NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

CRITICAL INFRASTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT

FINAL REPORT AND RECOMMENDATIONS

OCTOBER 14, 2008

ALFRED R. BERKELEY, III
WORKING GROUP CO-CHAIR
CHAIRMAN AND CHIEF EXECUTIVE OFFICER
PIPELINE TRADING SYSTEMS, LLC

MARGARET E. GRAYSON
WORKING GROUP CO-CHAIR
PRESIDENT
COALESCENT TECHNOLOGIES, INC.

GILBERT G. GALLEGOS
WORKING GROUP CO-CHAIR
CHIEF OF POLICE (RET.)
CITY OF ALBUQUERQUE, NM

TABLE OF CONTENTS

ACKNOWLEDGEMENTS 1

1. EXECUTIVE SUMMARY 3

Current Situation 3
Findings 5
Recommendations 8

2. STUDY OVERVIEW 14

Objective 14
Scope 14
Approach 14

3. CURRENT SITUATION 16

Background 16
The Sector Partnership Model 16
Current State of the Sector Partnership 17
Important Partnership Considerations 18
Alternative Partnership Models 24

4. FINDINGS 26

General Observations 26
Partnership Principles and Concepts 27
Partnership Structure and Design 29
Partnership Implementation 30

5. RECOMMENDATIONS 32

Reaffirm the Critical Infrastructure Protection Mission and the Public-Private Partnership 32
Reinforce Key Principles of a Successful Partnership Structure 35
Update the Sector Partnership Model to Be More Efficient and Effective 37

6. IMPLEMENTATION STRATEGIES 42

Near-term Actions for the Private Sector 42
Near-term Actions for the Next Administration 44

APPENDIX A: SUMMARY OF THE SECTOR PARTNERSHIP MODEL 45

APPENDIX B: SUMMARY OF PREVIOUS NIAC RECOMMENDATIONS ON PARTNERSHIPS 51

APPENDIX C: ACCOMPLISHMENTS AND SUCCESSES OF THE SECTOR PARTNERSHIP 55

APPENDIX D: REFERENCES 60

Acknowledgements

Mr. Berkeley, Mr. Gallegos and Ms. Grayson wish to acknowledge the efforts of the entire Study Group and extend their deepest appreciation to all who have offered their time and advice to support this effort.

Working Group Members

Alfred R. Berkeley III, Chairman and CEO, Pipeline Trading Systems, LLC
Gilbert Gallegos, Retired Chief of Police, Albuquerque, NM
Margaret E. Grayson, President, Coalescent Technologies, Inc

Study Group Members

Mike Wallace, Vice Chairman, Constellation Energy (NIAC Member, Study Group Chair)
Peter Allor, Security Director, IBM
Patricia Andrew, Director of Corporate Communications, Coalescent Technologies
Scott Blanchette, Senior Vice President, Healthways
Chuck Canterbury, National President, Grand Lodge, Fraternal Order of Police
General John Gordon (Retired)
David Heyman, Director & Sr. Fellow, Center for Strategic and International Studies
J. Michael Hickey, VP, Government Affairs – National Security Policy, Verizon
Bruce Larson, American Water
Hugh J. Kiley, Jr., Assistant Vice President Operations, Norfolk Southern
Ronald R. Luman, National Security/Warfare Analysis Departments Head, Johns Hopkins University/Applied Physics Laboratory
Bill Muston, Manager, Research & Technology Development, Oncor Electric Delivery
Kevin Nietmann, Vice President, Constellation Energy Nuclear
Ken Watson, Senior Manager, Critical Infrastructure Assurance Group, Cisco Systems

CEO Roundtable

David Bronczek, President and CEO, FedEx Express (NIAC Member)
Wesley Bush, President and COO, Northrop-Grumman (NIAC Member)
Donald Correll, President and CEO, American Water
Donald F. Donahue, Chairman and CEO, The Depository Trust & Clearing Corporation
Denny Houston, Executive VP, ExxonMobil (NIAC Member)
David Kepler, Executive VP, Dow Chemical (NIAC Member)
Ben R. Leedle, President and CEO, Healthways, Inc.
Jim Nicholson, President and CEO, PVS Chemicals (NIAC Member)
Todd Ramsey, General Manager, IBM Global Government Industry
Jim Reid, President U.S. Eastern Division, CB Richard Ellis (NIAC Member)
Rick Sergel, President & CEO, North American Electric Reliability Corporation
Stephen Tobias, Vice Chairman and COO, Norfolk Southern Corporation
Bob VanderClute, Sr. Vice President, Association of American Railroads
Larry Weyers, President and CEO, Integrys Energy Group

Other Study Contributors

Valerie Abend, U.S. Department of Treasury, Banking and Finance Sector
Jim Bentley, American Hospital Association, Public Health and Healthcare Sector
Cherie Black, New Jersey Office of Homeland Security and Preparedness
Stuart Brindley, Independent Electricity Systems Operator, Energy Sector
James Caverly, U.S. Department of Homeland Security
Kathryn Condello, Qwest, Communications Sector
Clay Detlefsen, International Dairy Foods Association, Agriculture and Food Sector
Stuart Ferency, U.S. Transportation Security Administration, Postal and Shipping Sector
Jessica Fontinato, U.S. Department of Agriculture, Agriculture and Food Sector
Gary Forman, NiSource – Columbia Gas, Energy Sector
Kenneth Friedman, U.S. Department of Energy, Energy Sector
Jeff Gaynor, Business Executives for National Security
Thomas Hughes, AT&T, Communications Sector
Leeann Jackson, U.S. Food and Drug Administration, Agriculture and Food Sector
Shawn Johnson, State Street Global Advisors, Banking and Finance Sector
Rick Kane, RHODIA Inc., Chemical Sector
Lynne Kidder, Business Executives and National Security
Steven King, U.S. Department of Homeland Security
Mike Lesnick, Meridian Institute
Jan Mares, U.S. Department of Homeland Security
General Michael McDaniel, Homeland Security Advisor and Assistant Adjutant General for Homeland Security, Michigan; Chair, State, Local, Tribal, and Territorial Government Coordinating Council
Rod Nydam, Nydam Law Practice
Will Pelgrin, Director, Multi-State ISAC
Roger Platt, The Real Estate Roundtable, Commercial Facilities Sector
Tom Rhatigan, National Sheriff's Association, Emergency Services Sector
Lewis Roach, U.S. Transportation Security Administration, Transportation Systems Sector
Tim Scott, Dow Chemical, Chemical Sector
Lyman Shaffer, Pacific Gas & Electric (Retired), Dams Sector
Robert Stephan, U.S. Department of Homeland Security
Denise Swink, U.S. Department of Energy (Retired)
Brian Tishuk, Executive Director, ChicagoFIRST
Billy Turner, Columbus Water Works, Drinking Water and Water Treatment Systems Sector
Hung Trinh, U.S. Department of Health and Human Services, Public Health and Healthcare Sector
Kory Whalen, U.S. Department of Homeland Security, Emergency Services Sector
Nancy Wilson, Association of American Railroads, Transportation Systems Sector
Nancy Wong, U.S. Department of Homeland Security

Department of Homeland Security Resources

Jack Eisenhauer, Energetics Incorporated
Jennifer Rinaldi, Energetics Incorporated
Michael Schelble, SRA International
Matt Sickbert, SRA International

1. Executive Summary

The National Infrastructure Advisory Council (NIAC) affirms that productive collaboration among federal agencies, state and local governments, and the private businesses that own and operate roughly 90 percent of the nation's critical infrastructures will lead to a safer, more secure, and resilient United States. Because partnerships play a central role in homeland security, the NIAC endeavored to assess the effectiveness of the public-private partnership for critical infrastructure protection and recommend opportunities to strengthen it.

The public-private partnership to protect the nation's critical infrastructures is a novel collaboration that has been growing and maturing since the 1990s. After the September 11 terrorist attacks, it expanded to include additional sectors, businesses, and state, local, and regional entities. The partnership aligns the interests of the private and public sectors to work together toward the shared goal of secure and resilient infrastructures without the need for excessive regulation. The Council continues to believe that where market forces are free to operate, they will be the most efficient and efficacious vehicle to enhance the security posture of critical infrastructures (NIAC 2004).

The tangible benefits of this partnership can be seen in U.S. chemical facilities, nuclear power plants, water systems, transportation networks, and other critical infrastructures, which are safer and more secure than they were before the partnership – an achievement made in a non-partisan manner under Democratic and Republican Administrations. Members of the Council are impressed with the progress that has been made but also recognize the need for continued diligence to preserve and expand this valuable collaboration. Through this report, we wish to provide guidance to the current Administration and the executive branch under a new President in 2009.

Although the partnership is built on long-established relationships between business and government, its current configuration was developed by the Department of Homeland Security (DHS) in 2005. In that year, the NIAC provided recommendations to DHS on the structure, function, and implementation of a proposed Sector Partnership Model. Over the three years that followed, the new partnership took form, key relationships were solidified, and we learned a great deal about what works, what doesn't, and what will make the partnership stronger.

The NIAC formed the Strategic Partnership Assessment Working Group to examine the sector partnership and recommend improvements moving forward. To conduct this study, the Working Group convened a Study Group consisting of senior executives and subject matter experts with extensive experience across numerous industries and business functions. The Study Group was augmented by a CEO Roundtable of senior leaders from nearly every critical infrastructure sector to provide insight on what emerged as core issues: the value proposition for the sector partnership and the leadership needed to sustain it.

Current Situation

Critical infrastructures, such as financial networks, the electric grid, and communication systems, are the lifeblood of our country. As the backbone of America's vibrant economic and political

systems, they are essential to our everyday safety, health, and security. We have a national interest to ensure these infrastructures continue to be robust, reliable, and resilient in the face of possible natural or manmade risks. This responsibility is shared by the government, which has a mission to protect the nation against foreign and domestic threats, and the private sector, which has a responsibility to provide continuity of critical services and a bottom-line obligation to protect assets and shareholder value. This collective responsibility is best accomplished through a collaboration that leverages the respective capabilities of the government and the private sector: the government provides intelligence about potential threats and mobilizes public resources for protection, response and recovery, and the informed private sector uses this information to effectively manage risks and operate infrastructures in the face of such threats.

The current Sector Partnership reflects the policies of the National Strategy for Homeland Security (2002) and the roles and responsibilities outlined in Homeland Security Presidential Directive 7 (HSPD-7) (2003). The National Infrastructure Protection Plan (NIPP) (2006) established the Sector Partnership Model as the framework for coordinating protection of critical infrastructures and key assets through all levels of government and across 18 critical infrastructure sectors. This public-private partnership approach has become the centerpiece of the federal government's infrastructure protection strategy.

The Sector Partnership Model

The National Infrastructure Protection Plan (NIPP) outlines the roles and responsibilities of public and private sector partners to "build a safer, more secure, and more resilient America." It established the Sector Partnership Model to implement a public-private partnership to foster "integrated, collaborative engagement and interaction." The model consists of a series of parallel government and industry councils designed to encourage collaboration across the entire range of infrastructure protection activities. For each sector, the Government Coordinating Council (GCC) coordinates government strategies, programs, and communication; and the voluntary Sector Coordinating Council (SCC) coordinates the strategies and activities of asset owners and operators. To date, 18 GCCs have been established (one for each sector) and 16 SCCs have been established (two sectors are government only). Cross-sector coordination and leadership is supported by a Private Sector Cross-Sector Council and a Government Cross-Sector Council. Three entities are contained within these cross-sector councils: 1) the Partnership for Critical Infrastructure Security (PCIS), which coordinates private sector interests; 2) the Federal Senior Leadership Council, which coordinates federal government interests; and 3) the State, Local, Tribal, and Territorial Government Coordinating Council, which coordinates the interests of all other government entities.

