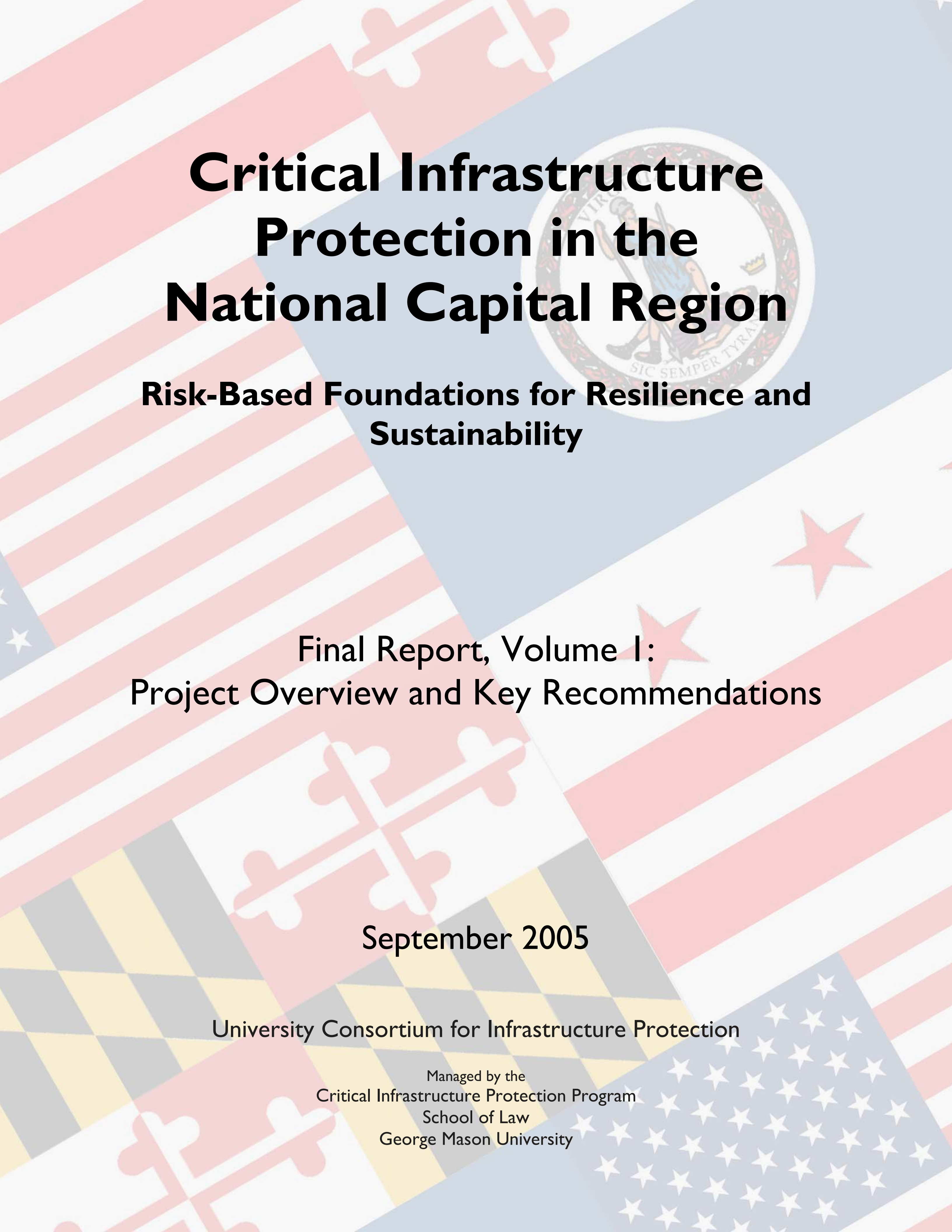


Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume 1:
Project Overview and Key Recommendations

September 2005

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

This Page Intentionally Blank

Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume 1: Project Overview and Key Recommendations

Submitted in fulfillment of:
Department of Homeland Security Urban Areas Security Initiative (UASI) Grant 03-TU-03; and
Department Justice Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199

September 2005

John A. McCarthy, Principal Investigator
Jerry P. Brashear, Project Director

Christine Pommerening, Jordana L. Siegel, James T. Creel, Ben Stafford,
Terrence P. Ryan, Larry J. Clark, and Brien Benson

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

The National Capital Region's Senior Policy Group Cover Letter
For the
University Consortium's Critical Infrastructure Report

George Mason University was awarded a sub grant by the National Capital Region's Senior Policy Group (NCR SPG) on March 17th 2004 based on the need for effective methods and practices to ensure security and operation of vital systems and services provided by the regions critical infrastructures. The intent of the sub grant was to gather a Regional and National perspective on global issues facing both the public and private sectors in critical infrastructure protection and to benchmark best practices.

As in any study of this magnitude, the research, benchmarking, and analysis take considerable time. As such, several of the observations and recommendations mentioned in the report have already been, or are in the process of being, addressed, adopted and or instituted within the NCR.

Though this study was a deliverable associated with GMU's sub grant, the views and opinions expressed are that of the contributing Universities and are not those of the NCR SPG.

Please contact Steven Kral of the DC Office of Homeland Security as the State Administrative Agent point of contact for the UASI grant.

Copyright © 2005 by George Mason University

Published in 2006 by George Mason University

Citation:
McCarthy, J.A., Brashear, J.P., Pommerening, C., Siegel, J.L., Creel, J.T., Ryan, T.P., Stafford, B., and Clark, L.C. (2005). *Critical Infrastructure Protection in the National Capital Region – Risk-Based Foundations for Resilience and Sustainability***.** Final Report. Arlington, VA: George Mason University.

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

John A. McCarthy, Director
3301 Fairfax Drive, MS 1G7, Arlington, Virginia 22201
Phone: 703-993-4840; Fax: 703-993-4847
jmccart6@gmu.edu

September 30, 2005

Senior Policy Group of the National Capital Region
And
Critical Infrastructure Working Group
c/o Mr. Steve Kral
Administrator
Office of Homeland Security
Office of the Deputy Mayor for Public Safety and Justice
Suite C-09
1350 Pennsylvania Avenue, NW
Washington, DC 20004

Ladies and Gentlemen:

We are pleased to submit ***Critical Infrastructure Protection in the Nation Capital Region – Risk-Based Foundations for Resilience and Sustainability.*** It is the final report of the National Capital Region (NCR) Critical Infrastructure Project, prepared by the University Consortium for Infrastructure Protection. This report is the deliverable fulfills the requirements under the terms of the two supporting grants, Department of Homeland Security, under Urban Areas Security Initiative (UASI) Grant 03-TU-03; and the Department of Justice, under the Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199. This report contains the final versions of research projects introduced in the Interim Report of May 2005 and research not previously reported.

Because of the breadth of the research topics explored in depth, we present the report in twenty volumes organized around specific topics to permit distribution of the volumes of interest to specific stakeholders. For example, the eight infrastructures examined are reported in seven volumes (two were combined for reporting) for the convenience of the respective sector managements. With the exception of several figures in Volume 9 (presented in both redacted and unredacted versions), there is no security sensitive information in the report.

This first volume, *Overview and Key Findings*, and a separately packaged “Special Summary for the NCR Leadership” introduce the principal challenges to the NCR identified during the investigation and summarizes the major findings and recommendations of the individual reports..

The subsequent volumes, which are enumerated in the enclosure, are stand-alone reports on specific research projects conducted as part of the overall program.

The findings and recommendations of this project are offered as a contribution to the NCR's strategic planning efforts, currently underway. I firmly believe that whatever directions the NCR leadership chooses for establishing a comprehensive program for critical infrastructure protection, this work will serve as a solid foundation for future organizers, planners and leaders. The scholarship of the dozens of dedicated researchers from six distinguished universities who worked on this project will contribute to a more resilient, sustainable, and secure region.

Finally, I would like to express my gratitude to the leadership of the National Capital Region – public and private sectors alike – for their vision to support critical infrastructure protection research and planning for our citizens and communities. This initiative truly has been in the vanguard of regional infrastructure protection.

Sincerely,

John A. McCarthy
Principal Investigator

Enclosure: Volumes Comprising *Critical Infrastructure Protection in the Nation Capital Region – Risk-Based Foundations for Resilience and Sustainability*

Enclosure

Volumes Comprising
Critical Infrastructure Protection in the Nation Capital Region – Risk-Based Foundations for Resilience and Sustainability

1. Project Overview and Key Recommendations
2. Energy Sector
3. Water and Wastewater Sector
4. Transportation/Postal and Shipping Sector
5. Health Services Sector
6. Emergency Services Sector
7. Telecommunications Sector
8. Banking and Finance Sector
9. Regional Analytics for Risk Management and Resource Allocation
10. A Database and Architecture for Comparing Vulnerability Assessment Elements
11. Criteria and Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures
12. Designing a Roadmap to Partnership: The First Step – Identifying the Key Stakeholders
13. The Region and its Governance Structure in Perspective
14. Critical Infrastructure: Citizens' Views of Protection in the National Capital Region
15. Critical Infrastructure Protection, Vulnerability and Public Confidence
16. Community Shielding in the National Capital Region: A Survey of Citizen Response to Potential Critical Incidents
17. Critical Role of Citizens in Biodefense and Early Warning
18. Epidemiology of Transportation Systems and Bioterrorism
19. Protecting the Nation's Blood Supply: A Critical Infrastructure
20. Hurricane Isabel: Critical Infrastructure Interdependency Assessment

This Page Intentionally Blank

Acknowledgements

The authors wish to thank the Senior Policy Group of the National Capital Region for establishing this project, their sage guidance and the opportunity to possibly contribute to enhancing the resilience of the region that is so vital to the stability and security of the world – and where we live.

We also want to express our heart-felt gratitude to the several thousand people who contributed their expertise, insights, opinions and judgments about the issues addressed in this report, ranging from the randomly selected thousands of residents of the region and even the United States outside the region, to – and especially – the representatives of the NCR’s key infrastructures and jurisdictions, whose patience we may have tried but to whom our greatest respect for doing daily the work that keeps our region going..

We also wish to thank the sources of the financial resources that permitted this study to happen, the Department of Homeland Security, under Urban Areas Security Initiative (UASI) Grant 03-TU-03; and the Department of Justice, under the Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199.

This research was conducted as part of the National Capital Region Critical Infrastructure Protection Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator. The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security, the Department of Justice or the Senior Policy Group.

This report has been prepared by the faculty and staff of the six members of the University Consortium for Infrastructure Protection (UCIP), organized and managed by the Critical Infrastructure Protection Program (CIPP) at George Mason University’s School of Law. To each of the contributors to the research reported here (below), the management of the effort extends deepest gratitude.

CIPP Staff

John A. McCarthy, Principal Investigator

Jerry Paul Brashear, Ph.D., Project Manager

Larry Clark, James Creel, Jessica Milloy, Christine Pommerening, Ph.D., Jordana Siegel and Kevin (Kip) Thomas

NCR-UCIP Members

George Mason University –
Farrokh Alemi, Ph.D., Vikas Arya, Ph.D., Brien Benson, Ph.D., Marcus Bowman, Ami Carpenter, Shaoming Chen, Osita Chidoka, Mike Giberson, PhD., Jonathan Gifford, Ph.D., Sean Gorman, Ph.D., Gerry Hanweck, Ph.D., Mark Houck, Ph.D., Saul Japson, Adriana Kocornik-Mina, Raj Kulkarni, Todd La Porte, Ph.D., Andy Loerch, Ph.D., Arnauld Nicogossian, M.D., Patrick O’Neill, Anoop Singhal, Ph.D., Laurie Schintler, Ph.D., Ted Smith, Roger Stough, Ph.D., Mohan Venigalla, Ph.D., Shanea Watkins, and Wayne Williams.

Virginia Polytechnic Institute and State University –

Frederick Krimgold, D. Tech., Director, Disaster Risk Reduction Program, Advanced Research Institute; John Bigger, Keith Critchlow, Tom Grizzard, Ph.D., Kitty Hancock, Ph.D., Nicholas Konz, Lamine Mili, Ph.D. Natasha Udu-gama, and Michael Willingham, Ph.D.

University of Maryland –
Gregory Baecher, Ph.D., Chairman, Department of Civil Engineering; Phil Tarnoff, Director, Center for Advanced Transportation Technology

University of Virginia –
Gregory B. Saathoff, M.D., Executive Director, Critical Incidents Analysis Group; Monica T. Williams, Thomas M. Guterbock, Ph.D., Anna MacIntosh, Robin Bebel

James Madison University –
George Baker, Ph.D., and Stephen Stewart, Ph.D., College of Integrated Science and Technology; Cindy Jane Allen, Institute of Technical and Scientific Communication

Howard University –
Kathleen Kaplan, Ph.D., Department of Systems and Computer Science

Independent Advisors –
P.J. Aduskevicz, Jeanne Geers, Terrence P. Ryan, Paula Scalingi, Ph.D., Benjamin Stafford, Lee Zeichner, Esq., and Thomas F. Zimmerman, Ph.D.

Table of Contents

List of Figures

List of Tables

1 Executive Summary

The National Capital Region (NCR) is a target-rich environment in a terrorist's eyes. As seat of government and military headquarters of the world's only superpower, home of many of the world's financial and economic development institutions and the fourth largest regional economy in the U.S., iconic and operational targets abound. Natural hazards also threaten to diminish the functioning of this region. Disturbances from either source disrupt the essential services necessary for life, health, public safety, economic well-being, public confidence and national security.

To help understand and address these threats, the NCR Senior Policy Group, the homeland security advisors to the Governors of Maryland and Virginia and to the Mayor of the District of Columbia, and the Director of the Office of National Capital Region Coordination of the U.S. Department of Homeland Security, commissioned a major project by the University Consortium for Infrastructure Protection, headed by George Mason University, to recommend steps to begin to make the region's infrastructures more secure, reliable and resilient. The specific infrastructures of interest are those that provide *life-essential services* – electricity, natural gas and fuels; potable water and wastewater services; healthcare; public safety, fire suppression and emergency medical care; transportation and shipping; finacial services and telephone service. This report summarizes the findings and key recommendations of the study. It is arranged in four general topics: the region as a whole, eight critical industry sectors, risk management for assets and the region, and citizen and community issues.

Region as a whole At the time of this study, the NCR had no standing mechanism specifically dedicated to enhancing the resilience of the region's critical infrastructures in case of terrorist attack or natural disaster. However, in 2002, the National Capital Region's Eight Commitments to Action identified critical infrastructure protection as a high priority of the region's homeland security strategy. This report therefore recommends the creation of a regional public/private partnership ("Partnership"), responsible to:

1. Coordinate with at least the eight critical sectors studied the use of appropriate risk management to evaluate the business case for private investment in infrastructure protection, reliability and resilience and to provide common metrics to permit prioritization of public resources across all sectors and jurisdictions.

2. Insure that each sector has its own coordinating committee to prioritize security needs, insure coordinated planning and procedures between public and private sectors, and coordinate with other sectors to assess and ameliorate risks arising from interdependencies.

3. Oversee the implementation of needed improvements in procedures throughout the region. One such procedure is insuring that restoration personnel from the critical sectors are properly credentialed to enter restricted areas promptly following a terrorist attack or natural disaster.

4. Coordinate with NCR utilities and their regulators to include cost-beneficial security improvements in their rate bases and harmonize their policies across the region.

5. Manage the interaction with federal agencies concerned with regional resiliency, including the Department of Homeland Security, the Department of Justice, and the Department of Defense, to make optimal use of the intellectual and financial resources they can bring to bear.

6. Draw knowledge from the experiences, organization and procedures of other public/private partnerships throughout the country and abroad dedicated to improved security and resilience.

Critical infrastructure sectors The eight critical sectors have important differences as regards resiliency to terrorist attack or natural disaster. Most obviously, each has its own technologies and institutional arrangements, implying different security requirements. These technological and institutional differences imply different degrees of concentration of facilities and vulnerability to disruption. At the one extreme, electric power in the region depends on a handful of power plants and is susceptible to disruption at a handful of distribution nodes, while emergency services and health services are widely dispersed and redundant. The state of risk management also varies widely among the sectors, with some approaching highest levels of risk-based decision-making, while others are at the most basic levels of checklist compliance.

Another important difference among the sectors is the role of government. In substantial part, water, highways and emergency services are government owned and operated. In the other sectors, government has varying degrees of regulatory power. The level of government authority in a sector has major implications for how directly government influence security enhancements.

Notwithstanding these important differences, there is a high degree of congruity in the issues and recommendations of the different sectors. All sectors are aware of the risks imposed on them by dependencies on other sectors. All sectors call for a better mechanism for managing these dependencies and coordinating planning among sectors at the regional level. Several want better coordination of operations in time of crisis, and nearly all recommend table-top exercises to test and improve coordination while building the shared understanding conducive to an effective public/private partnership for enhanced resilience and reliability.

Risk management for critical assets and the region as a whole Among the hundreds of vulnerability assessments and risk management methods in use, each sector has one or more favored tools. A review of the most 18 prominent found none that was comprehensive and universally applicable enough to yield directly comparable results. Two, however, both sponsored by the U.S. Department of Homeland Security – the Special Needs Jurisdiction Tool Kit and Risk Analysis and the Management for Critical Asset Protection (RAMCAP^{TM}) – are more comprehensive and applicable than most. RAMCAP^{TM} is being tailored to specific sectors, so will expand the ability to compare risks across sectors.

The only known method for risk analysis and resource allocation at a *regional* level is Critical Infrastructure Protection Decision Support System (CIP/DSS), under development by a consortium of National Laboratories under DHS sponsorship. It is currently at the initial field-testing stage and tests are being planned. The consortium recommends that the NCR leadership closely monitoring these plans and, if possible, participate. The required quantity of data and the fact that the model is planned to be offered only as a service of the Laboratories, however, leads to the recommendation that the NCR leadership also adopt or develop methods that can be used sooner and with largely available data and analytic techniques. One such approach is suggested as a point of departure to develop and test a near-term, practical, cost-effective approach

Citizens and Communities The project conducted citizen panels and surveys, which found that people in the region have a deep sense of vulnerability to terrorist attack, with two-thirds of respondents believing another terrorist attack in Washington, D.C., is likely. Furthermore, forty percent of respondents lacked confidence in the reliability of electric power and landline telephone service in case of terrorist attack. In response to these and related findings, the Consortium recommends improved communication with citizens, plus increased spending on selected upgrading of security preparations in the water, electricity and health care sectors. The report also recommends careful weighing of the pros and cons of evacuation vs. shelter-in-place in the event of a terrorist attack.