The Sector Partnership Model is one of the most comprehensive public-private collaborations ever undertaken by the federal government. It engages nearly every major sector of the economy and every level of government to ensure safe, secure, and resilient infrastructures in a changing risk environment. Under the leadership of DHS Assistant Secretary for Infrastructure Protection Robert Stephan, industry, federal, state, and regional organizations have built a network of collaborative councils that forms a sustainable partnership structure. Tremendous progress has been made in building trusted relationships among partners, creating information-sharing mechanisms, and implementing government and industry programs designed to mitigate infrastructure risks. Each sector now has a tailored plan that outlines goals and strategies for protecting their infrastructure, and reports annual progress toward these goals. Above all, the partnership model has achieved results: financial institutions are better prepared for a possible pandemic, control systems of electric and water utilities are better protected from cyber vulnerabilities, chemical plant owners are better trained to respond to

a variety of emergencies, and many owners and operators have diligently made their sectors better protected, prepared, and resilient.

With this strong foundation, the partnership is well positioned to face the needs of the future; yet the partnership also faces challenges. Some sector councils have been slow to form, some are active but lack sufficient resources, and a few are largely inactive. Some companies feel the government does not understand business operations and has created too many partnership requirements. These requirements are sometimes established without adequate dialog with the sectors about the need for and use of information. Consistent private-sector involvement is complicated by unique sector characteristics and the stage of development that each partnership is in.

Most important, broader senior leadership from both industry and government is needed to strengthen our national resolve to secure critical infrastructures. What is needed now is acceptance of the long-term value of this vital partnership and reinforcement of the bonds that have built productive public-private relationships. This requires a commitment to provide a means for all critical infrastructure and key resource sectors and government components to engage in a partnership that best serves their mutual national interest.

Findings

The Council fundamentally believes, and our study has confirmed, that the public-private partnership has been successful and must continue. It represents the best long-term strategy to secure our critical infrastructures, in contrast to regulatory approaches that are less efficient, are less effective, and create antagonism between public- and private-sector entities that must cooperate to succeed. While no modern and open society can completely eliminate all risks, the partnership approach unites the special capabilities and expertise of the public and private sectors to minimize infrastructure risks. The Council recognizes that regulations and standards, if developed wisely with the full collaboration of the regulated private sector entities, have their place in protecting critical infrastructures. However, the Council considers a non-regulatory approach, which encourages industry and government to diligently pursue common national infrastructure protection goals while avoiding unnecessary costs and inefficiencies, to be the preferred approach and in the best interests of the nation.

Our principal finding, which provides the foundation for our recommendations, is that future government efforts to promote critical infrastructure protection and resilience must embrace a full-fledged partnership between the public and the private sectors. The achievements of the past six years have validated the promise of the public-private partnership model as a highly effective strategy. The Council strongly recommends that this approach be embraced and strengthened by the current and incoming Administration to continue the infrastructure protection effort and build greater resilience in our society.

Our key findings are organized into general observations about the partnership, the principles and concepts that underlie it, the appropriateness of the partnership structure to uphold these principles, and the effectiveness in implementing the partnership model.

General

Business and government alike strongly support the public-private partnership as the preferred strategy for reducing infrastructure risks. The advantage of this collaborative approach is that it facilitates the development of trusted relationships that are essential in times of crisis and allows for constructive engagement in developing policies and programs during periods of relative calm.

Significant progress has been made in implementing sector partnerships by effectively leveraging government and industry capabilities. The partnership has prompted numerous initiatives to share information, develop new technologies, and help assess vulnerabilities within sectors. These efforts have reduced physical and cyber risks within critical infrastructure sectors. To continue this progress, the federal government should improve agency coordination, fully engage all sectors, and increase its efforts with state and local governments and regional coalitions.

Partnership Principles and Concepts

A strong value proposition must be articulated and reaffirmed to sustain private-sector participation in the partnership. Businesses need a compelling rationale to participate in the sector partnership for an extended period of time. For most, the benefits of collaboration are clear. Yet for some companies, the value of the public-private partnership becomes less clear as infrastructure threats appear to recede and resource requirements increase. Continuing to articulate and reaffirm a strong value proposition will help retain and expand the commitment of business leaders who can dedicate needed intellectual and financial resources.

Protection and resilience must be complementary elements of an integrated risk management strategy. Private-sector partners emphasized the importance of resilience in managing risks to ensure a robust, reliable, and rapidly recoverable infrastructure. The protection and hardening of key facilities was an appropriate priority for business and government immediately after the 9/11 attacks. Now, businesses are embracing integrated risk management strategies that consider a variety of operational risks in an all-hazards environment. As such, resilience has become an important element of the value proposition for critical infrastructure protection because it recognizes both the need for security and the reality of business operations.

Continued leadership, commitment, and engagement from senior executives in both government and the private sector are essential. The most successful partnerships have a strong commitment from senior government and corporate executives who are informed and engaged on infrastructure issues. If executive participation in the sector partnerships is lacking from both the public and private sectors, the effectiveness of the partnership is compromised. Senior leadership is critical because it supports sector efforts to build key relationships, set priorities, take collective action, and commit resources to address infrastructure challenges. When government and corporate leaders meet, it is essential that it is a collaboration of equals who have the ability to commit to action.

Trusted relationships are central to an effective partnership. The willingness of partners to share sensitive information, commit resources, and take rapid action when needed is based on trusted relations developed between individuals and between organizations. The NIAC observed that the healthiest partnerships exist in sectors where longstanding relationships between industry and government built trust over time. Sectors with a limited track record of working with government are still in the process of building these trusted relationships.

Partnership Structure and Design

The overall design of the partnership is sound but additional flexibility is needed to accommodate diverse sector needs. The Sector Partnership Model is fundamentally sound and received high marks by most partners. Yet, the government must avoid a one-size-fits-all approach that has hindered some sector engagement. Some sectors are quite diverse, have a limited history of working with the government, or have a weak value proposition. A flexible partnership approach allows time for certain sectors to discern the benefits of the partnership and develop strong relationships.

Cross-sector interdependencies require more attention, given their importance in ensuring safe, secure, and resilient infrastructures. Leading companies and sectors view cross-sector interoperability as the new frontier in infrastructure resilience. As knowledge of individual sector vulnerabilities improves, greater emphasis is needed to understand cross-sector interdependencies and the expectations and limitations of interconnected sectors. Cross-sector coordination is also an important part of the value proposition for partnership participation.

There continues to be an imbalance between the resources available to support the current requirements of the Sector Partnership Model and the demands placed on it. Although DHS resources to support Sector Coordinating Councils (SCC) secretariat and planning functions were deemed very helpful in augmenting voluntary private efforts, many private-sector partners and Sector-Specific Agencies (SSA) noted that the efforts required to respond to government requests, meet government requirements, and fully support the sector partnership outrun the resources available to support these tasks.

Partnership Implementation

Productive partnership efforts can get bogged down by inefficient government processes and cumbersome requirements. Although we have seen improvement, there are still opportunities to make partnership interactions more efficient and less burdensome. Both private-sector partners and SSAs see the need to revise government requirements and improve the processes used to request, collect, disseminate, and report information. Early engagement of the private sector strengthens outcomes and reduces inefficiencies. The unintended consequence of inefficiencies is that partners spend too much time responding to government requests and not enough time addressing substantive security issues.

Better coordination among government entities will strengthen the partnership. Some sectors feel that poor coordination among government programs has led to conflicting guidance given to the sectors. Although most SSAs report improvement in their relationships with DHS, a

few still characterize their relationship with certain programs as fair or poor. In addition, some SSAs do not appear to be fully committed to their partnership role. Better representation, participation, and coordination within the Government Coordinating Council (GCC) will be needed to help fortify the partnership.

A lack of partnership experience and skills hinders collaboration. The most successful sector partnerships have involved individuals who possess strong collaborative skills, past partnership experience, and knowledge of the needs, expectations, and motivations of their partners. However, some industry and government partners have limited prior experience working in collaborative partnerships or an insufficient understanding about how their counterparts operate on a day-to-day basis. This can lead to a "culture clash" that produces misunderstandings about government and industry approaches to managing infrastructure risks.

Recommendations

Based on the above findings, the NIAC offers eight recommendations that will strengthen public-private collaboration to achieve safe, secure, and resilient critical infrastructures. They are organized within three important efforts that should be undertaken by both government and industry:

- Reaffirm the critical infrastructure protection mission and the public-private partnership
- Reinforce key principles of a successful partnership structure
- Update the Sector Partnership Model to be more efficient and effective

The Council recognizes that the partnership is dynamic and will require additional adjustments and improvements as conditions change. However, we believe reinforcing partnership fundamentals through senior leadership and expanded collaboration will provide the foundation for a strong and enduring partnership.

Reaffirm the Critical Infrastructure Protection Mission and the Public-Private Partnership

Recommendation 1. Reaffirm the importance of critical infrastructure protection and resilience as a fundamental mission of government and a responsibility of business.

The growing uncertainty of natural and manmade threats and the increasing interconnections among our business and economic systems make us inherently vulnerable to infrastructure disruptions that can cascade across multiple sectors. Today's infrastructure challenges are so complex that they must be addressed through a collaborative network of organizations coordinated through a unified preparedness and response framework. Government, business, and not-for-profit organizations share the responsibility to protect key assets and to design, build, and manage more resilient infrastructures. Both Democratic and Republican administrations have recognized the critical importance of this issue. Thus, the incoming Administration should affirm its commitment to critical infrastructure protection while promoting continuity in ongoing resilience efforts. The NIAC proposes the following actions:

- *The Secretary of Homeland Security should communicate the importance of the critical infrastructure protection and resilience mission to the presidential candidates and their transition teams.*
- *The leader of each Sector-Specific Agency should ensure that tailored briefing materials are prepared for the President's transition team and executive appointees covering the status of their sector's infrastructure protection issues and the role of the public-private partnership.*
- *The NIAC should conduct a study to examine what steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.*
- *The NIAC Secretariat should make this study widely available and distribute it to incoming members of Congress and staff, as well as to the leadership of the nation's private sector.*

Recommendation 2. Reinforce the partnership as a priority throughout government.

The public-private Sector Partnership Model has been successful and should gain greater prominence and acceptance across government with fuller, expanded participation in both the public and private sectors. The model calls for accountability of the partners as well as a government culture that reinforces and nurtures partnerships as a means of achieving infrastructure protection goals. The NIAC proposes the following actions:

- *The Secretary of Homeland Security and the White House should reaffirm the goals, objectives, and vision of the sector partnership.*
- *The new President should affirm his commitment to the public-private partnership and make it a priority throughout the government with cabinet-level accountability.*
- *DHS, in collaboration with the White House, should identify incentives to promote interagency cooperation in critical infrastructure protection.*
- *DHS and the Sector-Specific Agencies should encourage the Sector Coordinating Councils and the Government Coordinating Councils to develop strong working relationships with appropriate business organizations, and state, local, and regional security partners within the sector partnership.*

Reinforce Key Principles of a Successful Partnership Structure

Recommendation 3. Strengthen senior leadership engagement in and commitment to the partnership in both government and industry.

The transition to a new Administration and a new Congress creates an excellent opportunity to build a broader and stronger commitment to the sector partnership at all levels of business and government. This commitment must start at the top with the President, leaders in Congress, governors, and CEOs of leading companies from the various infrastructure sectors, publicly declaring their support for a sustained public-private partnership that leverages the best capabilities of industry and government to achieve national infrastructure protection goals. High-

level leadership is essential for strengthening the partnership and accomplishing a myriad of other improvements. The NIAC proposes the following actions:

- *The private sector should initiate a strategic dialogue between industry CEOs and the White House soon after the inauguration to reinforce their commitment to partnership principles, followed by similar dialogues with the Congressional leadership and state governors.*
- *Owners and operators of each critical infrastructure sector should clarify their value proposition and work with DHS or the Sector-Specific Agency to reinforce it among government security partners.*
- *Private industry and government partners should adopt a self-scalable sector engagement model that builds trust among peers at the executive and operational levels.*

Recommendation 4. Leverage relationships to maximize engagement

The broad variety of business, government, and not-for-profit partners must become more actively engaged in partnership activities to achieve national infrastructure protection objectives. In the business community, the first step is to fully engage critical infrastructure owners and operators. Next, the leaders of the 18 critical sectors must work to ensure that sector councils are truly representative and that council memberships are broad and strong. Finally, as Sector Coordinating Councils strengthen their bases, they should be encouraged to collaborate with an even broader array of organizations that are equally committed to protecting the nation's critical infrastructure and key resources. The partnership model can be enhanced by the Partnership for Critical Infrastructure Security (PCIS) and the sector councils establishing collaborative relationships with additional business, trade, and not-for-profit organizations. The NIAC proposes the following actions:

- *Each Sector Coordinating Council should develop a partnership map that identifies complementary and interdependent partners who can help strengthen the country's critical infrastructure security.*
- *DHS or the Sector-Specific Agencies should encourage each Sector Coordinating Council to develop strategies to diversify sector council membership and broaden partnership connections by tapping into established sector organizations.*

Update the Sector Partnership Model to Be More Efficient and Effective

Recommendation 5. Increase flexibility in the sector partnership to better accommodate diverse sector needs.

Sector characteristics and partnership history affect the speed at which each sector partnership develops and is able to meet NIPP requirements. While DHS has afforded greater latitude in how sectors govern themselves and respond to government requests, DHS should continue to modify their expectations and requirements for those sectors that require more time or different frameworks for advancing their partnerships. Established private-sector partners should advise other sector leaders, if requested, on ways to create highly effective public-private partnerships

that contain trusted relationships, strong sector representation, and adequate resources. The NIAC proposes the following actions:

- *DHS should tailor partnership requirements to match individual sector characteristics and partnership development needs.*
- *The Sector Coordinating Councils and the Partnership for Critical Infrastructure Security should nurture peer assistance and share lessons learned to help all sectors improve their partnership practices.*
- *DHS should encourage Sector Coordinating Councils to develop strategic roadmaps to enable sectors to articulate a variety of sector needs, identify sector priorities, and implement protection and resilience strategies.*

Recommendation 6. Emphasize cross-sector interdependencies and collaboration through the Sector Partnership Model.

Cross-sector planning and collaboration will help mitigate cascading failures and strengthen infrastructure resilience. As companies improve their internal security plans, they must also focus on key cross-sector and supply chain vulnerabilities. Many sectors indicated that addressing cross-sector interdependencies was an important priority and a key component of their value proposition. The NIAC proposes the following actions:

- *DHS and other federal organizations should increase resources to conduct cross-sector studies and analysis, guided by private-sector knowledge of infrastructure operations.*
- *Increase understanding of cross-sector interdependencies and capabilities, led by the sectors that have a well-established partnership and a strong security posture.*

Recommendation 7. Improve government practices and coordination in strengthening the Sector Partnership Model.

Partnerships take time to develop. During that development process, partners accept that adjustments are needed and certain government practices should be revised. For instance, sector partners should be consulted early and consistently to help the government define problems and identify solutions to emerging issues. Improved coordination among DHS (in its HSPD-7 leadership role), Sector-Specific Agencies, and Government Coordinating Council members, is needed to create a more unified voice and make the federal government a stronger partner. The NIAC proposes the following actions:

- *DHS and federal agencies should reinforce partnership engagement expectations throughout government and create a culture of collaboration that includes incentives, training, and compliance with the Ethics Guidelines.*
- *The Secretary of Homeland Security should encourage adherence to established partnership processes and roles as defined by the National Infrastructure Protection Plan.*

- *DHS and the Sector-Specific Agencies should put processes and practice in place to ensure that owners and operators are engaged in the early stages of developing policies, processes, and documents that may affect them or result in requests for sector information and inputs.*

Recommendation 8. Streamline government processes and requirements on the Sector Partnership Model and provide adequate resources to comply with them.

Many sector partners and Sector-Specific Agencies view government requirements and processes as too burdensome and, in some cases, unnecessary. To improve process efficiency and responsiveness to requirements, an analysis should be conducted of legal authorities and internal processes to determine how requirements might be streamlined. In addition, DHS should work with the SSAs to determine realistic response times for meaningful sector input and to clarify partner expectations in developing sector plans and products. The NIAC also observed that resources to support the partnership are imbalanced. While government uses dedicated full-time staff and contractors to support the partnership activities, most sectors rely on volunteer company staff and some trade association support. The secretariat support currently offered by DHS should be augmented to include dedicated planning and analysis services to help the SCCs and SSAs provide meaningful input and timely products. PCIS should investigate options for obtaining private-sector resources to develop and promote their priority initiatives. The NIAC proposes the following actions:

- *DHS should reexamine its internal reporting requirements, establish realistic response times, clarify expectations of the Sector Coordinating Councils and the Sector-Specific Agencies, and conduct an analysis of authorities and internal processes to determine how requirements might be streamlined.*

- *DHS and the private sector should increase the availability of resources, where appropriate, to meet DHS partnership requirements and requests for information.*

Path Forward

The public-private collaboration must maintain momentum into the next Administration and Congress. Accordingly, the NIAC recommends that CEOs, private-sector partners, and the incoming Administration implement the following actions within the first 100 days following inauguration.

Near-Term Actions for the Private Sector

1. **Empower the Private Sector Cross-Sector Council, to be a more proactive and strategic private sector body, able to engage and leverage CEO-level involvement and support as needed.**

2. **Arrange a CEO summit with the White House and with Congress in the first quarter of 2009 to solidify the sector partnership and build senior-level commitment to the partnership.** This summit should be well publicized and should include both private and

public sector senior executives as well as the leadership of private-sector organizations engaged in critical infrastructure protection**.**

3. **Support the rapid integration of the incoming Administration officials, members of Congress, and staff described in Recommendation 1.**

Near-Term Actions for the Next Administration

1. **In the first 100 days of the new Administration, the White House should implement the following actions contained in Recommendations 1 and 2.**

   - The Secretary of Homeland Security should communicate to both presidential candidates prior to the November 4th election the need to address homeland security issues as a priority during the transition period following the election, and request a meeting with appropriate members of the President-elect's transition team in November 2008.
   - The DHS Assistant Secretary for Infrastructure Protection should hold a follow-up meeting in December 2008 to provide a more specific briefing for appropriate members of the transition team. Private-sector partners should also participate in these briefings.
   - The leader of each Sector-Specific Agency should ensure that tailored briefing materials are prepared for the President's transition team and executive appointees covering the status of their sector's infrastructure protection issues and the role of the public-private partnership.
   - DHS, in collaboration with the White House, should identify incentives to promote interagency cooperation in critical infrastructure protection.
   - DHS and the Sector-Specific Agencies should encourage the Sector Coordinating Councils and the Government Coordinating Councils to develop strong working relationships with appropriate business organizations and state, local, and regional security partners within the sector partnership.

2. Study Overview

In October 2005, the National Infrastructure Advisory Council (NIAC) issued recommendations on the structure, function, and implementation of a new Sector Partnership Model outlined in the National Infrastructure Protection Plan (2006). Over the past three years, considerable progress has been made to implement the partnership model and the NIAC recommendations. Because the public-private partnership is central to the government's strategy to protect critical infrastructures, the NIAC resolved to form a working group to review recent developments in the partnership and help ensure its effectiveness as we transition to a new Administration.

Objective

The purpose of this study is to assess the effectiveness of the public-private partnership for critical infrastructure protection and identify opportunities to strengthen collaboration that can reduce risks to critical infrastructures. In particular, the NIAC sought to:

- Assess the effectiveness of the Sector Partnership Model in achieving its stated objectives
- Identify options to improve the efficiency and effectiveness of the partnership
- Identify opportunities to update the partnership model to respond to changing requirements

Scope

The NIAC Working Group focused its review on the conceptual design, structure, function, and implementation of the Sector Partnership Model as described in the National Infrastructure Protection Plan (NIPP). In its review, the Working Group sought to answer four fundamental questions:

1. Are the underlying principles of the partnership being fulfilled?
2. Is the basic structure of the partnership appropriate for the requirements?
3. Is the partnership model being implemented in an effective manner?
4. What steps can be taken to improve the efficiency and effectiveness of the partnership?

The Working Group limited its assessment to the eighteen sectors identified as critical infrastructures and key resources (CIKR or CI/KR) by the NIPP.

The national infrastructure protection policies that underlie the partnership model are described in HSPD-7, the National Strategy for Homeland Security, and the Homeland Security Act of 2002. The NIAC concurs with these policies and believes that they provide a strong foundation for the partnership model. As such, the Working Group did not conduct a separate assessment of these policy documents.

Approach

The study consisted of three interrelated phases.

- Phase 1 – Assess the current state of the sector partnership – Examine developments and progress in the sector partnership over the past three years and identify common successes and shortcomings.

- Phase 2 – Identify options and opportunities for improving the partnership – Determine the successes of high-functioning sectors and other successful partnership models to extract key lessons learned that could be incorporated into the Sector Partnership Model.
- Phase 3 – Recommend changes for improving the efficiency and effectiveness of the sector partnership – Build on past partnership successes and lessons learned to identify the steps that government and industry partners should take to improve the partnership moving forward.

To conduct the study, the NIAC convened a diverse study group consisting of senior executives and subject matter experts with extensive experience across the 18 CIKRs. The NIAC Study Group conducted and guided all aspects of the study through weekly and monthly conference calls. The Study Group gathered information from the following sources:

- A review of over 30 studies related to the public-private partnership, including several past NIAC reports
- Perspectives of senior executives and subject matter experts from business and government obtained through a total of 38 structured one-hour interviews
- A facilitated meeting with 15 members of the Partnership for Critical Infrastructure Security (PCIS) representing the leadership of the Sector Coordinating Councils (SCC)
- Presentations on innovative partnership models, forums, and organizations from leading experts
- Background research on partnerships, collaboration, and critical infrastructure needs

An important feature of the study was the formation of the CEO Roundtable whose members represented a spectrum of critical infrastructure sectors drawn from the larger Study Group. The CEO Roundtable included directors, presidents, CEOs, COOs, and senior executives of leading companies that discussed key issues, findings, and recommendations through monthly conference calls. The CEO Roundtable contributed invaluable insights that helped to validate and sharpen the study findings and recommendations.

3. Current Situation

The protection of the nation's critical infrastructures is a shared responsibility of the federal government, state and local governments, and private sector owners and operators. Governments are empowered to protect communities and the public, and businesses seek to protect customers, the supply chain, assets, and shareholder value. This principle guides decisions throughout business and government as they share the common goal of protecting the vital functions of critical infrastructures that serve our communities, businesses, government agencies, and the American people.

With nearly 90 percent of all critical infrastructure owned and operated by the private sector, it is essential that industry and government coordinate to protect these assets. To this end, the federal government has forged public-private partnerships to encourage coordination among federal agencies, state and local governments, not-for-profits, and the asset owners and operators who manage and operate critical infrastructures. By aligning the interests of business and government, the intellectual and financial resources of the private sector, state and local governments, regional organizations, and the federal government can be leveraged to reduce risks to critical infrastructures and key resources (CIKR).

Background

The public-private partnership for critical infrastructure protection has its roots in policies and relationships established before the September 11 terrorist attacks. The President's Commission on Critical Infrastructure Protection, formed in 1996, raised concerns about vulnerabilities to the nation's critical infrastructures. This led to Presidential Decision Directive 63 (1998), which created a national goal to protect the nation's critical infrastructure from intentional attacks. To meet this goal, the directive called for a *"public-private partnership to reduce vulnerability"* that should avoid outcomes that *"increase government regulation or expand unfunded government mandates to the private sector."* In the communications sector, public-private collaboration to secure critical infrastructures traces back even farther to the creation of the National Security Telecommunications Advisory Committee (NSTAC) in 1982 and the National Communication System (NCS) in 1962.

The current partnership, known as the Sector Partnership Model, was established in 2005 by the Department of Homeland Security (DHS). It reflects the policies contained in the National Strategy for Homeland Security (2002) and the roles and responsibilities outlined in Homeland Security Presidential Directive 7 (HSPD-7), issued in 2003. The structure, functions, roles, and responsibilities for the model were proposed in the Interim National Infrastructure Protection Plan (2005), modified by NIAC recommendations, and formalized in 2006 in the National Infrastructure Protection Plan (NIPP). The Sector Partnership Model is a cornerstone of the NIPP and has become the centerpiece of the federal government's infrastructure protection strategy.