The following sections specify these principal findings and recommendations further. Section 2 presents recommendations regarding the region as a whole. It draws on the total research effort and especially the material on structuring regional partnerships summarizes Volumes 12 and 13. Section 3 summarizes the key findings for the eight critical sectors (Volumes 2 - 8). Section 4 summarizes the evaluations of vulnerability assessment and risk management tools (Volumes 10 and 11). Section 5 considers methodologies for risk-based benefit/cost analysis and resource allocation on a regional scale (Volume 9). Section 6 discusses public confidence, sheltering-in-place and community shielding, and related special studies (Volumes 14 - 19).

2 RECOMMENDATIONS FOR THE REGION AS A WHOLE

2.1 Introduction

As Hurricane Katrina, 9/11, the Northeast Blackout of 2003, and Hurricane Isabel remind us, certain services are absolutely critical to physical and economic survival. Among them are shelter, food, water, sanitation, evacuation and transportation, power and fuels, medical care, public safety, communications and access to financial resources. Disruption of any of these defines a crisis. The systems that provide these essential services are critical infrastructures (CIs).

Eighty-five percent of CIs in the National Capital Region are owned and operated by the private sector, but the public looks to governments at all levels to prevent and resolve the crisis, as Katrina demonstrated. Losses of life and health, national security, economic production and public confidence due to CI disruptions can be vastly reduced if the CIs are *resilient* – they can withstand attack or natural disaster or they can restore service quickly. Continuity of both the private CI (i.e., reliability of service) and public CI is essential to sustaining the viability of the community.

A disruption in a CI in a specific region is most likely to affect not only the damaged CI but a variety of others, creating cascades of disruptions in life-essential services and spreading the risks to all elements of the regional populace and economy. These *dependencies* among infrastructures, especially CIs, frequently result in circumstances where the benefits of reducing the risks of CI failure accrue to others than the owners of CI who would bear the cost of risk reduction. This results in systematic under-investment in risk reduction relative to the region's resiliency requirements.

The National Capital Region (NCR) is one of the world's most important regions – seat of the world's most influential government, headquarters of the world's only super-power military, headquarters to global businesses, center of national and global systems of central banks and development finance, hub of a significant portion of the world's information and communications infrastructure, and institutional and symbolic center of the nation. It is a terrorist target of the first rank. Disruptions of essential services in the NCR have not only regional impacts, but national and global ones as well. The leaders of the NCR governments are not only responsible for their own jurisdictions, but are stewards of a region whose impact extends well beyond the NCR.

At the time of this study, however, there was no regionally responsible, accountable management body to plan for, finance, and execute out necessary improvements to the reliability and resilience of critical infrastructures other than those directly supporting emergency services. This gap is reflected in the distribution of funds from the Urban Areas Security Initiative (UASI), where CI projects have faced unfortunate and unnecessary competition with the needs of first responders and response-focused initiatives.

2.2 Goal

The strategy and recommendations that follow advance one strategic goal: ***to significantly enhance the resilience of the National Capital Region to disruptions to the critical infrastructures that provide life-essential services.*** Such resilience would be manifested in the ability to withstand attack without service interruption, to continue in operations despite or during an attack, and/or to restore service quickly. Its hallmarks (and the basis for its metrics) are reliability, continuity of service and minimized disruption.

2.3 Organizational Arrangements in the NCR

There is at present no single organization in the region with the authority and responsibility to plan for, finance, and carry out programs to improve the resiliency of the region's infrastructure to terrorist attack or major natural disaster. It is true that there are information-sharing councils, voluntary public/private partnerships concerned with emergency response, and laudable emergency response and citizen education and preparedness plans and projects. The U.S. Department of Homeland Security and private sector associations have undertaken major initiatives and investments to organize and coordinate with private- and public-sector CI owners on a national scale, as evidenced by the Interim National Infrastructure Protection Plan and the many sector councils.

However, the NCR's 14 jurisdictions and its numerous private CI owners have yet to evolve the organizational and institutional means to undertake needed critical infrastructure resilience analyses, define risk reductions, allocate resources to their execution, or evaluate their resulting heightened resilience. All current initiatives and plans, including the critical infrastructure elements of the Emergency Support Functions under the Council of Governments, are only partial solutions, and need to be combined in a single entity. This situation will not fundamentally change without federal legislation or major policy directives by the executive branch.

2.3.1 Proposal for a new region-wide Organization

Barring such fundamental change, there is an alternative that could provide a major increase in the effectiveness of NCR planning, preparedness and operations. This is a public/private partnership that is built on the three existing regional coordinating bodies of particular importance for CIP:

1. The NCR Senior Policy Group (SPG), which consists of the homeland security advisors to the Governors of Maryland and Virginia the Mayor of the District of Columbia, and the Director of the Office of National Capital Region Coordination (ONCRC), each with its own staff dedicated to homeland security matters;
2. The Greater Washington Board of Trade (BoT), representing the region's private sector, including business and not-for profit civic institutions. The Board of Trade has no statutory authority with regard to homeland security, but acts instead as the unofficial representative of businesses and non-profits on these matters; and
3. The ONCRC *per se*, representing the federal government, region's largest single stakeholder, and the conduit to the federal homeland security arena

The Consortium recommends the creation of a **National Capital Region Critical Infrastructure Partnership** that involves these three bodies and operates through two simultaneous processes: (1) a private-sector led initiative and (2) a public-sector led coordinating council. Both processes would be served by the Partnership's executive secretariat, which would include an executive director and a staff of some half-dozen professionals.

1. The private-sector led initiative would be a multi-step partnership process around infrastructure interdependency exercises and similar forums designed to encourage and facilitate the development of an action plan for stakeholders. This process involves identifying and bringing together the key infrastructures and organizations on which a region's viability depend, and then engaging them in collective activities to raise awareness, develop trust, and work together. The main task of this initiative would be defining the mechanisms and priorities for investments in infrastructure risk

management. This proposal is further elaborated in Volume 12, "*Designing a Roadmap for Partnership: The First Step – Identifying the Key Stakeholders.*"

2. The public-sector led coordinating council would include coordinators from the District, each state, the federal government, and the private sector, for a total of five. Others could be added later as *ad hoc* or permanent members. The four public sector coordinators are already in place in form of the current SPG (or a designated subgroup). The private sector coordinator would be determined by the BoT. Each coordinator would have the authority to approve plans, assign and coordinate resources, set priorities, and approve preparedness and response actions within and using resources from his/her jurisdiction and stakeholders. During a crisis, these coordinators would have immediate access to all situational, resource, and operational information in the NCR. This proposal is further elaborated in Volume 13, "*The Region and its Governance Structure in Perspective*."

The executive secretariat would be led by an executive director and supported by a small full-time staff. This secretariat should not be staffed by one of the coordinating council members' organizations or by organizations currently addressing emergency response, but be independently contracted and responsible to and evaluated by the coordinating council. Among its tasks would be pulling together the private-sector led initiative and the coordination council; holding regular dialogues with other regions, federal agencies, and academic institutions; drawing industry representatives into the Partnership council as needed; assisting in table-top and interdependency exercises; and performing the staff work to support the decision-making of the Partnership.

One of the most important tasks of the Partnership will be to set funding priorities. The National Capital Region is the only region in the country explicitly cited in the Homeland Security Act and authorized federal funds for homeland security purposes. Apportioning these funds, and insuring that recipients are properly organized to spend the funds wisely, has been a principal task of the SPG. We envision that the Partnership will help guide the SPG in its determination of funding priorities.

The recommendations that follow presume the creation of the Partnership described above, with a mandate from the region to promote greater infrastructure resiliency, a strong executive secretary and supporting staff, and a reasonable sized budget.

2.4 Recommendations

These recommendations are grouped according to the four categories established in the draft NCR Homeland Security Strategic Plan: planning and decision-making, prevention and mitigation, response and recovery, and community engagement.

2.4.1 Planning & Decision-Making

a) The SPG and BoT should establish a provisional NCR coordinating council, charter the Partnership and establish the secretariat.

b) A greater and more carefully calibrated understanding of the relationships between the public and its supporting CIs is urgently needed. To foster greater awareness and to promote more robust public/private partnerships and CI resilience, The Greater Washington Board of Trade (BoT), in collaboration with the NCR's Senior Policy Group (SPG), should plan, organize, and capture the lessons of a relatively large scale discussion-based exercise or series of exercises stressing the private sector, dependencies and their implications for regional resilience. These discussions would be designed to build the private sector participation in the Partnership.

c) The U.S. Department of Homeland Security should provide its Office of National Capital Region Coordination, as the only governmental body with a truly regional mandate, with

   a. Sufficient staff of government employees and contractors to provide planning, analysis, and evaluation staff support and integration of the regional resilience effort, and

   b. Funding beyond its operational needs and separate from UASI grants to initiate uniquely regional resilience programs to complement those currently being conducted by the state and local jurisdictions and the private sector.

   The very special characteristics that make the NCR nationally and globally significant also argue for special precautions. While a specific programmatic budget line as the ultimate target, initial resources could be made available by other DHS offices needing field sites for exercises, testing, demonstrations and technical assistance programs.

d) The Partnership should convene CI operators, their suppliers, their customers, and appropriate regulators in each CI sector to develop means to reduce the risk of cascading disruptions due to dependencies.

e) The price-regulated CI utilities and the public utility commissions of the NCR should jointly identify procedures for the cost-recovery of security and resilience investments. This effort should be monitored across the NCR so that wherever possible, the efforts in the District and the States are harmonized.

f) Each CI sector should organize a regional coalition, beginning with the banking and finance sector. The financial institutions operating in the NCR should organize an NCRFirst public/private partnership modeled on the existing ChicagoFIRST program. This will both organize this sector and will provide a model and precedent for the other sectors in the NCR. A representative of each of these coalitions would serve as an advisor the coordinating council.

g) The Partnership should appoint a representative to serve as the NCR member of the National Coordination Center of the National Communications System in order to support communications reliability in the NCR and assist in communications restoration during and following a disruption, incident or special event.

h) The Partnership, through its members and secretariat, should aggressively monitor the progress of other regional partnerships being formed around the country for lessons learned and innovative initiatives. The partnership should thoroughly document its organization, processes, issues, and decisions and communicate these to DHS offices in order to advance the state of regional security alliances.

2.4.2 Prevention and Mitigation

a) The Partnership should use Geographic Information Systems (GIS) infrastructure mapping and other modeling techniques to analyze critical infrastructure services in the NCR. This will offer senior leaders a clear roadmap of infrastructure dependencies and impacts and show how best to allocate resources before, during, and after emergencies.

b) The BoT should expand the current continuity of operations training with training in risk management and coping with dependencies, using the appropriate risk management tools for each sector, starting with the CIs.

c) The SPG and BoT should provide the Partnership with funding for analysis and planning to conduct *regional service level* risk assessments and regional risk reduction. This capability should initially include or be tasked to create the ability to conduct:

- Consistent relative risk assessments of regional service levels and key assets, including the major dependencies with other assets and sectors, with the losses distributed by major jurisdiction and business sector;
- Design of risk reduction initiatives (to reduce vulnerabilities, target attractiveness, and/or consequences of disruption), along with costs of the initiatives and benefits (reduced vulnerabilities, attractiveness or consequences) distributed by major jurisdiction and business sector;
- Prioritization of risk-reduction initiatives accounting for their costs and the synergies and dependencies among them; and
- Monitoring to assure the decisions are implemented and evaluating outcomes to assess whether the reliability of the CIs is rising and the NCR's resilience is growing.

2.4.3 Response and Recovery

a) The Partnership and the BoT should work with the Office of National Capital Region Coordination of the U.S. Department of Homeland Security to implement credentialing of management and technical staff of CIs in the NCR who would need access to controlled areas during an emergency to sustain or restore service.

b) The Partnership should establish a permanent, coordinated operational management mechanism for the NCR which effectively links local level, state level and federal emergency operations centers, response agencies and first responders from the private sector charged with continuity and restoration of essential services. This mechanism should design, develop and extensively exercise an integrated regional command, control and public information system.

c) The representatives of the private sector who sit with the region's Emergency Operations Centers should meet periodically as a group to coordinate policies, practices, and lessons learned.

d) The SPG and key representatives of the Regional Emergency Support Functions should participate fully in the private-sector-oriented discussion-oriented exercise described in Recommendation "Planning and Decision-making a)", above**,** to assure a shared perspective on CI dependencies and their impact on their ability to provide first response and long-term essential services.

e) The jurisdictions of the NCR should develop the means for the most effective participation of the private sector in their EOCs in order to accelerate restoration of essential services during and after a disruption.

2.4.4 Community Engagement

a) The SPG and the BoT should expand the BoT's personal and family preparedness program to include credibility building for state and local agencies' ability to manage emergencies.

b) The SPG and local jurisdictions should determine the *criteria* for evacuation vs. sheltering-in-place and develop and widely disseminate these results.

c) The SPG and local jurisdictions should extensively *publicize and exercise* public evacuation and shelter-in-place plans. The public must know what course of action to take ahead of time.

d) The SPG and at least one local jurisdiction should conduct a detailed feasibility study of community shielding and the use of a local shopping center as emergency shielding/supply support/medical centers. Based on this study, one or more discussion-based exercises, followed by an operations-based exercise, should be conducted. If successful, the exercise should be scaled up to a demonstration project and evaluated after a year or more of operation.

e) The SPG should periodically (no less frequently than biennially) re-survey the NCR populace to see if there is a positive trend in credibility and confidence of the public.

2.5 Dependencies among Sectors

An overarching theme in critical infrastructure protection and regional resilience is the significance of dependencies and interdependencies among infrastructure sectors, and so merits a special discussion in this section.

A dependency exists when one sector relies on another for an input essential to providing its service, and an interdependency exists when two or more sectors rely on one another to provide their essential services. The words are used interchangeably in this report because dependencies often form "chains' that link back though other sectors

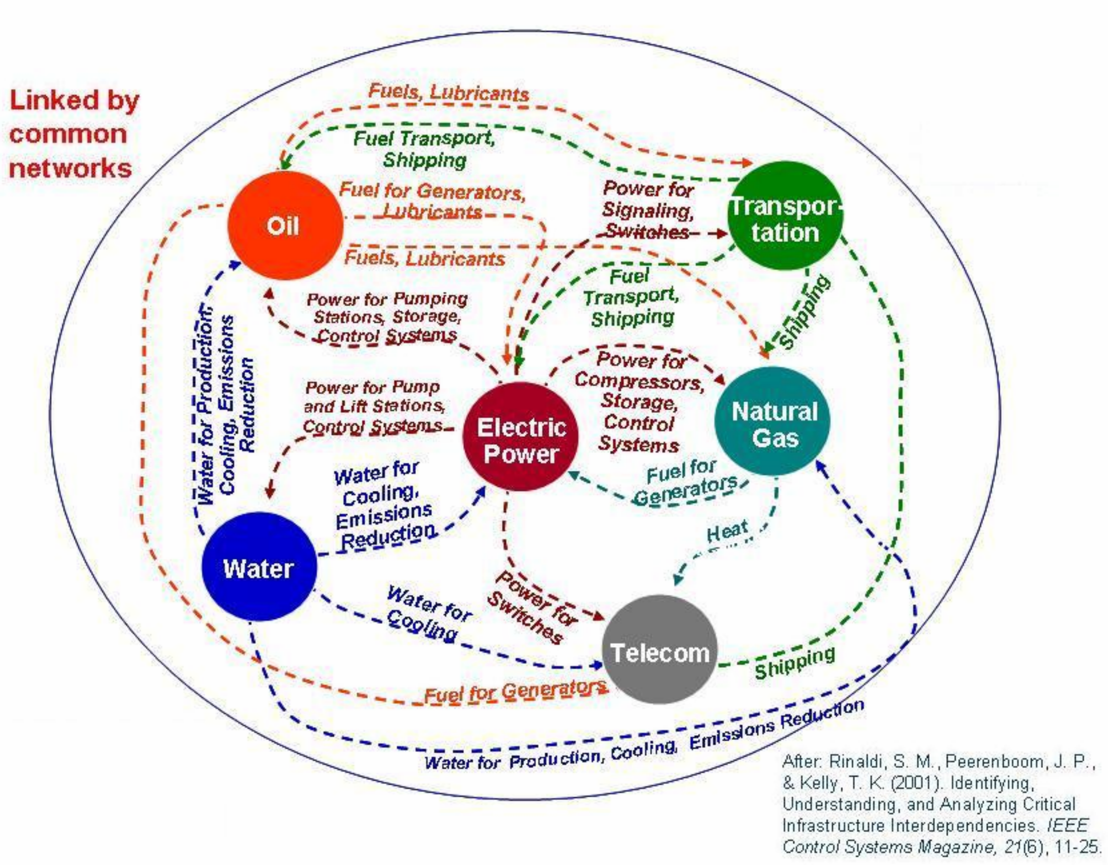
Understanding dependencies is an essential to risk reduction. This understanding requires cooperation across sectors, across the public/private boundary, and across jurisdictions to achieve the joint decision-making and coordinated actions required to enhance resilience, robustness and reliability of the NCR's infrastructures.

There are several types of dependencies, but most common are those created by co-location of infrastructures, supply chain (functional) relationships, cyber (electronic information) or mutual dependence on a third party (e.g., regulatory).

Infrastructures are often co-located to share right-of-ways, thereby containing costs and minimizing environmental, economic and political disruption of eminent domain proceedings. Often, major bridges and highways hold the same advantages for infrastructure developers. It has only been in the heightened security awareness since 9/11 has this practice of sharing right-of-ways come to be seen as a source of vulnerability.