The Sector Partnership Model

HSPD-7 is the primary authority that defines national policies for critical infrastructure protection. It identifies 17 sectors as "critical infrastructure and key resources" and defines roles

for a variety of security partners[1]. Each sector is aligned with a Sector-Specific Agency (SSA) that is assigned to a DHS office or another federal agency. The SSA serves as the key federal interface with the sector to provide coordination, planning and implementation of programs that reduce vulnerabilities and consequences of attack. Each SSA accomplishes this mission through risk-based assessments, industry best practices, protective measures, and comprehensive information sharing between industry and government. All SSAs are required to measure and report their progress to the Secretary of Homeland Security, the President, and Congress.

The core of the partnership model is a series of parallel coordinating councils formed for each sector. A Government Coordinating Council (GCC), led by its respective SSA, has been formed for each of the 18 sectors to coordinate federal, state, local, and tribal government interests for the sector. Voluntary Sector Coordinating Councils (SCC), which represent asset owners and operators, have been formed for 16 of the sectors (two sectors are government-only). Although most SCC members represent owners and operators from the private sector, some sectors, such as water, dams, and emergency services, have representatives from municipal, state, and federal government organizations that own and operate sector assets. In addition, many SCCs include industry association members who represent the interests of owners and operators, often for a distinct portion of the sector. Together, these coordinating councils form the basic structure through which security partners from all levels of government and the private sector collaborate to plan and implement programs aimed at reducing risks to critical infrastructures.

Coordination across sectors is reinforced through three additional groups. The Partnership for Critical Infrastructure Security (PCIS) is a private sector organization formed in 1999 that coordinates cross-sector initiatives to help ensure secure, safe, and reliable critical infrastructure services. PCIS includes representatives from each of the SCCs and is identified in the NIPP as filling the role of the Private Sector Cross-Sector Council. The NIPP also identifies a corresponding Government Cross-Sector Council, which includes the Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). In addition, a Regional Coordinating Council was created in 2008 to improve coordination with regional groups engaged in infrastructure protection. An additional description of the Sector Partnership Model is provided in Appendix A.

Current State of the Sector Partnership

The Sector Partnership Model is one of the most comprehensive public-private partnerships undertaken by the federal government, engaging nearly every major sector of the economy and every level of government. It seeks to address the security needs and expectations of a variety of highly diverse businesses, government organizations, and security partners under a common framework. In a very short time, industry, federal, state, and regional organizations have built a network of collaborative councils that forms a sustainable partnership structure. However, such complex partnerships take time for trust and relationships to develop. Also, infrastructure protection is a relatively new national paradigm in which the roles, responsibilities, and relationships of stakeholders are still evolving.

[1] In 2008, Critical Manufacturing was added as an 18th sector.

The sector partnership is at an important stage. Tremendous progress has been made in creating a foundational partnership structure, building trusted relationships among partners, creating information-sharing mechanisms, and implementing government and industry programs that help mitigate infrastructure risks. Sector-specific plans, which include tailored goals and strategies for implementing the NIPP, are now in place for each sector. Annual reports are prepared for each sector and metrics are used to track progress toward these goals.

While development of the partnership is a success, the partnership's true value lies in the tangible outcomes and accomplishments that improve security and reduce risks in critical sectors. Over the past five years, this collaboration has improved infrastructure protection and resilience in tangible ways that would not have occurred without it. For example:

- The financial services sector collaborated with the federal government to conduct an extensive, three-week voluntary exercise to improve the sector's preparation for a possible pandemic.
- The nuclear sector worked with multiple-agency teams to conduct comprehensive reviews of all of its power plants to identify potential soft spots in its already strong physical security practices.
- The water sector worked with EPA to develop consensus security metrics to help the sector track progress toward security objectives, thereby avoiding contentious regulations.
- The energy sector partnered with the Department of Energy, national laboratories, and equipment vendors to test sensitive control systems, isolate vulnerabilities, and implement fixes for both existing systems and new commercial products.
- Sectors that use control systems, including energy, water, nuclear, and chemical, used the partnership structure to work closely with DHS and national laboratories to mitigate a potentially serious cyber vulnerability that could affect many critical assets.

These examples illustrate how the sector partnership was pivotal in launching outcome-based security efforts that have made our critical assets safer, more secure, and resilient. Detailed descriptions of the above successes and additional examples are included in Appendix C.

Important Partnership Considerations

The current and future success of the partnership is influenced by several key considerations, including sector characteristics and diversity, the value proposition for owners and operators, the stage of partnership development, senior leadership involvement, and cross-sector interdependencies. Some of these factors present challenges for the partnership, but also opportunities to strengthen it. The large scope and scale of the sector partnership make it imperative that these factors are carefully considered and addressed.

Sector Characteristics and Diversity

The characteristics of a sector affect the ability and motivation of its companies to partner for infrastructure protection, and determine the nature of their collaboration. One key factor is sector diversity, including the variety and scope of sector operations, the number of companies and key assets, and the size and regional distribution of companies. Sectors such as electric and dams have fairly uniform and well-defined operations. By contrast, the commercial facilities sector

includes highly diverse activities and assets such as commercial real estate, sports stadiums, resorts, convention centers, hotels, shopping malls, and theme parks. Similarity in operations helps to provide common ground for identifying protection priorities, while highly diverse operations may present challenges.

The number, size, and regional distribution of companies also affect collaboration. The nuclear sector, for example, mainly encompasses the nation's 104 nuclear reactors, which are all owned by a small number of large companies. When a few well-resourced companies collaborate, collective decision making is often simpler. Firms in sectors such as financial services and oil and natural gas tend to concentrate in certain geographic regions, enabling close communication and convenient collaboration. By contrast, firms in the emergency services sector are geographically dispersed and represent smaller organizations, which makes national-level sector coordination more difficult.

Sectors that have a strong safety and security culture are more inclined to partner on infrastructure protection issues. For example, the chemical and nuclear sectors have sensitive physical assets that must be protected to prevent public exposure to harmful releases. Likewise, sectors such as financial services, energy, and information technology must protect critical cyber assets that are routinely attacked by malicious elements. As a result, companies in security-minded sectors have developed extensive internal security functions to protect assets and see clear value in collaborating to identify common solutions.

Sectors that operate in highly interconnected environments are also more inclined to collaborate with each other. The electric, communications, and IT sectors, for example, operate in complex national and regional networks that are highly interconnected with many sectors, making collaboration crucial. In the electric sector, for example, failure in one part of the grid can cascade to another part and potentially disrupt other sectors. Sector collaboration can help avoid this disruption, such as through the North American Electric Reliability Corporation (NERC), which was created after the Northeast blackout of 1965 to improve reliability across the entire electric grid. Today, the Critical Infrastructure Protection Committee of NERC serves as the SCC for the electricity sector and operates the Electric Sector Information Sharing and Analysis Center. Similarly, the communication sector has a productive 25-year partnership with the government to help maintain a reliable, secure, and resilient national communications posture. The National Security Telecommunications Advisory Committee (NSTAC) brings together industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies to provide collaborative advice and expertise to the President. In 1984, NSTAC launched the National Coordination Center for Telecommunications to provide operational emergency response capabilities.

Sectors that have a history of working with the government as a result of regulation, technology development, or integration of services tend to have an easier time adapting to the Sector Partnership Model. The financial services sector has worked in partnership with the Financial and Banking Information Infrastructure Committee (FBIIC), which coordinates the efforts of federal and state financial regulators concerning critical infrastructure issues. Additionally, the energy and nuclear sector have a long history of working with the Department of Energy to develop new energy technologies. Such public-private partnerships have produced healthy

relationships between the sectors and their SSAs and have enabled these sectors to quickly adapt to the NIPP Sector Partnership Model.

The Value Proposition for the Sector Partnership

One of the most important and elusive challenges of the sector partnership is defining a compelling value proposition for businesses to engage in the sector partnership for a sustained period of time. Different sector characteristics and circumstances influence each sector's motivation and interest in collaborating with the government on infrastructure protection issues. Even within a given sector or company, the value proposition is dynamic. During periods of crisis or heightened risks, business leaders are motivated by a direct concern to protect assets, customers, and people. During periods of relative calm, private sector motivation may diminish and shift to an interest in shaping national policy and minimizing regulatory influences.

A 2006 study by the Council on Competitiveness examined the business case for security in the post-9/11 environment. They found that leading industries and companies managed security and infrastructure protection in the broader context of resilience. These companies recognized an increasing level of operational risk – from globalization, sector interdependence, terrorism, pandemic potential, energy volatility, and climate – that could trigger interrelated, cascading disruptions. The study concluded that the ability of companies to anticipate and manage emerging risks and recover from disruption will become a competitive differentiator in the 21st century. In another study conducted by the Conference Board in the same year, a survey of 213 senior corporate executives found that over half of executives see excellence in security as a significant competitive advantage and over 40 percent feel the government is too concerned with terrorism and not enough with protecting routine business operations, which the NIAC found to be critical for maintaining continuity of critical infrastructure services to the public.

What Is Resilience?

Infrastructure resilience has been defined in various ways. For this study, we have adopted the definition provided by Stephen Flynn (2008). Resilience includes four factors: 1) **robustness** – the ability to keep operating or stay standing in the face of disaster, 2) **resourcefulness** – skillfully managing a disaster once it unfolds, 3) **rapid recovery** – the capacity to get things back to normal as quickly as possible after a disaster, and 4) **learning** – the ability to absorb new lessons that can be drawn from a catastrophe.

Each sector has a distinct value proposition that motivates companies to participate in the partnership for critical infrastructure protection. The financial services, IT, and energy sectors, for example, are motivated to partner with government agencies on cyber security issues because their member companies have critical electronic systems that are subject to constant threats from insiders, criminals, hackers, and other malicious actors. Sectors in which security is integrated into operations may have a stronger value proposition to collaborate with the government to better integrate infrastructure protection into their businesses.

While companies in some sectors have an inherent incentive to work together, other sectors do not. Several companies from fairly concentrated industries expressed a reluctance to meet with their business competitors due to antitrust concerns. Some companies are also concerned about having open discussions of threats and possible mitigations due to liability or other legal concerns. To address these concerns, that government provides two important enablers for the

value proposition. First, the government is often viewed as a neutral party, which eases companies' concerns about holding discussions with competitors. Second, Section 871 of the Homeland Security Act of 2002 provides a special exemption to the Federal Advisory Committee Act (FACA). This exemption allows companies to conduct sensitive discussions with their government counterparts without the requirement to provide public disclosure of the details of these discussions. This was a key recommendation of the 2005 NIAC report on *Sector Partnership Model Implementation* that was successfully implemented by the government.

Although the reasons for engagement are as diverse as the sectors themselves, there do appear to be some common denominators. The shared elements of the overall value proposition identified by executives and security professionals include the desire to:

- Better understand the threat landscape from government intelligence sources
- Build a more complete picture of sector interdependencies that could affect their operations
- Leverage resources and access new technologies of government programs
- Promote business concepts such as operational risk and resiliency in shaping national policies and programs
- Build trusted relationships at executive, operational, and organizational levels that are critical for emergency response, program development, and cross-sector interoperability

Partnership Development Process

Partnerships typically progress through different stages of development. The initial formation of a partnership is a prerequisite to the long-term, sustained work needed to achieve results and outcomes. Successful partnerships require a mutual value proposition, a set of clear objectives, discernable outputs to support the value proposition, and a clear sense that those outputs actually make a difference. They also need time.

The "culture" of partnership does not arise spontaneously. Sector partnerships at different stages of development have different requirements, support needs, and abilities to handle operational activities. Recognizing these differences and tailoring expectations is paramount to achieving long-term success. Well-developed partnerships are best equipped to deliver effective engagement behaviors and discernable outputs that produce desired outcomes.

Each sector partnership is at a certain stage of development, from early formation (e.g., the Critical Manufacturing Sector) to the implementation of robust initiatives (e.g., the Financial Services Sector). It can be argued that some sectors, such as the Emergency Services and Commercial Facilities sectors, are not true industrial sectors but rather related communities tied together by a common need to protect infrastructures and people. Many of their owners and operators may need additional time to form new relationships and outline their basic priorities. Well-defined sectors, such as Financial Services, Chemicals, and Energy, have longstanding relationships and have been able to advance quickly to focus on innovative initiatives involving complex cross-sector analysis.