Dependencies from supply chain or cyber relationships exist when one infrastructure's services or products are required for another infrastructure to produce its services and products. As illustrated in Figure 1, each infrastructure has many connections with others. Both direct and indirect links can lead to the conclusion that virtually all infrastructures are interdependent with all others, and with other organizations in their own sector.

Figure 1. Functional Interdependencies


Linked by common networks
Fuels, Lubricants
Fuel Transport, Shipping
Oil
Fuel for Generators, Lubricants
Fuels, Lubricants
Power for Signaling, Switches
Transportation
Fuel Transport, Shipping
Shipping
Power for Pumping Stations, Storage, Control Systems
Water for Production, Cooling, Emissions Reduction
Power for Compressors, Storage, Control Systems
Natural Gas
Power for Pump and Lift Stations, Control Systems
Electric Power
Fuel for Generators
Water for Cooling, Emissions Reduction
Heat
Water
Water for Cooling
Power for Switches
Telecom
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

After: Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine, 21*(6), 11-25.

2.5.1 Hurricane Isabel Demonstrates Cascading Failures due to Dependencies

The NCR's experience with Hurricane Isabel (see Volume 20, "*Hurricane Isabel Critical Infrastructure Interdependency Assessment*") illustrates the propensity of interdependent infrastructures to suffer "cascades" of failures. During Isabel, cascading failures were experienced in the region highlighting the significance of electric power as a principal infrastructure input for water utilities. The Fairfax County Water Authority (FCWA) experienced a prolonged power outage, causing a shut-down of a pumping station. This prevented water from reaching customers as the system is not gravity driven, but rather relies on electricity for its functionality. Nearly one third of their customers were without water for about eight hours.

Although customers were advised to boil water to ensure safety, this was impossible for many customers who lacked gas – which relies on electricity for pumps and controls – or electricity to operate stoves. Furthermore, health services depend on water for many things: drinking, bathing, cooking, etc. They also rely heavily on laundry facilities to provide clean linens. These facilities require water, and are unable to function without it. During Isabel, disposable linen in the hospitals was depleted within 6-12 hours. Hospitals had to consider redirecting new patients to other facilities that had water and electricity services and/or transferring current patients. The cascading failure stemming from the loss of power underscored the interdependence of the region.

2.6 Conclusion The national capital region is a reality – its position in local, national and global affairs are readily recognized. Its people, businesses, institutions and infrastructures are intimately inter-connected across city, county, and state lines. The National Capital Region as an entity that can advance the resilience of the critical services, however, does not exist at present. No single institution or coordinated set of institutions is fully able to prepare, prevent, protect and restore vital services on which depend the region's physical and economic well-being and its national and global roles. The recommendations made here are directed to creating robust, capable institutional structure – a public/private/non-profit partnership – along with a series of planning and operating procedures to make the NCR a resilient region and a model for other regions.

Additional findings and recommendations that relate to the eight specific sectors studied in detail are summarized in the next section and described in greater length in the respective sector reports.

3 FINDINGS AND RECOMMENDATIONS FOR CRITICAL SECTORS

3.1 Introduction

Teams of experts in each of the assigned eight critical infrastructures reviewed the security literature in their specialties and investigated their state of vulnerability assessment and risk management and resilience in the NCR by interviews or focus groups or both with key managers of the infrastructures. The state of risk management was assessed relative to five broad questions:

1. Are the owners and operators of the sector aware of the value of critical infrastructure protection?
2. If they are aware, do they have available a comprehensive set of tools, procedures, and processes for vulnerability assessment and risk management? What is the nature of the tools, procedures, and processes being used (using a rough scale from broad policy guidance, through compliance-oriented procedures, to relative risk management, to full risk management, as defined in Appendix C)?
3. If comprehensive tools are available, are they used in a process that appraises, selects and allocates human and/or financial resources to risk reduction programs?
4. If resources are allocated, are the risk reduction programs implemented in a timely, effective manner?
5. If the risk reduction programs have been or are being implemented, are their results in terms of reduced risk being evaluated for effectiveness and enhancement in reducing risk and increasing resilience?

These questions are cumulative, providing a rough gauge of the state of vulnerability assessment and risk management. Affirmative answers to all the questions indicate an advanced state of risk management, while increasing negative answers would indicate a lower state. In general, wherever along the scale the answers turn from affirmative to negative suggests the point at which to begin work to further the state of vulnerability assessment and risk management in the sector.

Both within sectors and across sectors, there was significant variation in the state of vulnerability assessment and risk management. The healthcare and public health sector is the least advanced of the sectors studied, largely due to its extensive redundancy and geographical dispersion. Banking and finance and telecommunications, by contrast, exhibit a very high level of risk management sophistication, possibly due to their close working relationships with government agencies that stress reliability and risk management. The other sectors fall between these extremes.

The results of these appraisals are summarized for the respective sectors in Appendix D and discussed at greater length in the seven sector reports (postal and shipping was combined with transportation) that are part of the present report series (volumes 2 through 8). The major findings and recommendations of the expert teams about vulnerability assessment and risk management, and resilience are reported below.

3.2 Energy Sector

Each energy infrastructure in the NCR (electric power, natural gas and petroleum products) is itself made up of complex physical, cyber, institutional, functional and human networks – a network of networks – owned and operated by both public and private organizations.

For the most part, the electric transmission and distribution facilities are above-ground and visible; the natural gas and petroleum products transmission and distribution facilities are below ground and out of sight. All fossil fuel products come into the area via pipelines, train, and trucks from outside the NCR. In the electric power sector, fuels are brought into the NCR via pipeline, train, and truck. Northern Virginia, the District, and Western Maryland do not generate sufficient electric energy to serve the NCR loads; therefore, high voltage transmission lines are also needed to bring electric power into the NCR.

An extensive array of Federal authorities, acts, and statutes relate to either the energy infrastructure generally, or the electric, natural gas, and petroleum sectors specifically. Regulatory authority in the energy sector is shared between Federal, state and local jurisdictions, with Federal oversight focused on interstate aspects. District and state regulatory authority is primarily serviced through three regional public utility commissions. Commission authority can encompass utilities, insurance, and it also includes monitoring operations and setting rates for investor-owned gas and electric utilities. In addition, one electricity cooperative and one municipally-owned electric utility serve customers in parts of the NCR.

The Energy Sector team first conducted a literature search to identify and obtain publicly available documents relating to both energy infrastructure security and vulnerability assessments. Energy industry personnel were then interviewed to document their organization's activities and experience related to vulnerability assessments. These activities, which focused on the assessment process rather than firm-specific details, resulted in the following three findings and recommendations.

3.2.1 Key Findings

1. *Publicly available methodologies examined, with two exceptions, do not adequately address the area of infrastructure interdependencies, either within a single sector or among infrastructures.* How the methodologies actually used by NCR electric utility organizations handle this aspect is presently unknown. Therefore, the actual vulnerability of infrastructure interdependencies in this area is still unknown outside the specific.
2. *The energy infrastructure organizations interviewed did not normally interact with upstream suppliers of critical services during the assessment process.* The assessment process was conducted to the organization's physical property lines, to common interconnection points, and no further. None had been invited to participate in other infrastructure organization's process where they were a critical supplier to the other organization.
3. *Considerable action by the federal government – Federal Energy Regulatory Commission and the Rural Utility System – and industry organizations – North American Electric Reliability Council –is expected to result in increased security-related actions, including conducting vulnerability assessments by electric utilities before the end of July 2005.* However, it is not clear whether any action will be taken to validate these actions or certifications.

4. *Electric utility personnel, emergency managers, and NCR Emergency Operations Center (EOC) personnel again brought one aspect identified in a number of earlier NCR-related infrastructure studies: the high failure rate of on-site emergency generation facilities at both public and private facilities.*

3.2.2. Key Recommendations

1. *A model "methodology framework" should be developed that includes all the areas (range and depth) that need to be considered; the framework should be compared to actual methodologies used by the NCR infrastructure organizations and modifications made where necessary.*
2. *All vulnerability assessments should include participation of critical upstream suppliers from the same and other infrastructures.*
3. *An independent monitoring and review pilot program should be initiated in order to assess and document electric utilities' (private, public, and cooperative) response to increased federal security recommendations and guidelines.*
4. *An in-depth survey of on-site emergency generators needs to be conducted – units tested and refueling strategies developed to increase the reliability and security of the hundreds of existing emergency units in the NCR.*

3.2.3 Conclusion

The energy sector is arguably a 'first among equals' in the critical infrastructure universe. Almost all energy sector stakeholder firms are actively pursuing programs to enhance their organization's security, including both physical and cyber aspects. However, there is generally insufficient awareness of the importance of incorporating upstream and downstream sectors into these analyses, and the potential for interdependent failures is not fully appreciated. Additional awareness-raising and tools to identify these specific factors is needed to remedy this deficiency.

3.3 Water and Wastewater Sector

The water sector in the National Capital Region (NCR) is complex. It comprises many water supply and wastewater utilities that range in scale from three utilities that serve more than one million people each to individual homeowners who have their own wells and septic systems. The water infrastructure sector includes not only significant physical facilities—pipes, pumps, treatment works, storage tanks, etc.—but also significant information/cyber assets, all managed by people in multilayered organizations.

The water infrastructure is ahead of some other critical infrastructure sectors with regard to formal vulnerability assessments, and perhaps risk management. It was federally mandated to conduct vulnerability assessments of water supply utilities no later than June 2004. Although wastewater utilities were not required to complete these assessments, many did so.

The water infrastructure is essential for the continued viability of the NCR. Residents of the NCR require safe, dependable drinking water and the disposal of wastewater to survive. Every other critical infrastructure system is dependent on the water infrastructure, and conversely water infrastructure is dependent on most other infrastructure sectors.

The NCR-CIP Water Sector Team conducted an extensive literature review, and held a series of interviews with groups of experts and leaders of the water sector. The results of these led to the following findings and recommendations.

3.3.1 Key Findings

1. *Inter-sectoral and intra-sectoral dependencies are important and need further exploration.* The water sector includes a large range of service providers that are interdependent. Because of political and physical characteristics of the NCR, these interdependencies between providers vary. All other infrastructure sectors depend directly on the water infrastructure sector. The water infrastructure sector directly and indirectly depends on the other infrastructure sectors. The dependencies within the water sector and especially between the water sector and other infrastructure sectors are critical to the functioning of NCR critical infrastructure and need better understanding.
2. *Improved procedures for conducting and implementing vulnerability assessments and risk management are needed.* Although a group of tools for conducting vulnerability assessments has been developed and used, there is a need for improved tools and procedures. Evolution from vulnerability assessment to risk management, and industry standards for the conduct of these methods/procedures are needed.
3. *Better communication is needed between threat-assessing agencies and the water sector.* Communication between threat assessment authorities, law enforcement agencies, and the water sector needs improvement if the vulnerability assessment/risk management procedures are to be meaningful.
4. *Improved mechanism for funding risk reduction that protects sensitive information about vulnerabilities from public disclosure is needed.* A common funding mechanism for water sector expenditures requires the public disclosure of the amount of and the reasons for the expenditure. This may result in the identification of existing vulnerabilities.

3.3.2 Key Recommendations

1. Improve funding mechanism for risk reduction to protect sensitive information about vulnerabilities from public disclosure.

2. Improve communication between threat-assessing and law enforcement agencies and the water sector

3. Institute regular tabletop exercises to illuminate and respond to intra-sectoral and inter-sectoral dependencies.

4. Establish special procedures for rate-setting to recover the costs of security investment.

3.3.3 Conclusion

The water sector is critical to the viability of the NCR. Immediate action should be taken on these key recommendations—as well as other recommendations in the full sector report—to enhance the security, resiliency and business continuity of this critical infrastructure.

3.4 Transportation / Postal and Shipping Sector

Transportation/postal and shipping infrastructures in the U.S. are critical in that they support national defense, move people and goods, employ millions of people, generate revenue and consume resources and services generated by other sectors of the economy. Consequently a reduction in service or loss of an asset in the sector either from natural disasters or terrorist attacks could have catastrophic consequences in terms of loss of life, long-term economic losses and national security.

Surface transportation in the NCR has a particular set of vulnerabilities to terrorist attacks, similar in many regards to the vulnerabilities of surface transportation in any major, well-developed metropolitan area. These vulnerabilities include:

- Traveler Exposure – Public transportation by its nature collects large numbers of people into small areas, rendering them vulnerable to various types of terrorist attacks.
- Regional Mobility Impacts – There are several bridges, interchanges and intersections whose disablement would severely impair travel within the region. Depending on the severity of the damage, disruption of traffic could continue for days or even weeks, shutting down not only commercial activity but vital functions of the federal government.
- Freight Movement Disruption – Should terrorist objectives evolve towards economic disruption, attacks on freight transport could become a serious problem, involving, in particular, assaults on hazardous material conveyance. Like passenger conveyors, freight conveyors travel over long routes which by their nature are impossible to monitor and harden in their entirety.
- Method of Delivery – Through hijacking, subterfuge, or even use of a legitimate Commercial Drivers License, terrorists could seize control of truck or train car carrying a toxic or explosive hazardous material and direct its lethal content to a pinpointed target.
- Costs – In most scenarios involving terrorist attacks there are likely to be both immediate and sequential costs. Immediate costs would include loss of life, injury and illness, and property damage. Sequential costs include vitiation of commerce, and undermining of confidence in a region’s or nation’s institutions.

3.4.1 Key Findings

1. *Inherent characteristics of transportation infrastructure create significant challenges.* Prevention of terrorist attacks is a particularly difficult task in an open and democratic society like ours, with our extraordinary attention to individual rights and individual privacy, and our strong aversion to group profiling. Even if the political and cultural resistance to strong preventive measures to be overcome, there would be major economic costs.
2. *Need for Transportation Infrastructure Security Strategies Imperative.* The potentially massive costs of terrorist attacks, as revealed on September 11th, make it imperative that we develop strategies for prevention. At this point in time, what seems to be the most sensible approach for the NCR to take is begin a serious assessment of risks of terrorist attacks on the region’s transportation system, and a strategy for managing these risks.
3. *Response activities are critical.* An efficient and adaptable transportation system is essential to effective response in most types of terrorist attacks. First responders need prompt access

to the scene of destruction, as will needed follow-up services. Additionally, the need to move population groups requires the capability to establish alternate routes to compensate for routes temporarily interdicted will be necessary.

3.4.2 Key Recommendations

1. *Designate and insure adequate funding for CapCOM which enables it to serve as the center for coordination of regional transportation communication, drawing, as it sees fit, on such resources as the Regional Integrated Transportation Information System.*
2. *Develop procedures that insure that, to the greatest degree possible, practices and procedures agreed to by the different jurisdictions of the region through CapCOM be implemented by the jurisdictions.* Such implementation may best be achieved through appropriate Memoranda of Agreement, Memoranda of Understanding, or changes in the regulations of participating jurisdictions. Critical to the success of such initiatives is that the planning process and the operational activities be brought into closest possible cooperation.
3. *Create, or designate, the organization and appropriate staffing to evaluate various risk management tools currently available to the NCR, and charge this group with choosing the one or more tools that are most appropriate.* Further, insure that the tools are applied to the region and a suitable risk management strategy is developed.
4. *Provide the mechanism, staff, and resources to insure that the application of these tools, and the risk management strategy, is continually revised to keep pace with changing conditions and evolving technologies.*

3.4.3 Conclusion

The economic well-being and security of the NCR is dependent on the vast transportation network in the region. Immediate actions on the above recommendations should be taken to help foster the safest and most efficient possible movement of people and goods.

3.5 Health Services Sector

The National Capital Region (NCR) Health Services Sector is comprised of over 20 thousand “points of service”. These include hospitals, nursing facilities, ambulatory clinics, pharmacies, laboratories, private professional offices, and a plethora of other kinds of organizations. The substantial redundancy and geographic dispersion of points of health services and of the workforce across the NCR serves as an advantage in a catastrophic event. While a specific incident may destroy some geographic health services resources, duplicate and redundant services exist adjacent to an area of loss.

Normally these mostly private sector organizations are competitive, focused on providing acute, chronic, and rehabilitative services and products to individuals and families. Less visible than these clinical care functions are the sector’s Public Health community population-directed functions. A catastrophe within the region swiftly changes the normal pattern. The “center of gravity” shifts from the acute care provided by a plethora of private healthcare organizations and practitioners to the regions’ under funded and loosely articulated public health elements.

The workforce is the sector's most critical asset. It possesses the skills to mitigate the mortality and morbidity of destructive events. Their numbers, geographic distribution, and range of skills can be leveraged to the benefit of the health of the region. This sector is one of the region's major employers. Tens of thousands are dependent on the sector for jobs and economic security.

Developing a resilient health services sector prepared for a range of hazards requires finding new points of balance in the midst of countervailing pressures and contrasting operating values:

- Shifting from a preoccupation with acute care to the building of vital Public Health structures and resources.
- Tempering the climate of competition with values and benefits of collaboration.
- Balancing "open access" with the need for controlled access and protection.
- Breaking out of day-to-day "silos" and thinking "systems".
- Mobilizing the political will to transcend jurisdictional constraints for the benefits of a regional perspective.

3.5.1 Key Findings

1. *Health-sector workforce is ill prepared and trained for biological, chemical and radiation threats.* The findings are consistent with numerous studies of physicians, nurses and other health professionals. Most judge themselves ill prepared. The preponderance are concerned that their immediate medical communities are not prepared.
2. *Public Health community-level population-directed functions are under funded and loosely articulated for confronting challenges of Weapons of Mass Destruction (WMD).* The WMD threat has placed an added unfunded burden on health services organizations and professionals funded from acute and chronic services revenues sources. Vulnerability assessment and preparedness planning can be a significant expense. Much of the preparedness planning and mitigation is not directly related to day to day revenue producing activities of healthcare organizations.
3. *Neutral collaborative forums are needed to facilitate alignment of interest and resources between and among Public Health agencies and private healthcare organizations, and across entrenched geopolitical entities.* Most healthcare is offered by private organizations and professionals. Past efforts to improve the regionalization and integration of the health services planning and delivery has met with limited success. The most vexing challenges relate to working within and around strong geopolitical demarcations.

3.5.2. Key Recommendations

1. Develop a NCR Public Health based "Command and Control" utility that picks up from EMS and attends to population level intermediate and long term phases of recovery.

2. Develop electronic Weapons of Mass Destruction training resources for health professionals.

3. Standardize NCR workforce credentialing and develop a database of proximate points of service to individuals work and residence locations would aide region wide preparedness planning.

3.5.3 Conclusion

The health services sector is in the early period of dealing with the unfolding realities of malicious threats. Three underlying challenges will greatly determine progress in improving the preparedness of the NCR; effective regional collaboration and governance, a strategic plan and investments in a regional robust Public Health infrastructure, and development of population-level community-focused medical and health-care delivery.

3.6. Emergency Services Sector

The National Capital Region (NCR) is recognized as a leading target for terrorist attack.

The Emergency Services Sector (ESS) is the first line of defense against natural and man-made disasters. First responders' coordinated functions of detection, assessment, alerting and dispatch are key to the security of residents, and crucial to sustaining the region's quality of life and economic development. Enhanced emergency response has been a first priority for homeland security investment – initially, in the form of equipment procurement and specialized training.

The inclusion of emergency services as a critical infrastructure recognizes the ESS as a service delivery system. The ESS is made up of sub-sector systems: Emergency Management, Law Enforcement, Fire and Rescue (including Hazardous Materials and Search and Rescue), and Emergency Medical Services. In light of the expanded range of threats and experience of large-scale disasters, the domain of emergency services in the National Capital Region also includes Public Health, Public Works and Social Services Departments at the local level. The sub-sector workforce and resource systems are integrated at the twelve local NCR jurisdictional levels. The extent of inter-jurisdictional coordination varies between the sub-sectors.

On the basis of review and analysis of relevant documents, and interviews with key ESS leadership in the NCR, a number of specific findings have been revealed and recommendations developed to help assess and enhance ESS effectiveness in the NCR.

3.6.1 Key Findings

1. Emergency services agencies do not traditionally view themselves as an infrastructure. While there have been vulnerability assessments and response training exercises directed toward others, *little attention has been paid to the specific vulnerability of emergency services organizations themselves to loss of services due to critical infrastructure system failure.*

2. *Local or state-level agencies have not developed an integrated regional system of emergency services delivery.* Local, state and federal response agencies must share the vision of a regional ESS infrastructure.

3. *The complex inter-governmental relationships of the National Capital Region pose a major challenge for efficient, effective regional emergency response to large-scale threats.* Notwithstanding well-working mutual aid agreements between Fire Departments of adjacent jurisdictions, Local efforts require support and coordination from the state and Federal levels.

3.6.2 Key Recommendations

1. *Develop a coordinated operational management mechanism for the NCR that effectively includes local level, state level and federal response agencies.*
2. *Develop a dynamic, real-time, GIS-based common operating picture (COP) for the National Capital Region to optimize application and deployment of emergency response.*
3. *Organize and train private sector and citizens to augment ESS resources for large-scale response including shelter-in-place.*
4. *Establish permanent mechanisms for consultation between emergency services and each of the other critical infrastructure sectors to identify and resolve potential ESS vulnerabilities.*

3.6.3 Conclusion

The primary mission of the Emergency Services Sector is to save lives and protect property and assets. The capacity of Emergency Services to fulfill this mission is most centrally affected by, and so vulnerable to, its ability to remain agile, flexible and consistently coordinated in the face of a wide range of threats and hazards. The under-scrutinized dependency of Emergency Services upon critical infrastructure is the single most important topic of potential vulnerability revealed in this study.

3.7 Telecommunications Sector

The area of service for providers in the NCR varies – for example, some provide only local infrastructure and services while others extend internationally. There are local service providers, long distance providers, internet service providers and wireless service providers. The sector is dominated by a handful of very large firms such as AT&T, MCI, Nextel, Sprint, and Verizon.

There are roughly 1100 establishments in the NCR that fall under the category of communications as defined by the 2-digit Standard Industrial Classification (SIC) code 48. This includes all firms related to telephone communications, telegraph and other message communications, cable and other pay television services as well as other communications services not elsewhere classified. These establishments are scattered across the region although some clusters are located along major transportation corridors.

In 2003, there were 196,890 persons employed in the Information Technology sector: 110,729 in Virginia, 59,164 in Maryland and 26,997 in the District of Columbia. A more detailed breakdown of these figures by sub sector is available through the Bureau of Economic Analysis. The telecommunications sub sector employment in Virginia is 40,138, Maryland is 22,991, and the District of Columbia is 4,638. There are 1617 fiber lit buildings fairly evenly distributed throughout the region. The region has 44 co-location facilities, 76 carrier points-of-presence (POPs) and 209 wired connection centers. Most of these facilities are located along the main transportation lines, many west of the District of Columbia and within the Dulles Corridor.

3.7.1 Key Findings

1. *Active involvement by industry and government in critical infrastructure programs.* The government has sponsored and is currently sponsoring forums for private industry and the government to work through common issues involving CIP. Examples include National Security Telecommunications Advisory Council (NSTAC), Network Reliability and Interoperability Council (NRIC), and National Coordination Center for Telecommunication (NCC). Private Industry has also invested resources on their own to review and develop new standards and business processes as mentioned above.
2. *Risk Management/Business Continuity are important to this industry since stable reliable infrastructure is a key attribute to successful business for the Telecom sector.* These processes were established and incorporated into business plans and operations prior to September 11th. The aftermath of September 11th has increased the activities/assessments in risk management/business continuity models overlaying terrorist threats modes.
3. *The National Capital Region (NCR) has had special activities that require the assistance of the communications sector.* The NCR has unique activities that require the assistance of the telecom sector. The NCS/NCC for daily activities and in special events should be a focal point for telecommunication needs for the NCR. The NCC will be able to provide a vehicle for specific needs during an event/crisis or preplanning required for an event/crisis. The NCR could benefit from the ongoing vulnerability and risk assessment activities conducted at the NCC with the participation of the private industry.

3.7.2 Key Recommendations

1. Create a single Point of Contact (POC) for perimeter control process and, once established, maintain the process; eliminate the need to change the process during the incident or function.

2. Increase the NCR's awareness about the services the NCS/NCC performs for the government and the communications sector and those that rely on telecommunications services.

3. Encourage the participation of a senior representative from the NCR in the NCS/NCC and utilize the NCS/NCC as the single point of contact for any communications issues of national security and emergency preparedness within the region.

4. Conduct tabletop exercises – interdependencies with other sectors. Expense reimbursement funding for sector participation at the exercise should be part of the process design to enable success.

3.7.3 Conclusion

The telecommunications industry and the government have recognized the importance of telecommunications as a critical infrastructure for a long time. Immediate action taken on the above recommendations will enhance the security, resiliency and business continuity of this critical infrastructure.

3.8 Banking and Finance Sector

The infrastructure of the financial services sector consists of a variety of physical structures, cyber as well as human capital. The physical structures to be protected contain retail or wholesale banking operations, financial markets, regulatory institutions, and physical repositories for documents and financial assets. Today's financial services companies conduct the payment and clearing and settlement systems and are primarily electronic, although some physical transfer of assets, such as checks and cash, still occurs. This infrastructure includes such electronic systems as computers, digital storage devices, and telecommunication networks. In addition to the sector's key physical and cyber components, many financial services employees have highly specialized skills and are, therefore, considered essential elements of the industry's critical infrastructure.

An integral part of the banking and finance sector is the federal and state regulatory and supervisory community because of the reliance of the economy on the payments system and the severe adverse economic consequences of the loss of public confidence in the financial system. The federal regulatory agencies, such as the Federal Reserve Board, Office of Comptroller of the Currency, Office of Thrift Supervision, National Credit Union Administration, Securities and Exchange Commission, Commodities Futures Trading Commission and the Treasury Department, are all located in the National Capital Region (NCR) and concentrated in a very short radius of the White House. Private institutions such as Bank of America, Capital One, Chevy Chase, E*Trade, GEICO, PNC, State Farm, and Wachovia, and several credit unions also have major operations in the NCR. This high degree of geographical concentration is alleviated to some degree by the geographic dispersion of the regional offices of the federal banking regulators and private institutions with offices in major metropolitan areas and the wide dispersion of state regulatory bodies.

The NCR-CIP Banking and Finance Sector team conducted an extensive literature review and held two focus groups engaging high-level representatives from the federal and state financial services regulators, trade associations, and banking institutions. These activities resulted in the following three findings and recommendations.

3.8.1 Key Findings

1. *Need for a single point of contact and communication structure among institutions regarding homeland security and critical infrastructure protection.* A regional coalition in the NCR is necessary to build cooperation relevant to homeland security and critical infrastructure protection among the banking and finance firms, their regulators, those critical to its business continuity, and appropriate federal, state, and local government agencies. ChicagoFIRST is a suitable model for the Banking and Finance Sector in the NCR largely because the development and implementation of a single point of contact and the establishment of a communication structure among institutions, governmental bodies, and first responders has been, and continues to be, successful for homeland security and critical infrastructure protection.
2. *Potential denial of access to restricted areas during and immediately after an emergency.* One of the major problems within the financial services sector of the NCR identified by the focus groups is credentialing key NCR banking and finance personnel to access restricted areas to maintain or restore operations during and immediately after an emergency.

3. *Limited understanding of interdependencies in the NCR.* There is a need for private sector tabletop exercises focusing on interdependencies amongst critical infrastructures and state and local jurisdictions in the NCR. These should be done at the physical, cyber, state and regional levels.

3.8.2 Key Recommendations

1. Improve coordination, cooperation, and communication, by adopting ChicagoFIRST as a model for the NCR.

2. Collaborate with the Department of Homeland Security's (DHS) Office of the National Capital Region Coordination to extend federal credentialing to the banking and finance sector.

3. DHS should coordinate and fund interdependency tabletop exercises at the physical, cyber, state and regional levels, emphasizing the private sector, critical infrastructures and interdependencies in the NCR.

3.8.3 Conclusion

The effectiveness of the financial services sector depends on the continued maintenance of public confidence and involvement to maintain normal operations. Immediate action taken on the above recommendations will enhance the security, resiliency and business continuity of this critical infrastructure.

4 TOOLS FOR VULNERABILITY ASSESSMENT AND RISK MANAGEMENT

Risk-management means developing plans and allocating resources in a way that balances security and freedom when calculating risks and implementing protections. The most effective way, I believe, to apply this risk-based approach is by using the trio of threat, vulnerability and consequence as a general model for assessing risk and deciding on the protective measures we undertake.

Each threat must be weighed, therefore, along with consequence and vulnerabilities. As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities. Our strategy is to manage risk in terms of these three variables – threat, vulnerability, consequence. We seek to prioritize according to these variables, and to fashion a series of preventive and protective steps that increase security at multiple levels.

> Secretary Michael Chertoff, Center for Catastrophic Preparedness and Response and the International Center for Enterprise Preparedness, April 26, 2005

4.1. Criteria for Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures

Literally hundreds of tools and methods exist for conducting vulnerability assessments and risk management of critical infrastructures. They differ widely in terms of approach, scale, and scope. Selecting the most appropriate and relevant for a particular sector, asset, and system is necessary to assure adequate protection and resilience of a critical service, facility or function. This section sketches the nature and completeness of the most widely used tools for those in the public and private sector tasked with risk management for their organizations. An analysis to characterize the most prominent tools relative to standard criteria consisted of the following steps:

- Establishing criteria;
- Identifying a broad set of vulnerability and risk management tools;
- Determining the small subset of tools in the studied sectors that are widely used and accepted by the critical infrastructure owner/operators, referred to as "Good Practice" tools; and
- Analyzing the nature of the available tools, contrasting the properties of all tools analyzed with the traits of the "Good Practice" tools.

In conjunction with the Tool Database this analysis serves as a means to improve the quality of the risk management process by giving users a quick way of comparing and contrasting different tools, and specifically selecting parts or all of them according to their needs. The more complete reporting can be found in Volume 11, "*Criteria and Evaluation of Vulnerability Assessment and Risk Management Tools and Procedures.*"

4.1.1 Major Findings

The primary findings from the assessment were:

- The majority of tools reviewed (a total of 62), both the general list of tools and the "Good Practice" subset, are at the lower end of the risk management continuum defined in Appendix C. This includes simple compliance, through a level of basic analytical risk reduction.

- Two of the few high end risk management tools that include relative risk reduction and relative economic optimization while considering potential threat probabilities and consequences were:
    - Special Needs Jurisdiction Tool Kit, by the Office for Domestic Preparedness, State Homeland Security Assessment and Strategy Program of DHS
    - Risk Analysis and Management for Critical Asset Protection (RAMCAP™), by ASME Innovative Technologies Institute, LLC
- The topic of interdependencies is systematically included in many assessment tools, but is addressed on a rather superficial level. The checklist for interdependencies within the tools is mostly a simple review of dependent utilities and communication lines. The tools give little guidance for understanding the levels of interdependencies and where vulnerabilities may lurk, which is the underlying intention for this guidance.
- Most of the assessments address protecting buildings, facilities and operations, but less than half consider protecting "people". However, most of the "Good Practice" tools systematically include "people" as assets in their calculations.
- A majority of the tools address or measure financial and capacity impacts in their analysis of the consequences of loss. However, environmental degradation is considered in less then a quarter of the cases.
- Of tools surveyed, 75% of the general group and 89% of the "Good Practice" tools use qualitative data (expert assessment and relative ranking scales) rather then quantitative data (a cost/benefit analysis). The associated scales for the threat, consequence and vulnerability factors varied widely across the studied tools and were not readily comparable.
- Very few tools have a wide spread use. Even among the "Good Practice" tool subset, only 33% were accepted as a standard practice in the sector.
- Most of the assessment tools do not take an all threat / hazard approach, but most of the "Good Practice" tools systematically include both man made and natural threats in their calculations.
- Assigning relative and absolute probabilities or likelihoods based on failure analysis is conducted in only about 20% of the assessment tools. This was found in quantifying threats, vulnerabilities, and consequences of loss.

4.1.2 Major Recommendations

To enhance the security and resilience of the critical infrastructure in the NCR, these findings lead to the following recommendations:

- Encourage the evolution of business practices that are currently simple compliance based assessment processes towards using a risk based methodology.
- Establish a common "Consequence of Loss" reference table. The majority of current assessment tools use qualitative data (expert assessment and relative ranking scales) rather then quantitative data (a cost benefit analysis). A common relative scale is required to use these results to compare disparate assets in a region wide risk management program.

- Establish a regional assessment process that can accept and harmonize data from the many different asset level assessment tools. There are so many different assessment tools used on so many different types of assets that it would be cost prohibitive to require each to conduct a new assessment with a new tool. The private owner/operators have also stated strong opposition to assessment tools developed outside of their trade associations or even their control. A regional assessment processes that can accept and normalize the basic data (threat, consequence, vulnerability, risk, and risk reduction) from assessments is required.
- Request and encourage professional organizations (e.g., American Society of Mechanical Engineers, American Water Works Association, Association of American Society of Civil Engineers), and government laboratories and agencies (e.g. Sandia National Laboratory, US Environmental Protection Agency) to develop Good Practices in assigning relative and absolute probabilities or likelihoods based on failure analysis.
- Require assessment methods and tools to assess inter-sectoral dependencies.
- Give priority to infrastructure security strategies and measures that both enhance infrastructure safety and security as well as support or enhance normal operations.

4.2. Database and Architecture for Critical Infrastructure Protection

4.2.1 A Database for Enhancing Risk Management Tools

Conducting vulnerability assessments of complex critical infrastructure – with interdependencies among a variety of sectors such as electricity, water, chemical, transportation, telecom, and related networks – is a challenging task. Owner/operators and industry associations have developed detailed specialized assessment methodologies for their specific facilities or functional area. However, most of these assessment tools do not have specific details regarding functions or infrastructure asset and features outside of the developer's expertise. For example; an assessment tool might be very comprehensive in the area of physical security, but examine relatively little the areas of cyber security or human resource management. This project overcomes this situation by developing a relational database to categorize the components of risk and vulnerability assessment frameworks to allow users a quick way of comparing and contrasting the components of different tools, and enable users to extract selected elements according to their needs.

A database was created to capture the information about the categories, sub-categories, and questions. Sixty-three different vulnerability assessment procedures, processes and tools were loaded into the database at the highest level of categorization. Of these, nineteen tools containing several thousand elements, nominated by the sector study teams, were categorized to the most detailed level. The subsequent database files, a user guide, and installation instructions were recorded on a CD. The database and associated documentation are described more fully in Volume 10, "*A Database and Architecture for Comparing Vulnerability Assessment Elements.*"

4.2.2 Recommendation

The SPG initially and the partnership ultimately should engage a computer support firm to make available, maintain and enhance the database. Additional functionality and additional tools should be entered continuously in response to users’ suggestions and the evolving field of risk management.

5 REGIONAL RISK MANAGEMENT AND RESOURCE ALLOCATION ANALYTICS

5.1 Underinvestment in Critical Infrastructure Security – the Public Good Problem

The critical infrastructure sectors of the NCR vary widely in their approaches to vulnerability assessment and risk reduction. The area of greatest underestimation and underinvestment is interdependencies – the reliance on other sectors' performance to continue to provide critical services. These interdependencies create a class of market failures that economists call "externalities" – cases where the party making an economic decision, like an investment in CIP, does not include ("internalize") all the benefits and costs of the decision in his decision calculation distorting the decision from what would be socially desirable.

5.2 Regional Risk Management

Among the most pressing CIP needs in the NCR is establishing an overall management framework for coordination of NCR-CIP initiatives, developing methods for defining and estimating the magnitude of risks to infrastructures, evaluating the merits of risk-reduction programs and projects, and allocating resources to those with the greatest value relative to their cost. Because the vast majority of critical infrastructures are privately owned and operated, these methods need to include ways for firms to make a business case for investing in risk reduction.