To help protect the nation's critical infrastructures, DHS met an urgent need to establish SCCs and develop consistent Sector-Specific Plans. Although most sectors were able to meet this need, some sectors found themselves engaged in planning activities before their intra-sector relationships were fully developed. With the first versions of the plans now complete, these

sectors may be better positioned to reexamine their sector relationships, goals, and strategies, possibly through a high-level strategic dialogue with the government.

Role of Senior Leadership

Senior executives from both industry and government play a key role in the effectiveness of the sector partnership. Members of SCCs typically include the "practitioners" of infrastructure protection, including corporate security professionals, information officers, and government affairs managers, who must deal with either operational security issues or the infrastructure partnership processes that support them. Some councils include corporate executives, such as presidents, CEOs, COOs, CIOs, CSOs, and CISOs, although involvement varies greatly from sector to sector. Members of GCCs typically include government program managers and policy staff who are responsible for infrastructure-related activities within their agencies. Participation by government executives (e.g., assistant secretary or above) also varies from sector to sector, although the DHS Assistant Secretary for Infrastructure Protection, Robert Stephan, has regularly attended most SCC-GCC meetings.

Having the right people at the appropriate level of authority to work on the task at hand makes partnerships efficient and effective. A mix of staff-level personnel and executives as well as operational and government affairs professionals can help a SCC respond to a variety of tasks, decisions, and activities. However, this diversity also creates certain difficulties within a collaborative council because some individuals have the authority to commit to actions and provide resources while others do not. In addition, operational personnel tend to focus on security improvements and outcomes while government affairs personnel tend to focus on planning and government programs and processes. At times, these different perspectives may be at odds, affecting the effectiveness of the sector's security efforts and the type of relationship they have with the SSA.

The most successful partnerships have a strong commitment from senior government and corporate executives who are informed and engaged on infrastructure issues. Senior leadership is essential because it enables sectors to build key relationships, set priorities, take collective action, and commit resources to address infrastructure challenges. CEOs and senior government executives are uniquely positioned to offer both a strategic viewpoint and valuable resources to the public-private partnership for infrastructure protection. They are empowered to make immediate commitments of resources in a time of crisis. They also provide the vision needed for planning and strategy within the partnership, vital both during the response to an event and in preparation for the future.

Senior executive engagement and commitment should not be equated with frequent participation in meetings. Most sector partnership interactions focus on specific issues that are best addressed by security professionals and subject matter experts. CEOs and high-level government officials have very limited time to allot to partnership activities, yet their ongoing awareness of security issues is essential. Although executives typically delegate authority to their security professionals and other qualified representatives, the highest levels still need to be briefed and kept up to date on partnership activities and security matters. Executive participation can be effectively scaled, ready to be ramped up to full involvement in a time of crisis, provided that executives are informed on key issues and existing trusted relationships are in place.

Importance of Cross-Sector Interdependencies

Many businesses manage complex supply chains that operate across multiple companies, industries, countries, and time zones. The tight integration of services that supply materials, energy, transportation, and financing to businesses increases efficiency and improves competitiveness. By reducing lead times, minimizing inventories, and automating business processes, companies have been able to increase productivity and throughput. The increased use of cyber systems to control physical operations – previously studied by NIAC – also increases the productivity and functionality of complex systems.

Exhibit 1. Examples of Cross-Sector Interdependencies

- During the August 2003 Northeast blackout, most Banking and Finance sector companies in the affected areas recovered very smoothly due to successful collaboration with the power utilities to understand interdependencies. This permitted companies to develop the necessary provisions for backup generators and other emergency equipment. One of the market infrastructures, however, was unable to open until very late in the day on August 15th (even though it had the necessary backup generator capacity) because it was unable to activate its air conditioning systems to cool its data centers. The air conditioning system was dependent on steam from its power supplier and, due to the blackout, its power supplier was unable to generate the steam needed to drive the air conditioning. This interdependency between the electricity sector and the finance company had never been identified in the company's contingency planning.

- During the September 11, 2001 attacks in lower Manhattan, telecommunication services were disrupted when the 7 World Trade Center building collapsed into a major Verizon central switching office at 140 West Street that serviced approximately 34,000 businesses and residences, including the financial district. Although many financial firms were confident prior to September 11th that they had successfully put in place telecommunications infrastructures that had no "single points of failure," many connections failed on that day due to unforeseen factors. For example, prior to September 11th one brokerage firm had carefully implemented two completely separate telecommunications connections from its operations/data center complex in lower Manhattan, permitting it to communicate through separate connections through separate telecom "central offices" to the securities exchanges and other market infrastructures. Its normal ("primary") connections ran through the 140 West Street central office; its "backup" connections ran through a separate central office in midtown Manhattan. The brokerage firm did not understand that, due to Verizon routing procedures, the "backup" connection had to be manually activated by an operator at the 140 West Street central office before it could be used. When the 140 West Street central office collapsed, the "primary" connection became inoperable, but no one was able to activate the "backup" connection. The firm had to implement a completely new set of connections, which took several days to make operational. More extensive interactions between the telecommunications and banking and finance sectors prior to that event might have led to a more clear understanding by telecommunications companies of banking and finance sector needs, and by banking and finance companies of the complexities of assuring redundancy in the telecommunications networks.

- After September 11, a major water utility conducted risk assessments of its upstream and downstream interdependencies in order to determine critical suppliers that could affect their operations and key customers that could be affected during a prolonged service disruption. Their analysis revealed that part of the output from the utility's wastewater treatment process was the main source of cooling water for a nuclear power plant. This downstream interdependency had important implications for the water and electrical utilities if the treated wastewater output was disrupted. Based on this finding, the water company worked with the electrical sector partner to develop ways to reduce the vulnerability. This collaboration resulted in the water utility hardening some of their critical assets to resist attack as well as the nuclear facility increasing its on-site storage capacity for cooling water, thereby reducing the risk.

Although such integration creates economic benefits, it can expose companies to additional vulnerabilities. The complexity of today's interconnected infrastructures, particularly communications, energy, information technology, and financial services, make it difficult for other sectors to determine how vulnerable their businesses are to various types of service disruptions or cross-sector events. The increasing use of computers to manage and control infrastructure services such as electricity, water, and transportation also exposes infrastructures to new cyber risks. As sectors become more interdependent, the likelihood increases that a disruption in one sector or business will cascade across multiple sectors. The importance of understanding cross-sector interdependencies is illustrated by examples in Exhibit 1.

As companies continue to better understand how to manage their internal security risks, they are paying more attention to identifying and addressing cross-sector vulnerabilities. A company that assesses its interdependencies with the services of another sector can make informed decisions about how to prepare internally for possible disruptions (e.g., installing backup power systems) and how to work with companies in the other sector to provide needed services.

Alternative Partnership Models

The NIAC Study Group examined other successful partnerships to better understand the distinct factors that made them successful and derive any lessons learned that could be integrated into the Sector Partnership Model. The Group felt that the characteristics that make other partnerships and organizations successful could improve the long-term success of the sector partnership.

First, the Study Group identified factors that appeared to contribute to the success of the sector partnership based on numerous interviews with executives and subject matter experts. They then examined other partnerships that are within an industry, across industries, or between industry and government. This process helped to validate the preliminary success factors that the Group identified. A summary of the partnerships and organizations examined are shown in Exhibit 2.

The common success factors found in the most productive partnerships are shown below.

- A strong value proposition exists for partners to participate.
- Strong senior executive leadership allows partners to commit to action and direct resources.
- Trusted relationships exist among members.
- Adequate resources are available for the organization to function effectively.
- Sufficient flexibility exists within the organizational structure and practices to address emerging issues and cope with changing conditions.

The presence of these factors throughout the NIPP sector partnerships varies. For example, senior executive leadership was found to be strong in some sectors but weak in most. Elements of the value proposition also vary greatly along with their relative importance to the sector. Typically, strong executive engagement went hand in hand with a strong value proposition, as well as with other factors.

Exhibit 2. Comparative Partnership Models

The National Coordination Center for Telecommunications (NCC) provides coordination of the restoration and provisioning of national security and emergency preparedness telecommunication services and facilities during crises and disasters. Established in 1984, it has a permanent staff of government and loaned private sector employees that expands when needed. It is a combined effort of the nation's major telecommunications companies and the federal government. The NCC also serves as the information sharing and analysis center (ISAC) for the Communications sector and facilitates the exchange among government and industry participants on vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

Business Executives for National Security (BENS) is a national, non-partisan, not-for-profit organization comprised of more than 500 business executives committed to volunteering their time and talent to continuously improving the nation's security. BENS was founded in 1982 and is governed by a Board of Directors comprised of 36 members who are CEO's or of similar status. BENS has a permanent headquarters staff with regional offices and executive committees in 10 major metropolitan areas. Staff, offices, and other activities are funded primarily through membership dues with some additional revenue through charitable donations and grants. BENS has been a leader in the national security arena for many years and has played a major role in facilitating many public-private partnerships and homeland and national security initiatives.

Institute of Nuclear Power Operations (INPO) seeks to promote the highest levels of safety and reliability - to promote excellence - in the operation of nuclear electric generating plants. INPO membership includes owners and operators of the nation's commercial nuclear power plants and participation by nuclear power plant suppliers as well as international participants. INPO has a strong value proposition for its members in supporting strong safety and reliability performance. INPO was formed in 1979 and is funded by members' dues. It is headquartered in Atlanta, Georgia and has a permanent staff of INPO employees and loaned member employees.

The Financial Services Roundtable (FSR) is a CEO driven organization comprised of 100 member financial services companies that addresses issues important to the financial services sector. Members are drawn from the top 150 integrated financial services companies based on market capitalization. The FSR has a very experienced permanent staff and strong senior executive engagement from the financial services sector and has successfully addressed many financial services sector issues and initiatives.

Edison Electric Institute Business Continuity Task Force (BCTF) seeks to enhance operational continuity and prompt restoration of electric service following any event that disrupts normal utility operations. The BCTF addresses a broad range of issues related to maintaining operations: emergency preparedness and response (including response to acts of terrorism or health emergencies), mutual assistance, critical infrastructure security, and maintaining and sharing critical inventory. The BCTF includes about 10 electric utility company CEOs and reports to the board of Directors of the Edison Electric Institute. The Task Force is engaged to solve problems that are important to its CEOs on the task force and their companies. The Task Force meets minimally when no significant issues exist, typically holding about two phone calls of about one hour per year. In the event of a major business continuity event, such as a terrorist attack, the BCTF would meet to support a coordinated Electric industry response.

Industries of the Future (IOF) is a public-private partnership designed to improve the energy efficiency and productivity of energy-intensive manufacturers. The IOF was initiated in 1995 by the Department of Energy, which successfully built trusted relationships with key industries such as chemicals, steel, aluminum, and petroleum refining, as well as with companies in their supply chains. Shrinking corporate R&D budgets created a strong value proposition to form a collaborative partnership that aligns the R&D agendas of industry and government to focus limited resources on high-impact opportunities. DOE worked through existing industry associations to access owners and operators and allowed each industry to determine how to organize and engage. Industry executives developed a common vision for their industry, followed by an industry-led technology roadmap. Results are used by government to shape their R&D program and improve the relevance of their R&D activities. Industry benefits by leveraging government R&D to align with their priorities.

4. Findings

The Council fundamentally believes, and our study has confirmed, that the public-private partnership has been successful and must continue. It represents the best long-term strategy to secure our critical infrastructures, in contrast to regulatory approaches that are less efficient, are less effective, and create antagonism between public- and private-sector entities that must cooperate to succeed. While no modern and open society can completely eliminate all risks, the partnership approach unites the special capabilities and expertise of the public and private sectors to minimize infrastructure risks. The Council recognizes that regulations and standards, if developed wisely with the full collaboration of the regulated private sector entities, have their place in protecting critical infrastructures. However, the Council considers a non-regulatory approach, which encourages industry and government to diligently pursue common national infrastructure protection goals while avoiding unnecessary costs and inefficiencies, to be the preferred approach and in the best interests of the nation.

Our principal finding, which provides the foundation for our recommendations, is that future government efforts to promote critical infrastructure protection and resilience must embrace a full-fledged partnership between the public and the private sectors. The achievements of the past six years have validated the promise of the public-private partnership model as a highly effective strategy. The Council strongly recommends that this approach be embraced and strengthened by the current and incoming Administration to continue the infrastructure protection effort and build greater resilience in our society.