5.3 Risk Management Definitions

Modern risk management defines risk is a combination of threat, vulnerability, and consequence.

Risk = [Threat x Vulnerability] x Consequence

Where:

- Threat is a measure of the likelihood that a specific type of attack or natural disaster will be initiated against a specific target (that is, a scenario).
- Vulnerability is a measure of the likelihood that various safeguards against that scenario will fail.
- Consequence is the magnitude of the negative effects if the attack is successful.

The purpose of risk management is to reduce risk. Risk is reduced whenever any of the three defining terms is reduced. Threat can be reduced, for example, by reducing the value of the target to an adversary or removing the ability of an adversary to mount an attack. Vulnerability can be reduced by securing the perimeter of an asset, developing "buffer zones", "hardening" the asset to better withstand an attack.

Consequences can be reduced by increasing redundancies of supply of essential services, reducing geographical concentrations of infrastructures along certain right-of-ways and bridges, building strategic inventories, shortening the outage period, reducing restoration costs, building assets to codes that are more resilient to attack, etc. However risk is reduced, the benefit of risk reduction is the difference in risk, as defined above, due to the risk reduction investment of resources.

5.4 Concept

Funding of risk reduction can be conceived in three broad cases. These cases, illustrated in Figure 2 and Table 1**,** are:

- *Business Optimal*. If both the owners and the region's benefit/cost ratios are substantially greater than one (or the conventional decision criteria of that sector, e.g., return on investment meets the operator's standard), the operator's business case is made and he will make the investment – provided the operator can recover the costs of the investment, a serious challenge for price-regulated utilities.
- *Business Induced*. If the ratio is about one, even slightly less, the operator may be induced or compelled to make the investment through incentives, such as subsidies, standards tied to accreditation, insurance rates, credit ratings, or eligibility qualifications to conduct certain lines of business.

Regional Optimal. If the benefit/cost ratio for the operator is substantially less than one and cannot be induced, but substantially greater than one for the region as a whole, the operator will not invest unless reimbursed by others – government agencies if the benefits are widely dispersed, or other sectors or customers, where sufficiently concentrated to make *their* benefit/cost ratio favorable.

Table 1. Three Cases Affecting Operator's Willingness to Pay for CIP Investments

Case	Benefit / Cost ratio	Owner/Operator	The Public or NCR as a Whole
Business Optimal	**B/C > 1.0 for owner** **B/C > 1.0 for region**	Will invest	No action necessary
Business Induced	**B/C ~ 1.0 for owner** **B/C > 1.0 for region**	Needs incentives to make the business case	Need to provide incentives or inducements
Regional Optimal	**B/C < 1.0 for owner** **B/C > 1.0 for region**	Will not invest	Need to invest directly

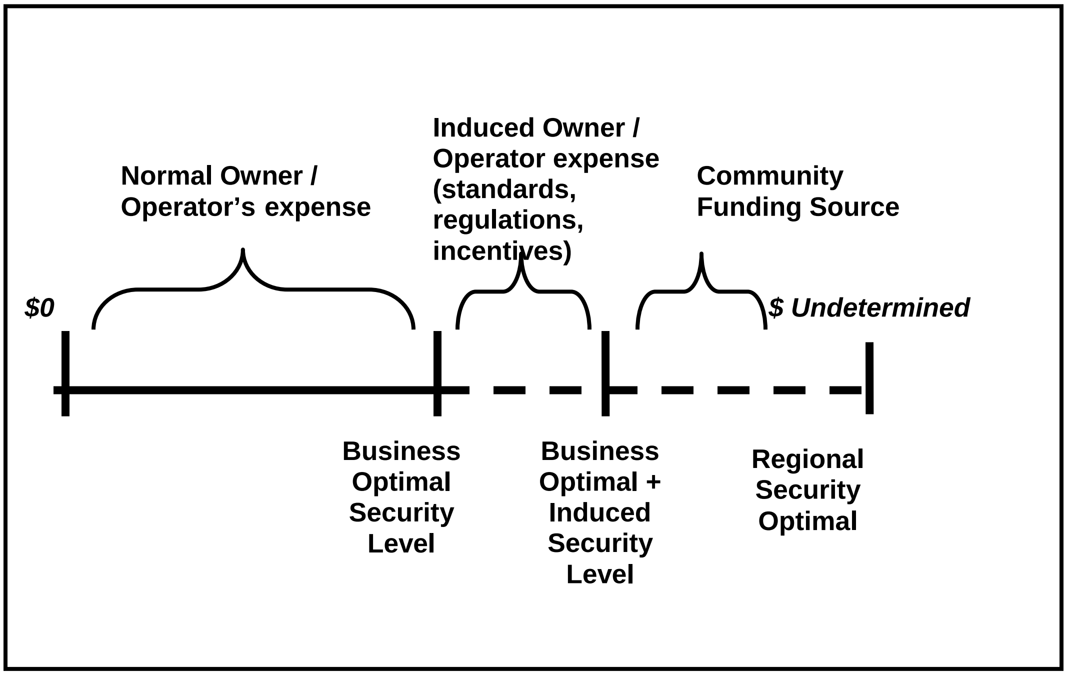

Normal Owner / Operator's expense
Induced Owner / Operator expense (standards, regulations, incentives)
Community Funding Source
$0
$ Undetermined
Business Optimal Security Level
Business Optimal + Induced Security Level
Regional Security Optimal

Figure 2. Financing Infrastructure Risk Reduction

5.5 Regional Risk Management Analytic Process

The analysis team addressed this challenge in two ways:

1. CIP/DSS. First, we examined the only known regional risk management tool, the Critical Infrastructure Protection Decision Support System (CIP/DSS) being developed by three National Laboratories. This is a system dynamics modeling of virtually the full economy of a metropolitan region, with detailed representation of the critical infrastructures. The method requires extensive data collection to "parameterize" the models and is so complex that it is offered only as a service by the Laboratories.

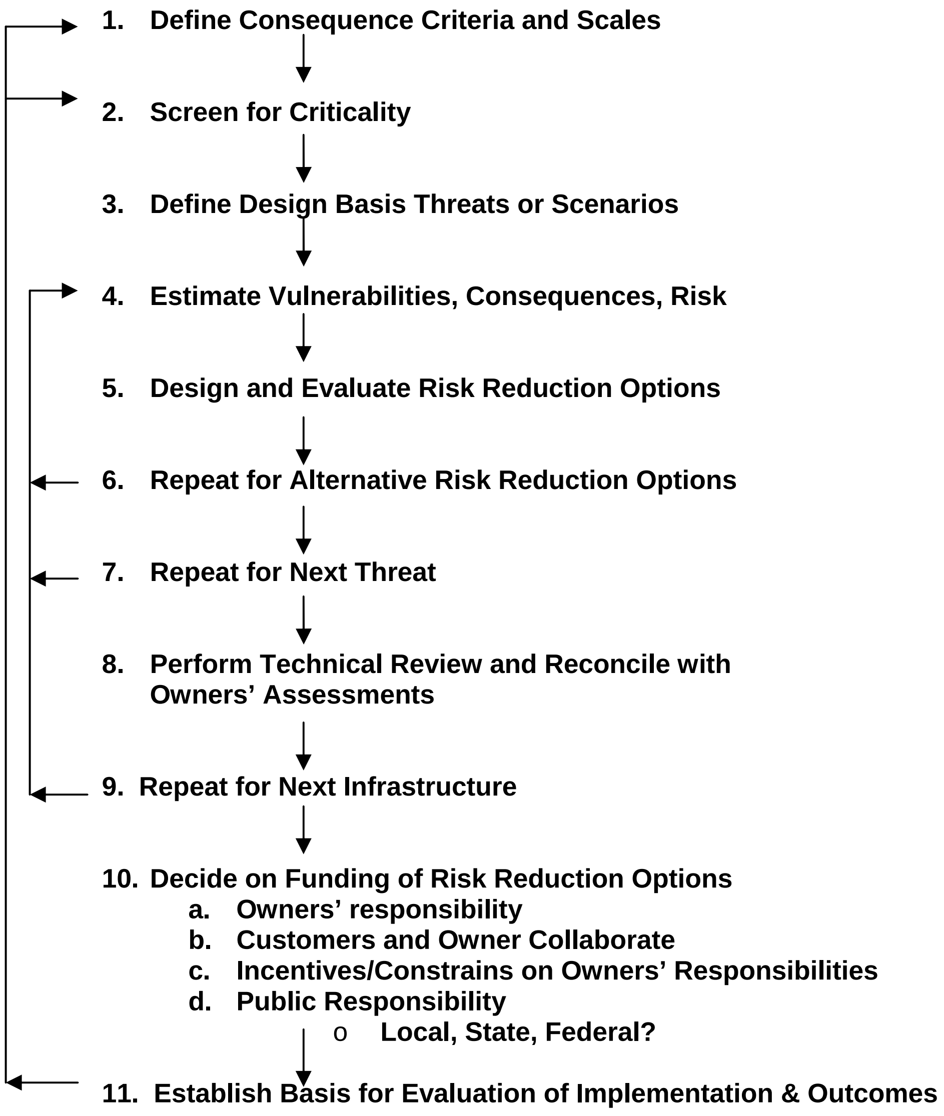
Recommendation: *The ONCRC should closely monitor the Seattle test of the CIP/DSS for its lessons. If the planning in Seattle results in early signs of utility, the ONCRC should evaluate the data requirements, functionality and applicability relative to negotiating and financing test in the NCR.*

2. Proof of Concept*.* The extensiveness of data requirements of the CIP/DSS and the plan to operate the model only as a service suggested a simpler and more direct approach, at least for the near term. A second approach was developed as a "proof of concept" that *available* tools and data could be applied to regional risk management. The rest of this section sketches the approach used; the actual tests are reported in Volume 9, *Regional Analytics for Risk Management and Resource Allocation,* and summarized below.

5.6 A Process for Regional Risk Management

The process described below (and illustrated in Figure 2) is designed to be used for analysis of individual assets, systems or whole infrastructures from a *regional* perspective. It is assumed that a parallel assessment from the owner/operator's perspective is performed using the owner's criteria.

Process: Steps in Regional Resource Allocation for Increased Resilience



1. Define Consequence Criteria and Scales
2. Screen for Criticality
3. Define Design Basis Threats or Scenarios
4. Estimate Vulnerabilities, Consequences, Risk
5. Design and Evaluate Risk Reduction Options
6. Repeat for Alternative Risk Reduction Options
7. Repeat for Next Threat
8. Perform Technical Review and Reconcile with Owners' Assessments
9. Repeat for Next Infrastructure
10. Decide on Funding of Risk Reduction Options
    a. Owners' responsibility
    b. Customers and Owner Collaborate
    c. Incentives/Constrains on Owners' Responsibilities
    d. Public Responsibility
        - Local, State, Federal?
11. Establish Basis for Evaluation of Implementation & Outcomes

1. Define Consequence Criteria and Scale. The comparability necessary for rational resource allocation requires common definitions in the major metrics of the consequence of loss. The USA Patriot Act of 2001, the 2002 National Strategy for Homeland Security, and the 2003 HSPD-7 all define critical infrastructures as "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on *security, national economic security, national public health and safety, or any combination of those matters*." (Italics added.) Subsequently, *public confidence and morale* were added. Other dimensions, e.g., environmental degradation, could also be added.

With this point of departure, a specific list of key metrics can be developed as definitions of the dimensions for measuring these concepts. For example, economic security could be defined as changes in the *gross regional product* for the region plus the cost of post-event restoration; public health and safety could be measured in lives lost and person-days lost due to injury and illness.

> *Output*: Concrete metrics of consequences for screening and later decisions

2. Screen for criticality. The next step is a screening to identify and roughly prioritize the Critical Infrastructure and Key Resources in a Region. This is done by quickly examining each major asset and grossly estimating the "worst case consequences" in the terms defined in step 1. These are compared to key cut-offs for each dimension, those with greater values are considered potentially critical, those not reaching these thresholds are excluded.

> *Output:* List of regional infrastructures, systems and assets prioritized for analysis.

3. Define a Design Basis Threat or Scenario. For direct comparability, it is necessary to establish a standard set of design basis threats or threat scenarios. The absolute likelihood of an attack by a particular means is beyond the resources of the region, but the relative likelihood can be defined by experts in at least an ordinal ranking. Some analysts use "attractiveness to an adversary" as a surrogate, but that has no equivalent for natural disaster.

> *Output:* Standard threat scenarios to use in risk assessments

4. Conduct the Risk Analysis. This step estimates vulnerabilities and consequences for the specific threat. Individual assets and confined systems can use ASME's sector-specific tools. The regional approach has the following steps: Geographical Information Systems (GIS) modeling of specific threat scenarios, an estimate of specific businesses impacted, preparation of data for the Input/Output economic model, and use of the I/O model to estimate economic losses for *each sector and major jurisdiction* in the region. Non-economic consequences could be estimated directly or by correlation with the economic impacts.

> *Output:* Estimates of risk to region of current status of each asset and system.

5. Design and Analyze Risk Reduction Initiative. Risk can be reduced by reducing any or all of its parts, threat, vulnerability and consequences. It is difficult to reduce the threat, but it is not infrequently possible to reduce the attractiveness of a target to an adversary. Most of risk reduction, however, consists of reducing vulnerabilities or consequences. The difference between the regional risk of the *status quo* and the regional risk under the initiative is the *risk reduction benefit.*

> *Output:* Estimated regional benefits (and their distribution by sector and jurisdiction) and costs of reducing the specific risk.

6. Repeat Steps 4 and 5 for any alternative risk reductions for the same risk. When there are multiple approaches to risk reduction for a specific threat and system, each (and their combinations if they are not incompatible) should be evaluated to determine which is most cost-effective.

> *Output:* Benefits for the most cost-effective initiative for each threat.

7. Repeat Steps 4, 5 and 6 for the next threat. This assures that all the design basis threats are addressed systematically. The aggregate risk to the infrastructure posed by the full suite of threats can be *approximated* by weighting the respective risks by the *relative likelihood* from Step 3. The combined benefits of the most cost-effective risk reductions can be aggregated in the same way, while the costs can be simply added.

> *Output:* Complete assessment of full program to protect the analyzed infrastructure relative to its benefits and costs from a regional perspective.

8. Perform a technical review of regional and owner's analyses. This step permits normalization of assumptions and reconciliation of methodological details in preparation for comparison in step 9. Some adjustments may be needed to make the assessment as comparable.

> *Output:* Approximately comparable assessments of the risk reduction options from both owner's and regional perspectives

9. Repeat Steps 4 through 8 for each infrastructure on the critical list. Usually, the respective analyses would be conducted simultaneously.

> *Output:* A full "menu" of candidate options for decisions by the owner/operators and the regional authorities.

10. Decide on funding the candidate options. The philosophy is to allow the marketplace to make as many of the decisions as possible. This requires four criteria.

1. Can the owners make the business case for any of the options?

2. Would the sectors that depend on the infrastructure in question be so damaged by its disruption that they find it in their own interest, individually or collectively, to cooperate in the funding or all or part of the options?

3. Can the owners be *induced* to invest in all or parts of the options, through, for example, security-related cost-recovery rules for price-controlled utilities, tax breaks, or national standards?

4. Are the benefits so widely dispersed among the general population that they can only be addressed by public agencies through subsidies, programs, procurements, etc.? The challenge here is deciding which options have greatest regional merit and which level of government and jurisdiction bears the responsibility.

> *Output:* An approximately *optimal regional risk reduction program* in which the principal and most immediate beneficiaries bear the costs of the program, while the region as a whole becomes more secure and resilient.

11. Establish a plan to monitor implementation and to evaluate the outcomes. Basic project management progress tracking should be established for each selected option and the results reported to the leadership of the public/private partnership. Another way to gauge increments in resilience is to periodically conduct a series of all-sector, public/private interdependencies exercises and note the changes over time.

> *Outcome:* A plan for orderly, monitored implementation and period re-assessment of the region's levels of risk and resilience.

Recommended Actions:

- The SPG should expand the number of critical infrastructure sectors evaluated from the eight in this report to the full federal list.
- The public/private partnership should consider continued development and full testing of analytic tools for simulating infrastructures and interdependencies in the NCR and evaluate for possible use the National Infrastructure Simulation and Analysis Center (NISAC) and Critical Infrastructure Protection Decision Support System (CIP/DSS).

- The public/private partnership should test, enhance, and employ the simpler, near-term relative risk and benefit evaluation model. This process should begin with a conference of experts in regional and infrastructure modeling and risk management and senior public officials to refine the requirements, exchange ideas and approaches and define an overall strategy. The method descried in Volume 9 could serve as appoint of departure.
- The public/private partnership should develop, along with infrastructure owners and DHS, carefully defined and implemented protocols and safeguards for information capture, storage, sharing and data security.

6 CITIZENS AND COMMUNITIES

6.1 Introduction

First and foremost, it is the citizens of the NCR for whom the resilience of essential services is sought. It is their lives and livelihoods that are to benefit. In many cases, it is the attitudes and understandings of the public that determine the success or failure of a policy or plan. This has recently been demonstrated in the levels of compliance with evacuation orders, but would also be critical to the success of a shelter-in-place order accompanying a biological or radiological attack. Further, the general levels of confidence in government agencies and infrastructure operators can profoundly affect the behavior of the populace under various circumstances. Many economic and policy analysis models attempt to predict the behavior of the public in response to alternative policies or programs.

The NCR-CIP commissioned a series of 6 studies of the attitudes and level of information of the public in the NCR and, in one case, the rest of the U.S. The studies also address specific infrastructure issues that are of concern to the public at large such as mass transit, provision of shelter, and biodefense. For detailed information on the methodologies, references, and data sources used for arriving at the findings and recommendations, refer to the individual volumes.

6.2 Critical Infrastructure Protection, Vulnerability and Public Confidence

Issue

Since the terrorist attacks of September 11th, 2001, the United States has made significant progress in devising national and local policies for mitigating and responding to future large-scale threats. However, as witnessed in recent natural disasters, that progress has been uneven, and the results have been accompanied by considerable doubt and controversy among different decision-makers as well as from community groups and average citizens. Public support for and understanding of the far-reaching policy changes in the field of homeland security are critical to the actual success – or failure – of such initiatives. Thus, it is important to understand citizen preferences and confidence in critical infrastructure protection, and make them part of the decision-making process.

Volume 14, "*Critical Infrastructure: Citizens' Views of Protection in the National Capital Region*" describes a policy analysis tool known as a citizens' panel to capture data and information beyond that which is available through surveys. While public opinion polls are useful in their own right, these instruments cannot capture citizens' true preferences and value orientations because most people lack the kind of detailed information required to make informed choices and tradeoffs. During the Citizens' Panel, a small group of representatively selected residents of the NCR interacted with experts, heard presentations, and discussed information concerning disaster response, terrorism and critical infrastructure protection in the National Capital Region. The group's deliberations and assessments were recorded to serve as input for policy research and decision-making.

Key Findings and Recommendations

1. Government should conduct better community outreach, particularly in the form of credible and useful information directed to citizens, to improve the public's confidence in homeland security.

2. Governments should communicate more clearly communication of issues about terrorism and homeland security, with the very complexities of policy requiring more direct and localized initiatives.

3. Government should to de-politicize security issues, because citizens currently perceive the substance and timing of security alerts as being politicized; such matters should be placed into the hands of more neutral actors. A recurring theme in the recommendations phase of deliberations was that government needed to do more outreach on localized levels.

6.3 CIP, Vulnerability and Public Confidence in the NCR and the US

Issue

Public confidence in government, emergency response and recovery agencies, and critical infrastructure service providers is vital to the maintenance of the social compact between citizens and the state, and to assuring order in the event of large-scale disruption due to extreme events, either terrorist attacks or major natural or technological disasters. Weakened or destroyed public confidence in the most critical public and private institutions would likely invite widespread social collapse, diminished investment, economic decline, and calls for political and institutional reform. Thus understanding and measuring public confidence in homeland security institutions and policies is vital to the successful achievement of homeland security policy objectives.

Specifically, Volume 15, "*Critical Infrastructure Protection, Vulnerability and Public Confidence*" measures the public's perceived vulnerability to extreme events, including terrorist attack, its preparedness to deal with interruptions of essential services, and its confidence in the organizations responsible for attack prevention and disaster preparedness, response and recovery, for both the National Capital Region and the United States.

Key Findings

1. The public has a deep sense of vulnerability to terrorist attack

Seventy-eight percent of both residents of the United States and the NCR believe another terrorist attack is likely in the United States, and 66 percent of respondents in the NCR think another attack is likely in Washington. Fifty percent of residents outside the NCR think the closest major city to them is likely to be attacked. Forty-one percent of respondents in the NCR worry that they or a family member will be a victim.

2. Public lacks confidence in most essential infrastructure services

About 40 percent or respondents nationally and regionally are not confident about the reliability of electric power and standard landline telephone services. Fewer were concerned about water, cell phones and television, and natural gas. Radio instilled the most confidence of all essential services. At the same time, from 33 percent to 62 percent of respondents in the United States said they could go for a week or more without one or more critical infrastructure services. NCR results were about 9 percentage points lower in each category than results from the country as a whole.

3. Public confidence is low in some, but not all, government and homeland security agencies

Just 31 percent of both the U.S. population and the NCR trust the government. But respondents vary in their confidence in specific local, state and federal agencies: local emergency medical units enjoy the confidence of more than 80 percent, while the Department of Homeland Security, Customs and the Transportation Security Administration have the lowest ratings, at about 30, 20 and 25 percent, respectively. The Federal Emergency Management Agency received positive responses from about 45 percent.

Key Recommendations

1. Improve public confidence in homeland security and essential service providers by effective, consistent public-oriented performance. The public seems to distinguish between rhetoric and action in homeland security affairs. Therefore, avoid politicizing homeland security.

2. Make essential services more robust by encouraging modest increases in spending by some infrastructure providers, such as water, electricity and healthcare. Citizens seem willing to entertain small, targeted increases to make these services more reliable during extreme events.

3. Improve federal and state to local partnerships for disaster communication and response. People feel most comfortable with local agencies and law enforcement officials. Consider eliminating the color-coded alert system.

6.4 Community Shielding and Public Preparedness in the NCR

Issue

When a terrorist attack or other disaster occurs, individual and community responses will be the most important determinants of survival.

Over the past decade, public preparedness has often been defined in terms of evacuation readiness. Certainly, when given prior warning for a major national disaster such as a major hurricane, an effective evacuation strategy is the key to a community's successful response. Effective evacuation, however, requires extraordinary planning and collaboration between local, state and federal agencies, as well as an ability to access geographically and socially diverse community resources.

Although successful evacuation acknowledges the need for adequate physical and social infrastructure, as a society we expend few resources in preparing to address the other side of the public preparedness coin; shelter-in-place. Perhaps it is because the concept is by its nature individual and dependent on the resources within our living spaces. Preparedness attitudes within communities provide a window of understanding that is necessary for effective response policy development and implementation.

Volume 16, "*Community Shielding in the National Capital Region. A Survey of Citizen Response to Potential Critical Incidents.*" assesses emergency preparedness, public knowledge of biological and radiological emergency preparedness, finding safety in an emergency, obstacles to shelter-in-place, sources of trusted information in an emergency and attitudes toward anti-terrorism policies.

Key Findings

1. Similar to existing networked evacuation resource planning, we need a Community Shielding planning strategy in order to plan for coordination of shelter-in-place. Shelter-in-place is an important concept that has limited utility in a major disaster, as currently defined. Attempts to educate the public towards needed preparation have been only partially successful. Our survey revealed that a sizeable portion of the National Capital Region population is currently unwilling or

unable to shelter-in-place, and about half of the respondents in the survey did not feel that they would be able to shelter at home for more than a week. Respondents in Washington D.C. expressed the strongest preference for remaining in their communities, even though they were the least likely to have prepared to shelter-in-place.

2. Confidence in government's ability to respond to disaster reflects significant regional differences. Compared to respondents living in Washington D.C., respondents in Virginia and Maryland were more than twice as confident in their attitudes toward local government and its ability to respond to disaster. As a result, an overwhelming majority of respondents in both states noted that they would strictly follow local government instructions in the event of an emergency. This contrasted with respondents in Washington D.C., who were less likely to follow instructions from their local government.

3. Shopping Centers are desirable locations for distribution of community-specific homeland security information. Respondents identified shopping centers as locations where they would be comfortable receiving specific homeland security information about their individual communities. These privately-owned spaces are potential central public homeland security information sites, and could anchor the local community in disaster preparedness and response planning. Respondents expressed a preference for electronic information exchange augmented by a volunteer who could provide necessary informational support to the process.

Key Recommendations

1. Develop a strategy of Community Shielding that utilizes social and governmental networks to enhance a community's ability to shelter-in-place.

2. Assess and address current social disaster preparedness needs within Washington D.C. so that trust in local government can be strengthened. This should lead to greater compliance with government directives during a course of a disaster.

3. Develop a public-private initiative with the NCR shopping centers to create a system of information delivery and exchange related to local and regional homeland security needs.

6.5 Citizens in Biodefense and Early Warning

Issue

The anthrax attacks affecting the National Capital Region in 2001 highlighted our vulnerability in this new asymmetric warfare, and triggered a reexamination of our readiness to respond and search for means to better protect citizens against future attacks. Most of the available disaster response training protocols involves the "traditional first responders" such as emergency medical services and fire and rescue. An increasing effort to involve communities through the Citizen Corps and the affiliated Community Emergency Response Teams (CERTs) and the Medical Reserve Corps (MRC) has been underway since September 11 2001. Despite the importance of the community and school civil defense preparedness, allocated resources remain inadequate. For example, a 2004 study by the Trust for America's Health finds that over two-thirds of states and D.C. achieved a score of six or less out of the 10 possible preparedness indicators.

Based on these issues, Volume 17, "*Critical Role of Citizens in Biodefense and Early Warning*" suggests that experience gained from training in civil defense, first aid, cardiopulmonary resuscitation (CPR) and automatic external defibrillators (AED) can serve as a potential guide and model for such education and training of citizens as immediate first responders. It is also proposed that every disaster mitigation training strategy should target and involve each and every community member as a resource for emergency preparedness and response.

Key Findings

1. Health and science literacy are prerequisites for understanding bioterrorism

In order to understand the bioterrorism effects on health, and to act accordingly, adequate health and science literacy are a prerequisite. Based on the literature reviews and our pilot survey, community organizations such as Citizen Corps (MRC and CERTS), should be a resource for raising health literacy and disaster and bioterrorism preparedness.

2. A model for potential impacts can assist in preparedness

Neighborhoods are the building blocks and serve as the basic web of relationships in the community. Conscious efforts to build and strengthen these basic blocks, or modules, are an essential step in achieving preparedness. The GMU research team has adopted a model for potential impacts resulting from natural and human-made disasters. The impacts were subdivided into business, health, policy and societal categories. Well structured educational and training materials should recognize and address every sequential event presented in the model.

3. Survey on knowledge, attitudes and practices to determine citizen preparedness

The survey developed and presented in this research on knowledge, attitudes and practices (KAP) should be widely distributed and the information obtained can be used to guide the development of the training curriculum.

Key Recommendations

1. Health and science literacy of citizens should be emphasized and addressed

2. The model for potential impacts as described in the Report should be implemented to characterize the socioeconomic consequences of potential bioterrorists attack in the NCR area and develop proper mitigations strategies

3. The knowledge, attitudes and practices survey has identified significant issues with the NCR area community preparedness status and willingness to participate in the learning of new coping skills. This was a pilot study and the survey needs to be administered to a broader segment of the NCR community especially to minority groups.

4. Additional resources should be made available to the Citizen Corps to ensure better community preparedness

5. Resiliency and recovery process for small businesses, the backbone of the national economy, following a biological attack should be addressed and the information and training made available to employers, employees and their families

6.6 Transportation Systems and Bioterrorism

Issue

Widely available, rapid, and easily accessible transit for passengers and goods is a key ingredient for economic development and global prosperity. These same attributes, notably ease and accessibility, can facilitate the spread of infectious diseases and make it an attractive target for a terrorist attack. The problem of decontamination of a large scale area following even a small spill might also present a significant regional, societal, psychological, and economic impact. Based on the experience from the 2001 anthrax spores delivered by mail, it is reasonable to assume that the number of "well and worried" visitors to emergency and health care facilities might overwhelm the health care system even when the actual threat is rather small. The delivery of anthrax spores into the NCR subway system likewise is liable to preclude the use of the system for months, if not years.

In Volume 18, "*Epidemiology of Transportation Systems and Bioterrorism*", the research team modeled the dispersion of a significant amount of anthrax spores on a large geographic scale. Such a scenario calls for major production and stockpiling of the spores, requiring advanced technical capability, and as such is considered difficult to accomplish. Nonetheless, as the model revealed, the significant disparity in the distribution of medical and public health facilities and limited surge capacity within the NCR area needs to be addressed.

Key Findings

1. Transit systems in NCR are attractive targets for terrorists

Historical assessments indicate the NCR rapid transit system can be an attractive target, already identified as such by the intelligence and law enforcement officials, as vulnerable to bioterrorism.

2. The Internet is a source of information for terrorists planning attacks on transit systems

Certain information available on the internet pertaining to detailed transit plans, building plans, etc. may aid terrorists in planning an attack and as such should be carefully screened for information and made available as demanded for legitimate and/or limited use. Due to freedom of expression and information, this is an area that needs further consideration and policy refinement.

3. An anthrax attack on the METRO system proves highly detrimental to NCR area

Under the current scenario, an attack using anthrax spores will put the subway passengers at risk of exposure and re-exposures until the event is discovered. The population under the plume will be at risk of exposure as well. This might result in a significant number of cases requiring hospitalization and a major public health burden for tracking individuals requiring diagnostic procedures and /or prophylactic treatment with antibiotics. In addition, the decontamination process for the area and the subway system will be required.

Key Recommendations

1. Due to the impact of the release of a large amount of anthrax spores (bacillus anthraces) on the availability of hospital beds, proper provisions must be made to secure additional medical resources for the NCR.

2. A regional public health authority should be identified to develop, coordinate, and implement prevention and mitigation strategies to be used in case of emergency for the NCR region.

3. The Federal Government, in consultation with leading experts in the field, should establish and adopt safety, isolation, and decontamination standards for weaponizable biological agents to prevent unnecessary confusion within the community and loss of public confidence.

4. Develop means for isolating contaminated segments of the underground METRO system, including interrupting air ventilation. A capability for safe and rapid passenger evacuation into aboveground and uncontaminated areas (safe or cold zones) is required.

6.7 Blood Supply Infrastructure

Issue

Contamination and disruption of the blood supply can have dire consequences for medical safety, patient confidence, and the regional and national healthcare industry. Because of the nationwide allocation system, there is a risk of a terrorist infecting the donations and thus threatening numerous patients' lives.

The purpose of Volume 19, "Protecting the Nation's Blood Supply" was to conduct an in-depth evaluation of the vulnerabilities of the existing collection and distribution processes and procedures for the collection, processing, and distribution of blood products. In addition to a bio-terrorism event, other issues were addressed such as the potential for using blood products to detect sentinel events from bio-terrorism attacks and barriers to the implementation of a biomedical monitoring system of blood donors and products.

Key Findings

1. Effective safety and control measures are currently in place to protect the blood supply, distribution, and infrastructure. However, these measures might not be immune to a terrorist event.

2. Periodic shortages of blood supply often dictate remedial collection practices which could result in potential safety and control gaps during exceptional periods, leading at best to the destruction of valuable and life saving products, or at worst to potential contamination of the blood products.

3. The most significant threat of concern is the ability to terrorize the public without actually compromising the collection and distribution chain of blood products.

4. There are potential deficiencies in modeling capabilities that are intended to support policy and decision-making, as well as the management and implementation of actions intended to reduce and mitigate the impact of terrorist-generated blood-borne infections.

Key Recommendations

1. Design and execute policies for implementing a "sentinel monitoring" system, especially in the context of evolving global health interdependencies.

2. Establish a federally-funded and maintained registry for blood and blood products, including an epidemiological database of donors and the carrier state of blood-borne pathogens suspected as etiological agents for chronic diseases. To this end, proper legislation should be enacted to ensure the deployment of such a system.

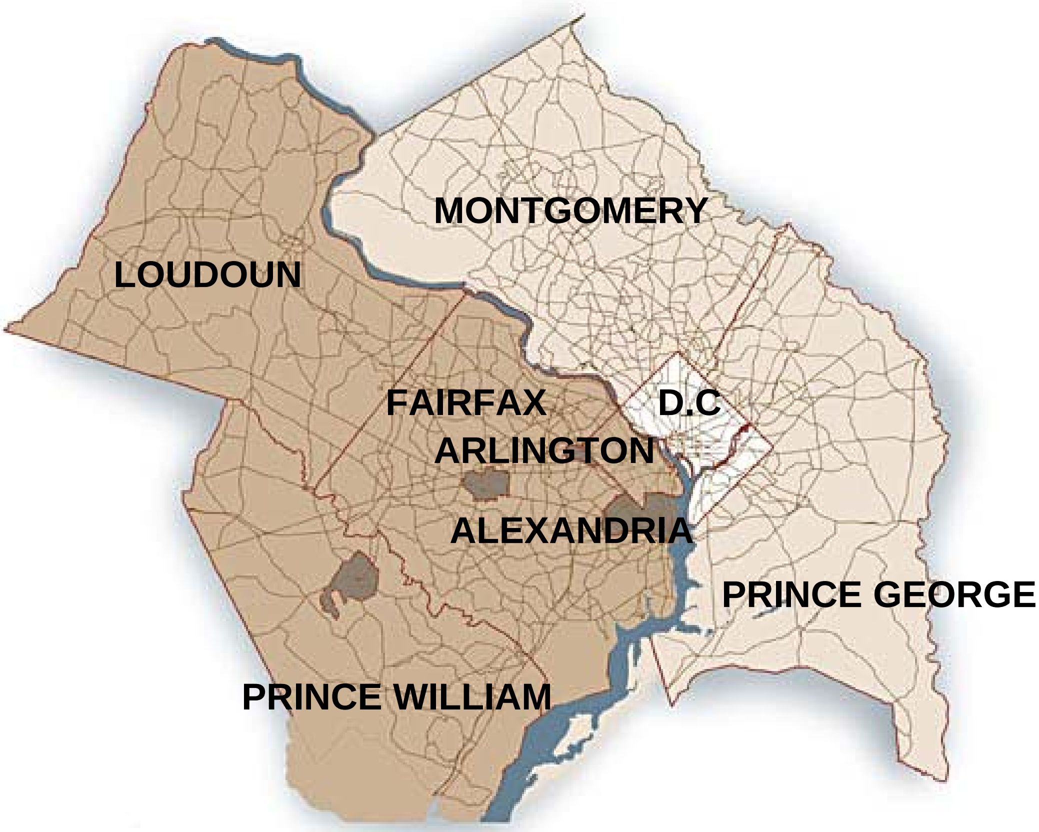
3. Funding of focused research to accelerate the development of blood and blood product substitutes.

APPENDIX A . INTRODUCTION TO THE NATIONAL CAPITAL REGION

A.1 Definition

The National Capital Region (NCR) consists of, "the geographic area located within the boundaries of (A) the District of Columbia, (B) Montgomery and Prince Georges Counties in the State of Maryland, (C) Arlington, Fairfax, Loudoun, and Prince William Counties and the City of Alexandria in the Commonwealth of Virginia, and (D) all cities and other units of government within the geographic areas of such District, Counties, and City."[1] The map in Figure A-1 displays the NCR.