Our findings reinforce and build upon the recommendations of previous NIAC studies. Chief among them are that:

- Where market forces are free to operate, they will be the most efficient and efficacious vehicle to enhance the security posture of critical infrastructures.
- The partnership must be a collaboration of equals in which all partners bring value.
- All partners must have adequate and legitimate opportunities for meaningful participation.
- Partner roles and responsibilities must be clearly defined.
- The model generates true value when all partners work together effectively and efficiently.

Our key findings are organized into general observations about the partnership, the principles and concepts that underlie it, the appropriateness of the partnership structure to uphold these principles, and the effectiveness in implementing the partnership model.

General Observations

Business and government alike strongly support the public-private partnership as the preferred strategy for reducing infrastructure risks. Without exception, the executives and security experts we spoke with in industry and government support a collaborative approach to infrastructure protection, believing it is essential for achieving homeland security goals and in the best interest of the country. As indicated in our 2004 report on *Best Practices for Government to Enhance the Security of National Critical Infrastructures*, market forces that allow sectors to collectively achieve security goals are the most powerful drivers of change. The key advantage of a collaborative approach is that it facilitates the development of trusted relationships that are

essential in times of crisis and allows for constructive engagement in developing policies and programs during periods of relative calm. Collaboration is likely to increase as government and businesses embrace an all-hazards approach that emphasizes resilient, reliable, and robust infrastructures.

Significant progress has been made in implementing sector partnerships by effectively leveraging government and industry capabilities. The partnership has enabled numerous government programs to share information, contribute new technologies, and help assess risks with their sector partners. Under the leadership of the Department of Homeland Security (DHS), industry, federal, state, and regional organizations have created a network of interconnected coordinating councils under a common framework, providing a solid foundation for a sustainable partnership. These include 18 Government Coordinating Councils (GCC), 16 Sector Coordinating Councils (SCC), a non-federal government council (for state, local, tribal, and territorial governments), and a regional council. A Sector-Specific Plan has been developed for each sector that outlines tailored goals and strategies for implementing the National Infrastructure Protection Plan (NIPP). Each sector uses a common risk management framework to set goals, identify vulnerable assets, assess and prioritize risks, implement protective measures, and assess effectiveness. Sector annual reports are prepared and metrics are used to track progress toward goals. However, the sector partnership has not yet achieved its full potential. To continue this progress, the federal government should improve agency coordination, fully engage all sectors, and increase its efforts with state and local governments and regional coalitions.

Partnership Principles and Concepts

A strong value proposition must be articulated and reaffirmed to sustain private sector participation in the partnership. In today's demanding business environment, companies require a compelling value proposition to participate in the sector partnership for an extended period of time. The NIAC found that the value proposition varies by the characteristics of the sector, the requirements of individual companies, and the current threat environment. For most, the benefits of collaboration are clear. Yet for some businesses, the value of the public-private partnership becomes less clear as infrastructure threats appear to recede and resource requirements increase. Without a clear value proposition, it will become increasingly difficult for companies to provide voluntary staff resources and support to the partnership.

Effectively managing operational risks in an all-hazards environment is a fundamental responsibility of companies in critical infrastructure sectors. While each company and sector has a unique risk profile, the CEO Roundtable, formed for this study, identified several common benefits that motivate these groups to participate in the partnership, including:

- Having the opportunity to shape national policy and strategies for infrastructure protection by providing private-sector insights on infrastructure risk management and business decision processes
- Building personal relationships with government executive counterparts and CEOs in other sectors to better understand interdependencies, clarify business expectations, and share information that improves continuity planning

- Encouraging a non-regulatory approach as the preferred strategy to achieve national infrastructure protection goals that ensures market efficiency, encourages private sector investment, and promotes infrastructure resilience
- Sharing information with government counterparts to gain new insights and understanding of potential threats, vulnerabilities, and consequences that could affect their business operations at a strategic level
- Providing an opportunity for government and industry to build consensus on key infrastructure protection priorities

Protection and resilience must be complementary elements of an integrated risk management strategy. Private sector partners emphasized the importance of resilience in managing risks to ensure a robust, reliable, and rapidly recoverable infrastructure. The protection and hardening of key facilities and assets from terrorist attacks was a justifiable immediate priority for business and government after the 9/11 attacks. In the ensuing seven years, good progress has been made in protecting our most critical assets, and businesses are now embracing integrated risk-management strategies that consider a variety of operational risks in an all-hazards environment across the full spectrum of prevention, protection, response, recovery, and reconstitution activities. In critical chemical or nuclear facilities, for example, attacks cannot be tolerated because of the potential loss of life, making protection paramount. In other situations, such as electric delivery, brief power outages can be tolerated and rapid recovery is essential. As such, resilience has become an important dimension of critical infrastructure protection and a key element of the value proposition because it recognizes both the need for security and the reality of business operations.

The 2006 National Infrastructure Protection Plan recognizes the role of resilience in its overarching goal to "build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR." It supports an overarching risk-management strategy that acknowledges that individual sector needs may determine where "CI/KR resilience may be more important than CI/KR hardening." Yet most SCCs have focused their effort on protection activities rather than response and recovery activities, due to the composition of council membership and the strong emphasis on protection strategies contained in the NIPP.

Continued leadership, commitment, and engagement from senior executives in both the government and private sector are essential. The most successful partnerships have a strong commitment from senior government and corporate executives who are informed and engaged on infrastructure issues. If executive participation in the sector partnerships is lacking from either the public or private sectors, the effectiveness of the partnership is compromised. Senior leadership is critical because it enables a sector to build key relationships, set priorities, take collective action, and commit resources to address infrastructure challenges. CEOs and senior government executives are uniquely positioned to offer both a strategic viewpoint and valuable resources to the public-private partnership for infrastructure protection. They are empowered to make immediate commitments of resources in a time of crisis. They also provide the vision needed for planning and strategy within the partnership, vital both during the response to an event and in preparation for the future.

Too often, however, executive participation in the sector partnerships is limited from both the public and private sectors. This lack of participation can create a leadership void that hinders government and sector coordination and the national resolve to implement productive policies and programs. In sectors where relationships are still developing, senior executive leadership is even more important. Yet. the NIAC observed that in some instances senior leaders in these sectors have not been successfully engaged.

Because demands on a CEO's time are enormous, the value proposition must be compelling, the problems must be significant and tangible, and engagements must be targeted and efficient. As infrastructure threats appear to recede, it may become harder to sustain the engagement of senior leaders. Therefore, it is an opportune time to renew senior leader participation. This renewal effort will continue to require high-level participation from governmental officials; it is essential that when government and corporate leaders meet, it is a collaboration of equals with the ability to commit to action.

Trusted relationships are central to an effective partnership. The willingness of private and public-sector partners to share sensitive information, commit resources, and take rapid action when needed is based on trusted relationships developed between individuals and between organizations. The NIAC observed that the healthiest partnerships were found in sectors such as financial services and nuclear, where longstanding relationships between industry and government built trust over time. Sectors with a limited track record of working with government, such as the commercial facilities sector, are still in the process of building relationships with their government counterparts.

The NIAC also found that when trust is violated, which has happened in several sectors, it takes a long time to rebuild these relationships. For example, one sector recounted an incident that occurred when the government, without first consulting the sector, released non-critical, but commercially-sensitive, information to the public without regard to the potential impact it might have on the affected industry. To prevent this from happening, government must work to gain knowledge and understanding of its partners' business environments and competitive issues. The challenge of creating trusted relationships is compounded by the large turnover of DHS staff and company representatives to the councils.

Partnership Structure and Design

The overall design of the partnership is sound but additional flexibility is needed to accommodate diverse sector needs. The Sector Partnership Model described in the NIPP is fundamentally sound and was given high marks by most partners. Few could find fault with the overall structure of coordinating councils, the use of cross sector councils, and the Sector-Specific Agency (SSA) concept. Yet, the government must avoid the one-size-fits-all approach that has hindered some sector engagement. The sectors that are very diverse, have a limited history of working with the government, or have a weak value proposition are having the hardest time building their relationships and meeting DHS requirements.

The NIAC observed two basic types of sectors in the partnership: 1) "natural" sectors with integrated security such as nuclear, chemical, energy, and financial services; and 2) "combined"

sectors, such as commercial facilities, food and agriculture, public health and healthcare, and emergency services, where security is a common thread that connects related but sometimes disparate sector components. A flexible partnership approach allows time for certain sectors to solidify their value proposition and develop strong relationships.

Cross-sector interdependencies require more attention given their importance in ensuring safe, secure, and resilient infrastructures. Leading companies and sectors view cross-sector interoperability as the new frontier in infrastructure resilience. Throughout the United States and the world, businesses and supply chains are becoming more interconnected, physical and cyber systems are becoming more integrated, and the connections among sectors are becoming more complex. As knowledge of individual sector vulnerabilities improves, greater emphasis on understanding cross-sector interdependencies and the expectations and limitations of interconnected sectors will be needed.

Many sectors, particularly those with well-developed sector partnerships, expressed a strong desire to increase emphasis on cross-sector analysis, coordination, and emergency planning. The Partnership for Critical Infrastructure Security (PCIS) has a strong cross-sector mission and has initiated several important cross-sector efforts. However, it has been increasingly difficult for PCIS to sustain this focus due to increasing requirements from DHS. Cross-sector coordination is also an important element of the value proposition and was identified by the CEO Roundtable as a reason for joining the partnership and staying engaged.

There continues to be an imbalance between the resources available to support the current requirements of the Sector Partnership Model and the demands placed on it. Many private-sector partners and SSAs noted that the efforts required to respond to government requests, meet NIPP requirements, and fully support the sector partnership outrun the resources available to support these tasks. Unrealistic deadlines to respond to government requests and the lack of funding and personnel to meet numerous requests for information were frequently mentioned as problems with the partnership model. DHS resources to support SCC secretariat, facilitation, and strategic planning services are greatly appreciated by private sector partners and deemed very helpful in augmenting voluntary private efforts. However, these resources were either underutilized or insufficient to handle all requirements and requests, which some partners feel serve the government more than the private sector. Private sector partners often noted that their participation and donated time is entirely voluntary. Many SSAs also indicated that they have very limited resources to support DHS requirements, in part because their agency's core mission is only marginally related to the infrastructure protection mission.

Partnership Implementation

Productive partnership efforts can get bogged down by inefficient government processes and cumbersome requirements. While there is widespread support for public-private collaboration and the Sector Partnership Model, many partners feel that more can be done to improve how the government implements the partnership. Over the past three years, the NIAC has seen improvements in partnership implementation, but there are still opportunities to make interactions more efficient and less burdensome. Certain DHS requests were seen by partners as unnecessary or off the mark. Both private sector partners and SSAs see the need to revise the

NIPP requirements and improve the processes used to request, collect, disseminate, and report information. The unintended consequence of inefficient processes and unnecessary requirements is that the PCIS and many SCCs find they spend too much time complying with government requests and not enough time addressing substantive sector security issues.

Several partners noted that DHS does not always engage sectors in early discussions of key issues. Consulting with industry during the problem-formulation stage can save government and private-sector resources and lead to more informed and targeted solutions. Earlier engagement allows sector partners to participate in defining the problem, strengthening government understanding of the issue, and increasing sector-side engagement and buy-in to the resulting policy outcome.

Better coordination among government entities will strengthen the partnership. Some sectors feel that poor coordination among government organizations has led to conflicting guidance from the government. Although most SSAs report improvement in their relationships with DHS, a few still characterize their relationship with certain programs as fair or poor. In addition, some SSAs do not appear to be fully committed to their partnership role.

Redundant reporting requirements were cited as an example of the government's lack of coordination. Once required information has been reported to a federal agency, the expectation is that the government will share it appropriately and efficiently with other federal partners as needed. Better representation, participation, and coordination within the GCCs will help to fortify the partnership model.

The NIAC observed that some relationships between DHS and SSAs were dysfunctional or adversarial, even when the SSA resided within DHS. Causes seem to be varied but may include incomplete understanding of partnership principles, poor collaborative skills, or disagreement about respective organizational roles. Stronger and more consistent partnership behavior from participating government agencies will strengthen the value proposition for the sector partners, leading to more productive outcomes.