Figure A-1. Geographic Boundaries of the National Capital Region



A.2 Political significance

The NCR is the very symbol of the United States in the eyes of world. It is the seat of the national government, headquarters of national defense and home to numerous international institutions. On the positive side, representing American history and values, the region is a major tourist attraction, conference and convention center that attract 18 million visitors each year. On the negative side, standing for U.S. political power and global influence, the region is also a destination and potential target for anyone dissatisfied with domestic or international policies. Along with hundreds of such planned and legitimate democratic expressions such as demonstrations and rallies every year, there are also incidents such as the "tractor man" standoff in 2003 that cause traffic and business to be disrupted. And since the Oklahoma City bombing in 1995 and the attacks of September 11, 2001, it is evident that the region with its highly recognizable public and private facilities is extremely target-rich for terrorists.

The National Capital Region is an extraordinarily complex socio-economic and political agglomeration. It consists of 12 overlapping jurisdictions (two states and the District of Columbia); all three branches of the federal government; a large private sector; thousands of associations; the densest concentration of nonprofits in the country; and almost 5 million residents. While not the largest metropolitan area in the country by most statistical measures, it is arguably the most important place for public and private sector decision-making in the country.

A.3 Economic Significance

Over time, the structural and functional composition of the NCR has undergone major changes, but is unlikely to lose any of the economic, political, and symbolic functions. The region is one of the fastest-growing in the country. Between 1998 and 2003, the gross regional product (GRP, sum of all business transactions) grew by 23% (compared to 15% nationwide). Its population is projected to grow to 6.7 million residents by 2030. The functional boundaries of the region are expanding to counties beyond the current core, increasing the strain on existing infrastructures and the need for building new capacities.

While not as dominant as often perceived outside the region, the federal government's impact is still significant. Economically, the presence of the federal government determines both the employment structures and the production of goods and services in the region. Of the regional workforce of nearly 3 million, 11% work directly for the federal government. More importantly, government spending and procurement in the region is the single most important contributing factor for the higher growth rates of the gross regional product (GRP), currently nearly US$300 billion annually. Unemployment in the region is consistently lower than the national average. With increased spending on homeland security and defense, those traditionally strong sectors can be expected to expand even more, attracting more businesses and people to the region.

Almost equally as important as the federal government is the nonprofit sector.[2] It is the largest in any region in the country, consisting of over 7,600 organizations with approximately 218,000 employees or 11 percent of the total private employment. They generate $33 billion in revenues, and spend close to $30 billion.

The NCR's primary industry after the federal government and private and non-profit associations is tourism. Symbolizing American history and political power, the region is a major tourist attraction, conference and convention center that attracts 18 million visitors each year. Other important sectors are trade associations, legal and consulting services, higher education, medicine/medical research, government-related research, publishing, finance, and telecommunications.

The last major change to the regional economy before the current period was triggered by new technologies. Starting in the mid-1990s, the emerging information technology and biotechnology sectors have led to the establishment of new clusters on the sub-regional level. While some were originally centered around large government facilities and contractors like the National Institutes of Health (in the case of biotechnology) and Lockheed Martin (in the case of information technology), others, like AOL, have developed independently. What they have in common is the reliance on a much higher than average educational attainment (nearly 45% have a college degree), and an elaborate mass transportation infrastructure with three major airports and a heavy rail transit system that is used by more than 40% of commuters in the central city and the inner suburbs.

A.4 Military Significance

As the NCR is the real and symbolic center of the American political process, so it is the real and symbolic center for the military power of the country.   While there are commands and highly secure military centers across the country and world, all roads lead back to the Pentagon. While military operations are executed by the Unified Commands headquartered outside the NCR, the taskings are authorized by the National Command Authority (the President and the Secretary of Defense). And although the Pentagon is the most visible and notable DoD facility, hundreds of buildings in the NCR are Department of Defense (DoD)-owned or DoD-leased.

Within those buildings are housed components or commands of the military services, elements of the Joint Staff, or functions of DoD itself. They are staffed by a mix of DoD employees, uniformed service members, and on-site contractors. Alongside these defense offices are a myriad of contractors ranging from small companies with a handful of employees (or less) to entire floors and buildings operated for major defense and multi-national corporations.

With DoD's level of outsourcing and contracting, in many cases it is impossible to tell what elements or components of a defense project or operation are completed by government employees, which are produced by contractors, and which are blended products. All of this speaks to the requirement for complex computing, data storage, and communications systems.

With a large number of DoD-leased spaces (according to recent stories in the Washington Post -- approximately 8 million square feet of leased office space, in 140 buildings, in Northern Virginia alone) and the spaces used by the contractor community, it is clear that much of the work that DoD needs to get done requires the same shared networks of infrastructure support -- used simultaneously by the government, contractors, and everyday businesses and citizens.

A.5 State of Security in the NCR

The National Capital Region has always been particularly sensitive to large-scale incidents involving its infrastructures. While not necessarily a target themselves, critical infrastructures such as transportation arteries, postal centers, and emergency services are always affected by disasters, and often a vector of disruptions due to the geographical proximity of facilities, and the economic and political immediacy of their functions. The following examples highlight the vulnerability of infrastructures to man-made and natural disasters.

A.5.1 Pre 9/11

Before the attack of September 11, 2001, on the Pentagon, the single-largest disruption of infrastructures requiring emergency response and recovery efforts in Washington, DC took place due to three concurrent events on January 13, 1982.[3] Starting around 3:00 pm, a major snowstorm led to the early release of federal employees, which caused unusual traffic volumes and stranded commuters. At 4:01 pm, a Boeing 737 taking off from National Airport with iced wings crashed into the George Mason (14th Street) Bridge and sank into the frozen Potomac River, killing 78 passengers and motorists. At 4:30 pm, an Orange line Metro train derailed south of the Federal Triangle station in downtown DC, and hit a concrete pillar that separated the inbound and outbound tunnels; resulting in 3 fatalities and 25 injuries.

Between the effects of the storm, and the separate rescue efforts around I-395, the George Washington Parkway, and the Metro system, the area lost the use of its major downtown bridge and interstate, its busiest metro line, and its domestic airport within less than two hours. Yet it took days to reopen airport and Metro, and weeks to repair the bridge connectors.

A.5.2 9/11

The September 11th attack on the National Capital Region was devastating. The Department of Defense reported a total of 125 service members, employees and contract workers died in the 9/11 attack on the Pentagon building. An additional 64 people died aboard the hijacked American Airlines Flight 77, which crashed into the west side of the building. While this represented a significant loss of life, the perpetrators of this event had sought to cause further destruction in the NCR with United Airlines Flight 93. This flight from Newark, New Jersey, to San Francisco, California, crashed in rural southwest Pennsylvania, with 45 people on board after a struggle apparently ensued onboard the plane. These events underscore the attractiveness of the NCR as a target as it is home to symbolic institutions, such as the Pentagon and the Capitol building. The events also highlight the capability of a determined actor seeking to harm the residents of the NCR and the vulnerability to such determination.[4]

A.5.3 Post 9/11

After the attack of 9/11, several events have impacted infrastructure operations in the NCR, the largest and most expensive in response and restoration cost occurred with Hurricane Isabel in 2003. The morning of September 18, 2003, seemed as pleasant as any fall day could be. Nonetheless, schools and businesses were closed, metro ceased its operations, and residents were stockpiling canned food, water, and batteries. In less than six hours, the calm would change to chaos as Hurricane Isabel swept through the area. Winds brought down trees in record numbers, causing damage to hundreds of power lines and streets, and storm surges flooded downtown Alexandria and other neighborhoods. A total of 1.3 million households and businesses were without electricity, and tens of thousands of residents were without water due to power outages at water treatment plants. This unusual level of severity provided a unique test bed for evaluating a large-scale emergency response and impacts to critical infrastructures under real conditions. Overall, collaboration functioned well across jurisdictional boundaries, most critical infrastructure functions were successfully restored in less than seven days (as compared to two weeks after Hurricane Floyd in 1999). But while the NCR's first responders and infrastructure providers generally performed well under difficult circumstances in the first 48 hours of the event, certain pockets still experienced delayed restoration of as long as eight days despite the weeklong advance warning and potential planning time.[5]

In the months following the 9/11 attacks, the NCR became aware of the very real threat of bioterrorism. Anthrax was sent to elected officials and news media through the mail, causing concern, confusion, and death. House and Senate offices were contaminated and employees infected, resulting in shutting down Congress. Postal facilities across the region were also contaminated and anthrax was discovered at off-site mail screening centers for federal buildings in the NCR. The incident ultimately killed five people and sickened 17.

Another anthrax scare in the region happened on March 10, 2005. Samples taken from sensors at the remote delivery facility of the Pentagon tested positive for anthrax. Pentagon official were notified on March 14th. That afternoon, an airborne biohazard alarm at an office building in Fairfax County that receives mail from the Pentagon went off prompting the quarantine of 800 employees for hours.

Due to the severity of the threat and susceptibility to quickly spread, since 2001, the Postal Service has been spending $1.4 billion to install a biohazard detection system at 283 mail facilities; the federal government has spent $370 million to boost state and local public health labs, the backbone of the CDC's 140 bioterrorism Laboratory Response Network; and Homeland Security has launched a $60 million-plus BioWatch system to monitor air in more than 30 U.S. cities.[1] These examples underscore the vulnerability of the NCR to natural and man-made disasters that disrupt the provision of vital services to its citizens and institutions, with national and potentially global repercussions.

APPENDIX B. THE NATIONAL CAPITAL REGION CRITICAL INFRASTRUCTURE PROJECT

B.1 Mandates for Study

In 2002, the National Capital Region's Eight Commitments to Action identified critical infrastructure protection as a high priority of homeland security strategy: "Infrastructure protection – work in partnership with the private sector to jointly identify and set protection priorities and guidelines for infrastructure assets and services in the NCR." It also provided guidance on the approach: "citizen involvement, collaborative decision-making, exercises that are inclusive of all levels of government…and other private and non-profit partners as appropriate." The following year, the NCR Urban Area Homeland Security Strategy set as strategic objectives to "reduce the NCR's vulnerability to terrorism" and "minimize the damage and recover from attacks that do occur" – both CIP objectives.

With this focus, the Senior Policy Group (SPG) of the NCR directed an initiative funded by the Urban Area Security Initiative (UASI) Grant Program and Department of Justice Community Oriented Policing (COPS) to support regional critical infrastructure protection (CIP). The initiative, the National Capital Region-Critical Infrastructure Project (NCR-CIP) was undertaken by the Critical Infrastructure Protection Program of the George Mason University School of Law and a consortium of regional universities.

B.2 Scope: Sectors Included

The list of infrastructure systems that are deemed critical has expanded over time, from eight original ones identified in PDD 63 to seventeen in the current Interim National Infrastructure Protection Plan (INIPP):

Table B-1. Evolution of Critical Infrastructure Designation

	PDD 63 (1998)	**NCR-CIP (2003-2005)**	**INIPP (2005)**
1	Information and Communications	Telecommunications	Telecommunications
2	Banking and Finance	Banking and Finance	Banking and Finance
3	Water supply	Water and Wastewater Systems	Drinking Water and Wastewater Treatment Systems
4	Aviation, Highway, Mass transit, Pipelines, Rail, and Waterborne commerce	Transportation	Transportation Systems
5		Postal and Shipping	Postal and Shipping
6	Public Health Services	Health Services	Public Health/Healthcare

7	Emergency Fire Services and Continuity of Government	Emergency Services	Emergency Services
	Emergency Law Enforcement		
8	Electric Power and Oil and Gas production and storage	Energy	Energy
9			Information Technology
10			Agriculture and Food
11			Chemical
12			Defense Industrial Base
13			National Monuments and Icons
14			Dams
15			Government Facilities
16			Commercial Facilities
17			Nuclear Reactors, Materials, and Waste

Besides the numerical increase, there is also a different understanding now of what constitutes an infrastructure, and why it is critical. The relation of asset and system level, and organizational and institutional structures vary in each sector. This explains differences between sectors as described in the individual chapters.

B.3 NCR-CIP Goals, Objectives, Approach and Status in Brief

The region's ultimate CIP goal is a more robust, resilient, secure region. The overall goal of the NCR-CIP is, broadly, to help determine how to become such a region. More specifically, the goals of NCR-CIP are *to define the requirements for more resilient, robust critical infrastructures in the NCR and to develop the framework for a strategy for meeting those requirements at the asset, system and regional levels*. These goals are being accomplished by meeting four objectives, described below with a brief status report:

1. Build a University Consortium. George Mason University (GMU) identified distinguished researchers in six NCR area universities and organized them into the University Consortium for Infrastructure Security (UCIP), which is made up of:

- George Mason University
- The University of Maryland
- The University of Virginia
- Howard University
- Virginia Polytechnic Institute and State University
- James Madison University

GMU provides prime contracting, planning and management of UCIP. UCIP represents a substantial proportion of the infrastructure and security academic expertise in the NCR and remains open for new membership to meet evolving requirements of the NCR.

2. Construct a basic CIP tool kit. This objective is to make the available open source tools for infrastructure vulnerability and risk management readily accessible and useable to infrastructure owner/operators wanting to enhance the reliability, robustness and security of their assets and systems. It has been achieved by evaluating the open source tools for comprehensiveness and applicability, by making them word-searchable and a selection of the more important ones concept-searchable. **See NCR-CIP Volume 11.** The CIP tool kit assembles and makes available practical procedures used for critical infrastructure vulnerability assessment and risk management (CIVA/RM). It includes:

- Assessment of open source CIVA/RM tools
- Online library of tools & methods for CIVA/RM
- Searchable database of CIVA/RM guidance and questions

3. Evaluate the state of risk management in each of eight NCR infrastructure sectors and recommend enhancements. This objective was achieved by establishing teams of researchers who are experts in each sector and having them review the relevant literature in depth and conduct fieldwork with the sectors' owner/operators, regulators, and experts. A uniform set of issues were discussed to gauge the state of risk management, to assess the understanding of interdependencies, and to glean specific suggestions for improved security decision-making and implementing risk reduction initiatives in the sector. The sector-specific products provide a first baseline and actionable recommendations for advancing CIP in the eight sectors in the region. They include:

- Sector characteristics and interdependencies
- State of risk management assessments
- Recommendations for risk reduction programs and processes

This work is summarized in this report and and presented in greater detail in the respective sector reports.

4. Define a framework for developing a regional infrastructure protection plan. This objective has been achieved by monitoring the policy and programmatic developments at national, state and local levels, comparing the recommendations of the respective NCR sectors, and defining the requirements for effectively enhancing the reliability and security of the essential services provided by critical infrastructures. National policy has clearly adopted a risk management approach to CIP at sector and national levels, with implications of extending it to regional concerns as well. The notion of regional *resilience* as an approach to securing critical infrastructures is emerging as a broader, more inclusive and possibly more effective than more traditional infrastructure *protection.* In the NCR, this entails the formation of a public/private/non-profit partnership within and across sectors and jurisdictions to assess risks, evaluate alternative risk reduction initiatives, select the most promising and commit financial and human resources to their implementation and evaluation of effectiveness. The framework recommends a plan for organizing this partnership and providing it with the elements required for its success. These elements include:

- Executing awareness-building exercises in some sectors and across sectors
- Organizing cooperative councils within and across sectors and jurisdictions

- Adapting and/or developing analytic tools and processes to inform decision-makers' assessments of risks and evaluation of risk reduction initiatives
- Adapting and/or developing analytic tools to select among risk reduction alternatives and to make resource allocation and funding commitments by private or public sectors
- Providing metrics and baseline measurements to evaluate the NCR's progress toward more reliable, robust, secure essential services provided by critical infrastructures.

5. Also conducted were a series of supportive studies that enhance the regional framework. These include:

- A shelter-in-place survey was conducted out to identify typical communities in the NCR and their confidence level in CIP and emergency response measures. The findings suggest that shelter-in-place scenarios require different allocation of infrastructure services than evacuation plans. The result is a concept for community-based shelter-in-place programs.
- A novel citizen panel methodology was used to assess citizen confidence in CIP and governments' ability to provide essential services in times of disruption. Its results emphasize that CIP on the regional level requires cooperation between residents and government; understanding what citizens' attitudes and expectations are is important to better communicate measures, to achieve compliance, to earn and develop trust, and to use contributions and resources effectively.
- The panel results were extended and validated by a telephone survey of more than 2000 citizens that will permit comparison of confidence attitudes between NCR citizens and citizens of the U.S. as a whole. The outcome is shows the residents of the NCR are more wary of terrorist attacks and natural disasters and less confident in public agencies and essential service providers than their counterparts in the rest of the U.S. as a whole. This survey could serve as a baseline for future assessments of public confidence in government agencies and infrastructure providers.
- A stakeholder analysis of regional public, private, and civic actors was performed to assure all key stakeholders are represented in the regional CIP framework. The analysis identifies significant public, private, and civil-society actors in the region, identifies cross-jurisdictional challenges, and outlines a multi-stakeholder forum that clarifies and adapts pre- and post-event roles and responsibilities. The outcome is a detailed recommendation a facilitated conference or tabletop exercise focusing on infrastructure interdependencies and the private sector. Such exercises have been conducted in the Pacific Northwest, New Orleans, Iowa and elsewhere, resulting in the formation or focusing of cross-sector, cross jurisdictional public/private partnerships for greater regional resilience.

.