A lack of partnership experience and skills hinders collaboration. Strong partnership skills are key to successful public-private collaboration. The NIAC found that the most successful sector partnerships involved individuals who had strong collaborative skills, past partnership experience, and a good understanding of the needs, expectations, and motivations of their sector partners. However, some industry and government partners have limited prior experience working in public-private partnerships, which has hindered collaboration. The term “culture clash” was used by several partners to characterize misunderstanding and disconnects between government and industry approaches to managing infrastructure risks. The biggest complaint from industry was some government partners’ “command and control” mentality and lack of understanding of and experience with sector operations. The biggest complaint from government was industry’s lack of knowledge about government operations and processes that drive certain decisions and requests. The recently published *Critical Infrastructure Key Resources Sector Partnership Ethics Guidelines* outlines general principles for trusted partnerships for all sector partners and is a positive step toward establishing strong partnership practices.

5. Recommendations

The 2005 National Infrastructure Advisory Council (NIAC) report on *Sector Partnership Model Implementation* noted that a true partnership is based on a collaboration of equals in which all partners bring value. We maintain this belief and acknowledge two additional principles. First, both leadership and initiative are essential for the success of public-private collaboration. Accordingly, we propose that the private sector lead by example by endorsing and implementing recommendations that the private sector can initiate on its own to fortify the partnership. Second, leveraging relationships adds valuable capabilities to the partnership. We believe the partnership is strengthened when the sphere of partners is expanded to include organizations with legitimate expertise, interests, and equities in critical infrastructures. These principles are key themes woven throughout our recommendations.

The NIAC offers eight recommendations that will strengthen public-private collaboration to achieve safe, secure, and resilient critical infrastructures. The recommendations are organized into three important efforts that should be pursued by both government and industry:

- Reaffirm the critical infrastructure protection mission and the public-private partnership
- Reinforce key principles of a successful partnership structure
- Update the Sector Partnership Model to be more efficient and effective

The Council recognizes that the partnership is dynamic and will require additional adjustments and improvements as conditions change. However, we believe reinforcing partnership fundamentals through senior leadership and expanded collaboration provides the foundation for a strong and enduring partnership.

Reaffirm the Critical Infrastructure Protection Mission and the Public-Private Partnership

Recommendation 1. Reaffirm the importance of critical infrastructure protection and resilience as a fundamental mission of government and a responsibility of business.

The growing uncertainty of natural and manmade threats and the increasing interconnections among our business and economic systems make us inherently vulnerable to infrastructure disruptions that can cascade across multiple sectors. Today's infrastructure challenges are so complex that they must be addressed through a collaborative network of organizations coordinated through a unified preparedness and response framework. Government, business, and not-for-profit organizations share the responsibility to protect key assets and to design, build, and manage more resilient infrastructures. Both Democratic and Republican administrations have recognized the critical importance of this issue. Thus, the incoming Administration should affirm its commitment to critical infrastructure protection while promoting continuity in ongoing resilience efforts. The NIAC proposes the following actions:

- ***The Secretary of Homeland Security should communicate the importance of the critical infrastructure protection and resilience mission to the presidential candidates and their transition teams.*** Prior to the November 4th election, the Secretary of Homeland Security

should advise both presidential candidates on the need to address homeland security issues during the transition period. The Secretary should request a meeting with appropriate members of the President-elect's transition team in November 2008 in order to brief them on homeland security efforts. The DHS Assistant Secretary for Infrastructure Protection should also participate in that briefing, providing details as necessary to support the Secretary's position on the importance of critical infrastructure protection.

In December 2008, the DHS Assistant Secretary for Infrastructure Protection should hold a follow-up meeting, providing a more specific briefing on the critical infrastructure protection mission and the importance of the private-public partnership for appropriate members of the transition team. Private-sector partners should also participate in these briefings.

- ***The leader of each Sector-Specific Agency should ensure that tailored briefing materials are prepared for the President's transition team and executive appointees covering the status of their sector's infrastructure protection issues and the role of the public-private partnership.*** These briefing materials should be available for the presidential transition team and executive appointees upon their arrival at the agencies. The briefing materials should include a summary of key NIAC reports and their major recommendations, as well as contact information for the chairs and vice chairs of each Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). In addition, DHS and the SSAs should work with the SCCs and GCCs to develop a coordinated briefing to presidential appointees no later than March 2009.

- ***The NIAC should conduct a study to examine what steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.*** Resilience has become a central strategy for owners and operators in critical infrastructure sectors who manage a wide variety of operational risks in a competitive environment. Businesses must protect assets against plausible threats, as well as rapidly respond to and recover from emergencies and disruptions. Therefore, government and industry action plans for critical infrastructure protection must include steps for rapid response and recovery. Given the prominence of infrastructure resilience in business planning and government policy discussions, the NIAC should initiate a study on how best to integrate concepts of resilience and protection into a comprehensive national risk management strategy.

- ***The NIAC Secretariat should make this study widely available and distribute it to incoming members of Congress and staff, as well as to the leadership of the nation's private sector.*** In anticipation of the 111th Congress, this NIAC study and a summary of these recommendations should be provided to new and returning members of Congress and to critical infrastructure owners and operators through Sector Coordinating Councils, the Partnership for Critical Infrastructure Security (PCIS), and other business organizations associated with critical infrastructure protection.

Recommendation 2. Reinforce the partnership as a priority throughout government.

The public-private Sector Partnership Model has been successful and should gain greater prominence and acceptance across government with fuller, expanded participation in both the public and private sectors.[2] The model calls for accountability of the partners as well as a government culture that reinforces and nurtures partnerships as a means of achieving infrastructure protection goals. The NIAC proposes the following actions:

- ***The Secretary of Homeland Security and the White House should reaffirm the goals, objectives, and vision of the sector partnership.*** DHS and the new Administration should collaborate with sector partners to clarify the government's vision and reaffirm the goals and vision of the partnership. Once developed, this common vision must be communicated among the partners and serve as the basis for guiding future collaborative activities.

- ***The new President should affirm his commitment to the public-private partnership and make it a priority throughout government with cabinet-level accountability.*** This affirmation should reinforce the Sector Partnership Model as the government's central strategy for achieving critical infrastructure protection goals. Cabinet members who lead agencies that have Sector-Specific Agency responsibilities assigned in HSPD-7, including the Departments of Homeland Security, Defense, Energy, Interior, Treasury, Health and Human Services, and Agriculture, and the Environmental Protection Agency, should be held accountable for ensuring that adequate resources are available to support the sector partnership and that positive partner relationships are fostered. These cabinet members should communicate the importance of the critical infrastructure protection mission and the partnership model and make interagency and partnership cooperation a priority within their respective agencies.

- ***DHS, in collaboration with the White House, should identify incentives to promote interagency cooperation in critical infrastructure protection.*** DHS must encourage cooperation across government organizations, finding ways to promote a strong collaborative environment that reinforces cooperation toward a common mission and discourages competition that impedes that mission. DHS leadership should work with their counterparts at the Sector-Specific Agencies to clarify and reinforce HSPD-7 roles and responsibilities in the partnership. Work should be conducted within established roles to avoid the perception that DHS is encroaching upon the roles and responsibilities assigned to another agency. The next Administration should consider establishing an Office of Management and Budget (OMB) cross-cut for critical infrastructure protection and resiliency programs to provide greater transparency on agency efforts and resources. DHS leadership should also improve the dialogue among government partners within the Government Coordinating Councils to coordinate communications with partners and establish clear expectations for all members. The White House should work with DHS to identify positive incentives and/or performance

[2] The importance of expanding the prominence and acceptance of the critical infrastructure partnership in government is supported by a report issued by the GAO in 2007, titled *Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination* (GAO-08-36).

metrics to strengthen government cooperation and promote a common government voice in working with sector partners.

- ***DHS and the Sector-Specific Agencies should encourage the Sector Coordinating Councils and the Government Coordinating Councils to develop strong working relationships with appropriate business organizations, and state, local, and regional security partners within the sector partnerships.*** The NIAC is encouraged by the successful creation of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) and the recent addition of the Regional Coalition Coordinating Council. Yet both organizations are still in the early stages of developing their relationships with the various Sector Coordinating Councils and the Government Coordinating Councils. Both councils will need to create the systems, processes, and protocols that will ensure sustainable interconnections and relationships at the organization level as personnel change. DHS should continue to provide support for the rapid development and integration of the newly forming regional coalition groups through the Regional Coalition Coordinating Council. DHS should provide this support without creating requirements that could interfere with organic development around regions and critical infrastructure protection issues of concern.

Reinforce Key Principles of a Successful Partnership Structure

Recommendation 3. Strengthen senior leadership engagement in and commitment to the partnership in both government and industry.

The transition to a new Administration and a new Congress creates an excellent opportunity to build a broader and stronger commitment to the sector partnership at all levels of business and government. This commitment must start at the top with the President, leaders in Congress, governors, and CEOs of leading companies from the various infrastructure sectors, publicly declaring their support for a sustained public-private partnership that leverages the best capabilities of industry and government to achieve national infrastructure protection goals. High-level leadership is essential for strengthening the partnership and accomplishing a myriad of other improvements. The NIAC proposes the following actions:

- ***The private sector should initiate a strategic dialogue between industry CEOs and the White House soon after the inauguration to reinforce their commitment to partnership principles, followed by similar dialogues with the Congressional leadership and state governors.*** CEOs representing each of the critical infrastructure sectors should host a meeting with the leadership of the new Administration and the new Congress to initiate a strategic dialogue on national infrastructure priorities and policies. This initial meeting should be held soon after the transition in Administrations and should help to clarify policy objectives, build trusted relationships between government and industry leaders, and strengthen the value proposition. These actions will form the foundation for a sustained commitment to public-private collaboration.

While the meeting should focus on strategic issues, it should also educate leaders on partnership accomplishments and challenges. Because information sharing is integral to critical infrastructure protection, the meeting should seek to improve executive understanding on this topic. The government should discuss the requirements, resources, terms, and conditions of information sharing with the private sector. The discussion should also identify opportunities to strengthen partnership interaction in priority areas of the owners and operators.

- ***Owners and operators of each critical infrastructure sector should clarify their value proposition and work with DHS or their Sector-Specific Agency to reinforce it among government security partners.*** The partnership must produce significant value to all partners to ensure participation. To strengthen the value proposition, the private sector must clearly articulate their key needs and expectations to government, such as the opportunity to build trusted relationships, shape policy, reach consensus on priorities, build critical cross-sector relationships, share valuable information, and promote non-regulatory approaches to achieve infrastructure resilience and protection.

  The Secretary of Homeland Security and the Sector-Specific Agencies, consistent with their HSPD-7 responsibilities, should reinforce the private sector value proposition among the government partners. They should emphasize distinct private sector issues and priorities, such as the need for insightful threat information, cyber security improvements, or cross-sector initiatives to address interdependencies. The private sector partners, through the Partnership for Critical Infrastructure Security and Sector Coordinating Councils, should help refine the value proposition among their members to clarify desired needs and outcomes that reflect unique sector characteristics and risk conditions.

- ***Private industry and government partners should adopt a self-scalable sector engagement model that builds trust among peers at the executive and operational levels.*** A scalable engagement model supports two types of participation. At the operational level, it supports ongoing planning, program development, analysis, and information sharing among corporate security managers, subject matter experts, and their government counterparts. These individuals are most capable in determining how risks can be reduced throughout their enterprises and sectors. At the executive level, it enables CEOs, the Secretary of Homeland Security, and government leaders to come together to set strategic direction and build the trusted relationships that are essential in times of crisis. When the threat is believed to be lower, executive engagement is minimal but sufficient to establish trusted relationships. If threats increase, executive involvement scales up, commensurate with the emerging threat. If a significant event occurs, executive engagement increases to bring needed leadership to an appropriate response. The trusted relationships developed prior to the event support a stronger, more effective response. The NIAC believes that the Private Sector Cross-Sector Council of the Sector Partnership Model can be configured to accommodate senior executive participation for this scalable engagement model.