APPENDIX C. Characterization of Types of Critical Infrastructure Vulnerability Assessment and Risk Management Tools

			____________Aggregation Level________		
Sophistication Level	***Pros***	***Cons***	***Asset/Function Examples***	***System/Sector***	***Multi-Sector Region***
General Policy Guidance	Broadly stated requirements with maximum of flexibility in implementation	Lacks standards of compliance; difficult to audit	Sarbanes-Oxley	Sarbanes-Oxley	None available; not recommended
Detailed Guidance and Procedures	Consensus-based, qualitative or %-compliance; on/off priority lists; requires little or no professional training or expertise	No estimates of relative or absolute value, only gross rank comparisons and only with like assets and methods	ANSI	NCR-CIP Minimum: Assure sector guidance as extension of asset governance	NCR-CIP: Guidance to SPG: promote as minimum, standard-based
Relative Risk Management	Standard analytics; can compare results with others, possibly in different sectors using same method	Limited cross-comparisons; only relative values – no absolute values (cannot compare benefits to costs); requires moderate level of professional training/expertise	FEMA 426 Series; Sandia's RAM-W; RAM-D; Department of Veteran Affairs Guide; Current ODP Special Needs Tool Kit; ASME RAM-CAP	NCR-CIP: recommendations for sector tools, incentives, guidance – as generalized to systems	NCR-CIP objective: First approximation resource allocation tool; rough prototype expected from NCR-CIP Phase I
Full Risk Management	Standard analytics can be directly compared across assets and sectors; estimates absolute values of benefits	Requires high level of professional training/expertise	Nuclear/NASA risk engineering	NCR-CIP: specs for extension of ASME to systems; DHS-National Labs' CIPP/DSS	DHS-National Labs' CIPP/DSS NCR-CIP objective.: specs as phase II RIPP Long Term Target

Appendix D. State of Risk Management by Sector

Sector	Awareness of value of CIP	Availability of Tools	Allocation of Resources	Risk Reduction Implementation	Risk Reduction Evaluation
Banking and Finance	▪ Confident in the resiliency of critical operations and communications. ▪ The Fed, OCC, and SEC made extensive contributions to identify and recommend approaches and tools to mitigating vulnerabilities. ▪ The federal regulatory agencies are mandated to keep the system informed about CIP issues. ▪ Business continuity is critical to system functioning.	▪ Significant number of tools, questionnaires, and audit materials available through the Federal Financial Institutions Examination Council (FFIEC), Information Technology Handbooks and public/private sector frameworks. ▪ Many security- and vulnerability assessment-related questions and protocols exist for the banking and finance sector.	▪ Resource allocation is dependent on the type of business risk. Management needs to ensure sufficient resources employed to prevent harm to financial system. ▪ Regulatory agencies must probe and evaluate frequently. Monitoring can help avoid noncompliance issues.	▪ Building robust back-up systems outside of region is costly but necessary for continuity. ▪ Following FFIEC guidelines will ensure system continuity during a crisis. ▪ Regulatory agencies, as a goal, conduct inspections at least every 18 months, however, they must inspect more frequently to ensure compliance and resiliency.	▪ Regulators evaluate individual companies and enforce the compliance. ▪ There seems to be sufficient evaluation of critical infrastructure protection effectiveness.
Emergency Services (ESS)	▪ Relatively little attention has been paid to the vulnerability of emergency services organizations themselves to loss of service due to critical infrastructure system failure.	▪ Specific vulnerability assessment tools for emergency services organizations have not been developed. Available evaluation methodologies focus primarily on organizational and administrative issues, as is the case with NIMS, EMAP, and	▪ Resources are allocated to deal with the "normal" risk of service interruptions under the principle of short-term self-sufficiency, and for interoperability projects such as CapWIN. WMD threats require a reassessment of	▪ Risk reduction measures protect against the interruption of emergency services. ▪ Reduction of vulnerability of ESS assets and personnel and reduction of dependency upon other critical systems compromised by	▪ Encourage collaboration between ESS and critical infrastructures sectors to identify and mitigate interdependencies. ▪ Identify critical ESS assets in the NCR. ▪ Establish permanent regional EOC for NCR.

		TCL.	requirements for extended self-sufficiency for ESS operations.	terrorist attack.	
Energy	▪ Energy infrastructure executives are aware of vulnerabilities of their systems to both natural and human-caused events. ▪ They are aware of an increased need to reduce vulnerability and increase resiliency of their systems – hardware, cyber, and people, and have scheduled annual vulnerability assessments. ▪ Many executives have participated in industry-wide efforts to develop security procedures and tools.	▪ The methodologies used range from internally developed, building sometimes on the federally funded/developed efforts to those developed by private firms and consultants. ▪ Most regional electric and gas utilities are involved in conducting vulnerability/risk assessments of their systems. ▪ Most tools available are too complex for small organizations and they developed their own tools. ▪ Most publicly available tools are very weak in the area of interdependency.	▪ Both the industry associations and organizations indicate that results of specific VAs did result in changes in capital construction, operating budgets and modification of insurance programs. Expenditures ranged from less than $1 million to many $10s of millions. ▪ Smaller organizations are not able to fund significant mitigation efforts. ▪ Most investor-owned utilities have not sought reimbursement for security expenditures.	▪ Identification of the top critical facilities in their system almost always led to installation of new/increased security systems: physical, electronic, surveillance, personnel and training. ▪ Install new security systems, upgrade design parameters for facilities, coordinate communications, and increase exercise of emergency plans. ▪ A number of organizations conduct cyber exercises to test security of computer, communications and SCADA systems.	▪ After various mitigation measures had been implemented, most organizations had not gone back to redo their portions of the assessment so they did not know how the mitigation measures had changed their security or vulnerability level. ▪ Every organization expressed concern about revealing security related information and assessment results to any federal government collection and evaluation program.
Health	▪ Hospital professionals indicate an awareness of the basic concepts of CIP and the practice of VA and RM, though more so with CIP than VA. At times, VA appeared to	▪ Existing tools do not give adequate attention to workforce and public health factors. The existing Kaiser Foundation threat assessment tool and FEMA	o Disaster planning processes/VA activities are reported as being conducted for the most part by external consultants and by administration. Other departments	▪ Many hospitals have been funded for the purchase of an array of emergency related equipment, but this is perceived to be without an overarching plan or	▪ Table top exercises and community drills appear to be the method to test threat scenarios and response plans. ▪ But drills focus on first-responder and

	be substituted for “Threat Assessment”. ▪ Terrorism Risk management was less well-understood due to focus on reducing medical mistakes/malpractice, not vulnerabilities.	Publication 246 utilized by the Dept. of Veterans Affairs need to be upgraded (prototype developed by NCR-UCIP).	appear to be only marginally involved in these tasks.	priority. Funding to sufficiently support vulnerability assessments and preparedness planning is lacking.	EMS elements and do not embrace the scope of problems that may be encountered by the whole of the healthcare organization.
Telecommunications	▪ Active involvement of Industry and Government in CIP programs. ▪ Practices, standards, and policies are evaluated to determine which are applicable based on environment and criteria. ▪ Risk Mgmt./Business Continuity is important to this industry since stable, reliable infrastructure is a competitive edge and key to success.	▪ The Service Providers/Vendors keep abreast of the latest technology, practices, and standards by participating in the various forums such as NRIC, the standards bodies, and the Telecom Information Sharing and Analysis Center.	▪ The application of appropriate tool(s) through resource allocation is done via company internal programs or as part of an industry coordinated effort.	▪ Risk management is performed both within the companies and sector via joint activities of the NCC, Telecom ISAC and within the National Security Information Exchange. Individual service providers also perform risk assessment/business continuity processes. Risk management and vulnerability assessments are on-going since threats are on-going and changing.	▪ The sector uses a variety of risk management tools and best practices to evaluate vulnerabilities. There are ongoing programs for evaluating effectiveness. ▪ The Network Reliability Steering Committee evaluates the major outage reports sent to the FCC by the service providers. The results are published quarterly.
Transportation/Postal and Shipping	▪ Generally speaking, transportation/postal and shipping service providers understand the value of executing Risk Assessment/ Risk Management activities.	▪ Some tools have been adapted from their intended application for use with another mode or service, but none exists for the regional level. ▪ WMATA conducted a comprehensive risk	▪ Regional mass transit operators, including WMATA, MARC and VRE have primarily allocated resources to comply with DHS security directive of 2004. WMATA has	▪ Measures in the region focus on preventing malevolent attacks, lessen the impact of an attack, and support public safety and transportation agencies responses to	▪ Primary focus of risk reduction evaluation is on its negative impact on the operational efficiency. If negative, Security service providers are reluctant to implement such

		assessment funded by ODP. ▪ MSHA has conducted an in-house prioritization of critical facilities. ▪ DC DOT has begun conducting VAs using a process prescribed by the FHWA.	received grant funding from ODP.	attacks and recover from them (e.g. RICCS and RECP ESF-1). A focal point of these measures is to ensure that safety of travelers and transportation workers.	strategies. ▪ To date, measures of effectiveness have not been defined for evaluating measures implemented to enhance security.
Water	▪ The water sector is aware of the value of critical infrastructure protection. By federal mandate, all water supply utilities were required no later than June 2004 to complete a VA.	▪ Appropriate tools are available, but consideration of cross-sector vulnerabilities has been limited. ▪ Vulnerability assessments have been conducted by all water suppliers with more than 3,300 customers. ▪ Some tools explicitly include some form of risk management (RAM-W, VSAT) while most do not. ▪ Challenges: Improve risk management tools for future use.	▪ The vulnerability assessment process has led to many projects to reduce vulnerabilities. Providing reliable service and not leaving vulnerabilities unaddressed are top priorities. ▪ It is difficult to judge the extent to which subsequent resource allocations to reduce these vulnerabilities were effective.	▪ A focus group utility ranked the list of proposed projects in order of largest relative-risk-reduction per unit cost. Those projects that showed large relative-risk-reduction per unit cost were considered for funding. Those with very small relative-risk-reduction per unit cost were not a funding priority. ▪ Challenges: Institute a regular schedule of risk reduction as part of an overall risk management plan.	▪ It is difficult to judge the extent to which subsequent resource allocations to reduce these vulnerabilities were effective.

APPENDIX E. KEY NCR CRITICAL INFRASTRUCTURE INTERDEPENDENCIES

Key Dependencies of each Sector on other Sectors
Note: Table should be read from Column to Row, for example the Dependency of Emergency Services (Column) on Banking and Finance (Row)

	Banking / Finance	**Emergency Services**	**Energy**	**Health**	**Transportation / Postal / Shipping**	**Telecom**	**Water**
Banking / Finance	Payment system for clearing and distributing cash Interrelationship among banking and finance companies through the payments system, including lending in Fed Funds market, syndicated loans and the regulatory structure; Personal and business investments, provision of credit Social security, other benefits payments Support payroll function (Maintain public confidence)	* Protection, security and surveillance of key facilities and personnel Chem/Bio/HazMat response and decontamination Fire and other public safety/emergency response needs	Primary electric power for computer and other electronic systems, including communications, surveillance, alarms, etc Power to run ATMs Fuels to maintain other operations, including global networks Short term backup power for critical operations	Information on health hazards, including communicable diseases, that could impact staff/operations	Movement of financial documents (checks, etc) Transport of staff to and from job site	Support to financial services business operations including computer networks and internet for business operations - to maintain funds and order transfers Customer Service	Primary services to sector Continuity of multi-sector business operations Consumption and sanitation needs of staff Cooling of computer rooms in core clearing and payment settlement systems

	Banking / Finance	Emergency Services	Energy	Health	Transportation / Postal / Shipping	Telecom	Water
Emergency Services **(Police, Fire, EMS, HazMat, & Public Works)**	Emergency financial support to persons impacted by disasters and to meet broad emergency services needs (equipment, supplies, transportation, etc.)	Staff available for fulfilling responsibilities, necessary equipment, and supplies Monitoring/protection of scarce water, medical and other supplies	Primary power for facilities (work areas, communications HVAC, lighting, refrigeration, vehicle maintenance, Emergency Operating Centers, Public Safety Answering Points (9-1-1 system) Short term backup power for critical functions Short term power for field operations Fuels for emergency and other vehicles, generators Power for shelters and emergency relocation facilities	Personnel prophylaxis, medical care of first responders and dependents Reception and processing of emergency medical transport Laboratory services, monitoring & analysis, medical supply management, medical personnel management, hospital facilities Surveillance, warning, epidemiology, prevention, and levels of protection Healthcare and monitoring of vulnerable populations and displaced persons	Movement between facilities and incident sites via roads, bridges and tunnels, etc. Movement of emergency response personnel, resources, and patients Movement of critical supplies and personnel during response and recovery Auxiliary equipment Evacuation support Distribution of support to displaced and vulnerable populations	Full range of emergency and administrative communications (radio, PSN, internet, 9-1-1 system and other alert and warning systems) to fixed and mobile facilities Communication to the public	Firefighting, decontamination, vehicle and building coolant, drinking and sanitary, patient care, and hospital laundry Water service to relocation sites and vulnerable populations

	Banking / Finance	Emergency Services	Energy	Health	Transportation / Postal / Shipping	Telecom	Water
Energy **(Electric Power, Fuels/Oil, & Natural Gas)**	Provide financial services critical to the functioning of this sector, including power markets, customer billing. Financial instruments to support emergency contracting	Firefighting, rescue, EMS and HazMat services for facilities (production, refining, storage, distribution) * Protection, security and surveillance of key facilities and personnel Threat information and criminal investigation * Perimeter or Site access control	Fuel suppliers Electric Transmission Power for critical functions, including security and surveillance of key facilities HVAC	Emergency medical care for staff Information on health hazards, including communicable diseases, that could impact staff/operations	Movement of fuels Movement of critical equipment and parts Conveying maintenance crews to sites for repair and restoration Delivery of remittances	Land and satellite based capabilities and networks, including Supervisory Control and Data Acquisition (SCADA); other process controls systems for energy monitoring and management, etc.	Cooling water Fire suppression

	Banking / Finance	Emergency Serv.	Energy	Health	Trans/Post. & Ship	Telecom	Water
Health	Provide financial services critical to the functioning of these sectors (billing, purchasing supplies and equipment, etc.). Financial instruments to support emergency contracting	Pre-hospital care (EMS) and transportation Threat information and criminal investigations * Protection, security and surveillance of key facilities and personnel * Perimeter or Site access control HazMat response and decontamination Population management for evacuation to isolation and quarantine Warning and prophylaxis for CBR for critical personnel * Debris clearance and structural evaluation (includes red/yellow tag	Primary power and energy to facilities Emergency power generation	Coordination between health care providers Lab and epidemiology services Personnel resources	Continued operation and maintenance of transportation networks and services Delivery of medical goods/medicine Movement of patients	Full range of emergency and administrative communications (radio, PSN, internet) to fixed and mobile facilities and with other healthcare facilities, including state agencies and the Centers for Disease Control	Basic services, including healthcare, sanitation, disinfection Wastewater systems (including contaminated runoff)

	Banking / Finance	Emergency Services	Energy	Health	Transportation / Postal / Shipping	Telecom	Water
Telecom	Access to funds/cash to support technicians (i.e. pay for vehicle fuel, local repairs, and purchases Critical financial services (billing, purchasing) Financial instruments to support emergency contracting	* Protection, security and surveillance of key facilities and personnel * Perimeter or Site access control Threat information and criminal investigations HazMat protection and decontamination (particularly for CBR) * Debris clearance and structural evaluation (includes red/yellow tag	Primary power for facilities (work areas, lighting, HVAC, refrigeration, vehicle maintenance) Short term backup power for critical functions Short term power for field operations Fuels for equipment, vehicles for maintenance personnel	Emergency medical care for staff Information on health hazards, including communicable diseases, that could impact staff/operations	Movement of equipment, parts, and supplies Delivery of remittances	Back up communications such as satellite phones, etc.	Water for fire suppression Cooling Water

	Banking / Finance	Emergency Services	Energy	Health	Transportation / Postal / Shipping	Telecom	Water
Transport / Postal / Shipping	Cash to support operations Provide range of financial services critical to the functioning of these sectors. Financial instruments to support emergency contracting Cash to support toll operations	Traffic and access control for emergency response * Protection, security and surveillance of key facilities and personnel HazMat protection, decontamination and response Chem/bio warning, prophylaxis and protection for critical personnel/travelers * Debris clearance and structural evaluation (includes red/yellow tag Threat information and criminal investigations * Perimeter or Site access control	Primary and emergency power to critical facilities and services (Air traffic control, SCADA, /process control systems, etc.) Power to signals, stoplights, etc. Shared-right-of-way, debris removal HVAC Terminal and parking operations. Processing facility operations Fuels of all types to operate cars, trains, plane, ships and lubricants for vehicles and equipment	Emergency medical care for staff Information on health hazards, including communicable diseases, that could impact staff/operations	Rail, road, air, maritime movement of people, goods, and services and Intermodal operations	Connectivity for voice, data, and imagery via radio, telephone, internet, and satellite (base-to-base, base-to-vehicle, vehicle-to vehicle) Electronic inventories, vehicle and product tracking systems, data bases, customer service information Signals, switching equipment, security systems, field devices, signage and detectors Traveler information systems	Firefighting and decontamination Cooling equipment, refrigeration, sanitation

	Banking / Finance	Emergency Services	Energy	Health	Transportation / Postal / Shipping	Telecom	Water
Water	Maintenance of revenue streams Financial instruments to support emergency contracting	First responder for incidents at facilities HazMat response * Protection, security and surveillance of key facilities and personnel Threat information and criminal investigations Monitoring, testing, protection, warning and health surveillance of key facilities and personnel * Debris clearance and structural evaluation (includes red/yellow tag) * Perimeter or Site access control	Primary and emergency power to critical facilities (e.g., pumping stations, SCADA systems; process control systems for chemical treatment) Short term backup power for critical functions Fuel for maintenance vehicles	Public health advisories Laboratory testing for contamination Patient treatment in the event of water contamination	Delivery of key chemicals or material Delivery of services (i.e. trucked water) Movement of maintenance personnel for response and recovery Delivery of remittances	Internal data communications for SCADA Connectivity for voice, data, and imagery via radio, telephone, internet, and satellite (base-to-base, base-to-vehicle, vehicle-to vehicle) Customer service	Provision of potable water, wastewater collection and treatment Monitoring, testing of water and water system,

APPENDIX F: ENDNOTES

[1] Title 10 USC Sec. 2674 (f) (2)

[2] The Urban Institute (2005) The Business of Doing Good in Greater Washington: How the Nonprofit Sector Contributes to the Region's Economy. Washington, DC: The Nonprofit Roundtable of Greater Washington. Data were last available for 2003.

[3] "Series of Disasters Paralyzes Capital Area at Rush Hour", the Washington Post, January 14, 1982.

[4] Hsu, Spencer S. (2005). "Anthrax Alarm Uncovers Response Flaws", The Washington Post, March 17, 2005, pg A01.

[5] Critical Infrastructure Protection Program (2004) Hurricane Isabel Critical Infrastructure Interdependency Assessment. Arlington, VA: George Mason University.

This Page Intentionally Blank