Recommendation 4. Leverage relationships to maximize engagement

The broad variety of business, government, and not-for-profit partners must become more actively engaged in partnership activities to achieve national infrastructure protection objectives. In the business community, the first step is to fully engage critical infrastructure owners and operators. Next, the leaders of the eighteen critical sectors must work to ensure that sector councils are truly representative and that council memberships are broad and strong. Finally, as Sector Coordinating Councils strengthen their bases, they should be encouraged to collaborate with an even broader array of organizations that are equally committed to protecting the nation's critical infrastructure and key resources. The capabilities of other business groups complement the work of the Partnership for Critical Infrastructure Security and individual Sector Coordinating Councils. The partnership model can be enhanced by the PCIS and the sector councils establishing collaborative relationships with complementary business, trade, and not-for-profit organizations. The NIAC proposes the following actions:

- ***Each Sector Coordinating Council should develop a partnership map that identifies complementary and interdependent partners who can help strengthen the country's critical infrastructure security.*** Partners in each sector should develop a partnership map that identifies existing strategic and complementary partners that can help strengthen the country's critical infrastructure protection. The maps should show intra-sector relationships, important ties to other interdependent sectors, and ties to appropriate regional organizations. The completed maps should identify where new relationships should be established, or existing ones strengthened, to enhance critical infrastructure protection. The partners in each sector should use this map to improve business emergency preparedness, outreach, education, and collaboration activities.

- ***DHS or the Sector-Specific Agencies should encourage their respective Sector Coordinating Council to develop strategies to diversify sector council membership and broaden partnership connections by tapping into established sector organizations.*** The NIAC observed that the most effective Sector Coordinating Councils have a healthy mix of owner and operators who understand security operations, and representatives of industry associations who have a broad understanding of sector needs and government policymaking. Certain industry organizations also have well-established and trusted sector relationships that can be leveraged to increase participation in the Sector Partnership Model. For example, the Financial Services Roundtable, the North American Electric Reliability Corporation, and the Real Estate Roundtable are using their organizations to increase the awareness of owners and operators and integrate them into SCC partnership efforts. Outreach in each sector should seek opportunities to broaden CEO engagement within the owner-operator community as well as key national organizations.

Update the Sector Partnership Model to Be More Efficient and Effective

Recommendation 5. Increase flexibility in the sector partnership to better accommodate diverse sector needs.

Sector characteristics and partnership history affect the speed at which each sector partnership develops and is able to meet NIPP requirements. While DHS has afforded greater latitude in how sectors govern themselves and respond to government requests, DHS should continue to modify their expectations and requirements for those sectors that require more time or different frameworks for advancing their partnerships. Established private sector partners, if requested, should advise the leadership of other sectors on ways to create highly effective public-private partnerships that contain trusted relationships, strong sector representation, and adequate resources. The NIAC proposes the following actions:

- ***DHS should tailor partnership requirements to match individual sector characteristics and partnership development needs.*** The current Sector Partnership Model does not fully account for the variations between and among sectors, or the distinct challenges that each sector faces in achieving its desired outcomes. The NIAC observed that some sectors that are in the process of developing their partnerships have a limited capacity to contribute to Sector Specific Plans, Sector Annual Reports, and metrics development, which are required of all sectors. In the past, if sector input was difficult to obtain, the Sector-Specific Agencies provided that input, often with little or no sector participation or buy-in, which created frustration and eroded trust. The NIAC recommends that DHS work with the Sector-Specific Agencies and the leaders of the Sector Coordinating Councils to identify sectors that need additional time in developing meaningful partnerships, modify government reporting and planning requirements as appropriate, provide more flexibility in completing essential tasks, and provide tailored resources and capabilities to assist them.

- ***The Sector Coordinating Councils and the Partnership for Critical Infrastructure Security should nurture peer assistance and share lessons learned to help all sectors improve their partnership practices.*** The NIAC recommends that sectors that have strong and well-developed partnerships assist newer or more diverse sectors to build strong partnerships. The Partnership for Critical Infrastructure Security has proven to be an ideal organization for nurturing such cross-sector, peer assistance. Working through the PCIS, the more experienced sector leaders should develop a set of best practices and lessons learned to assist new or developing Sector Coordinating Councils or subcouncils. In addition, DHS, working with appropriate Sector-Specific Agencies and Sector Coordinating Councils, should establish guidelines to assist sectors in developing healthy partnerships with trusted relationships and strong sector representation. Senior executive involvement will also help ensure that a strategic sector organization is achieved. This will result in more consistent, efficient development across all sectors.

- ***DHS should encourage Sector Coordinating Councils to develop strategic roadmaps to enable sectors to articulate a variety of sector needs, identify sector priorities, and implement protection and resilience strategies.*** Not all owners and operators believe the Sector-Specific Plan reflects their sector's strategies and priorities for reducing infrastructure risks. Some Sector Coordinating Councils claim they had little or no input into the final plans, while others feel that their plan is adequate yet not detailed enough to indicate their sector priorities and desired programs. The NIAC encourages sectors to voluntarily develop strategic roadmaps, similar to the cyber roadmaps developed by the energy and water sectors, to outline sector needs, priorities, and initiatives for reducing infrastructure risks. Although

DHS has made contractor resources available to Sector Coordinating Councils to develop business plans and strategic roadmaps to advance partnerships, these resources have only been used by a limited number of Sector Coordinating Councils. DHS should continue to provide financial support for contract resources to assist sector coordinating councils in developing these plans. It is important, however, that planning efforts be led by sectors to ensure they reflect sector goals and priorities without government influence.

Recommendation 6. Emphasize cross-sector interdependencies and collaboration through the Sector Partnership Model.

Cross-sector planning and collaboration will help mitigate cascading failures and strengthen infrastructure resilience. As companies sharpen their internal security plans, they must also focus on key cross-sector and supply chain vulnerabilities. Many sectors indicated that addressing cross-sector interdependencies was an important priority and a key component of their value proposition. The NIAC proposes the following actions:

- ***DHS and other federal organizations should increase resources to conduct cross-sector studies and analysis, guided by private-sector knowledge of infrastructure operations.*** Cross-sector vulnerabilities often reveal themselves only after a disruption occurs. Although DHS has conducted studies that explore vulnerabilities along supply chains and between sectors, many private-sector partners believe more emphasis should be placed on cross-sector study and analysis, with a focus on recognized threats. Some government modeling, simulation, and analysis efforts may not fully consider how the private sector plans for emergencies and how decisions are made during a crisis. Therefore, the NIAC recommends that DHS increase government resources for conducting studies and exercises that address cross-sector interdependencies and that these efforts be informed by private sector experts through the Sector Coordinating Councils. As interdependency risks are identified, DHS should work with industry to develop solutions for mitigating risks that have no business case for investment.

- ***Increase understanding of cross-sector interdependencies and capabilities, led by the sectors that have a well-established partnership and a strong security posture.*** Not many sectors fully understand, nor have they tested, their interdependencies to identify and eliminate single points of failure. Even fewer understand all of the downstream effects of their disruptions. Several sectors, such as financial services, chemicals, nuclear, rail, water, and energy, are leading efforts to better understand the risks posed by their interdependencies with other sectors. Many of these interdependencies extend beyond critical infrastructures to include other sectors and services, such as day care services needed for essential employees during a crisis. Understanding interdependencies is detailed work that requires extensive dialogue and analysis among sectors. The NIAC recommends that the highly interconnected sectors lead efforts to work bilaterally through the Sector Coordinating Councils, and collectively through the Partnership for Critical Infrastructure Security to explore and examine cross-sector interdependencies. National planning priorities and sector best practices should be considered; however, interdependencies typically occur at the local or regional level, which is where these studies should focus.

Recommendation 7. Improve government practices and coordination in strengthening the Sector Partnership Model.

Partnerships take time to develop. During that development process, partners accept that adjustments are needed and certain government practices should be revised. For instance, sector partners should be consulted early and consistently to help the government define problems and identify solutions on emerging issues. Improved coordination among DHS (in its HSPD-7 leadership role), Sector-Specific Agencies, and Government Coordinating Council members is needed to create a more unified voice and make the federal government a stronger partner. The NIAC proposes the following actions:

- ***DHS and federal agencies should reinforce partnership engagement expectations throughout government and create a culture of collaboration that includes incentives, training, and compliance with the Ethics Guidelines.*** Public-private partnerships are a relatively new government phenomenon. The skills and experience needed to successfully develop and implement partnerships with the private sector are not widely found in government. In addition, there are few incentives for government employees to foster successful partnerships. DHS should support partnership skills training for government personnel (at all levels – from new hires to the SES level) who have partnership assignments. DHS should also create employee incentives and target recruitment of liaison staff for private-sector outreach. In addition, DHS Ethics Guidelines can reinforce partnership expectations and promote collaborative behaviors among partners. The NIAC recommends the full adoption of the Ethics Guidelines and annual compliance review for both government and private-sector partners.

- ***The Secretary of Homeland Security should encourage adherence to established partnership processes and roles as defined by the National Infrastructure Protection Plan.*** The NIAC recognizes the importance of flexibility in the Sector Partnership Model and opposes artificial limits to productive government-private sector communications. However, until trusted relationships are established, the Secretary of Homeland Security should insist upon the use of established partnership protocols by all DHS personnel. This includes the need to encourage government and private-sector communications through established Sector Coordinating Councils and Sector-Specific Agencies, as recommended by the NIAC in its 2005 report on *Sector Partnership Model Implementation.*

- ***DHS and the Sector-Specific Agencies should put processes and practices in place to ensure that owners and operators are engaged in the early stages of developing policies, processes, and documents that may affect them or result in requests for sector information and inputs.*** Partners should engage early in information requests and problem solving with a full explanation of the reason the information is needed as well as clarity on what is needed. Early engagement results in a better product and enhances the partnership relationship.

Recommendation 8. Streamline government processes and requirements in the Sector Partnership Model and provide adequate resources to comply with them.

Many sector partners and Sector-Specific Agencies view government requirements and processes as too burdensome and, in some cases, unnecessary. To improve process efficiency and responsiveness to requirements, an analysis should be conducted of legal authorities and internal processes to determine how requirements might be streamlined. In addition, DHS should work with Sector-Specific Agencies to determine realistic response times for meaningful sector input and to clarify partner expectations in developing sector plans and products. The NIAC also observed that resources to support the partnership are imbalanced. While government uses dedicated full-time staff and contractors to support the partnership activities, most sectors rely on volunteer company staff and some trade association support. The secretariat support currently offered by DHS should be augmented to include dedicated planning and analysis services to help the Sector Coordinating Councils and Sector-Specific Agencies provide meaningful input and timely products. Partnership for Critical Infrastructure Security should investigate options for obtaining private sector resources to develop and promote their priority initiatives. The NIAC proposes the following actions:

- ***DHS should reexamine its internal reporting requirements, establish realistic response times, clarify expectations of the Sector Coordinating Councils and the Sector-Specific Agencies, and conduct an analysis of authorities and internal processes to determine how requirements might be streamlined.*** Sector products should provide explicit value for the sector itself. They must serve the needs of the sector as effectively as they serve the needs of the Sector-Specific Agencies. To maintain balanced partnership outcomes, DHS and the Sector-Specific Agencies must work together to establish streamlined approaches to critical infrastructure protection planning and reporting. Explicit expectations should be set to enable partners to properly estimate the allocation of resources required to develop sector plans and products. Appropriate flexibility must be allotted for the private sector to meet those obligations. Sector products should not only meet National Infrastructure Protection Plan requirements, but provide explicit value for the sector itself, motivating member participation and buy-in of results.

- ***DHS and the private sector should increase the availability of resources, where appropriate, to meet DHS partnership requirements and requests for information.*** The government must provide the necessary support to Sector Coordinating Councils, to meet government-imposed planning and reporting requirements. The form and degree of that support depends on the needs of the sector. Sector Coordinating Councils must be made aware of available support services and that such support is offered without the potential to compromise Sector Coordinating Council independence.

6. Implementation Strategies

The National Infrastructure Advisory Council (NIAC) identified the strategies below to implement several of its recommendations. These strategies include concrete, near-term steps that will help strengthen the partnership by expanding the engagement of private- and public-sector leaders, providing private-sector resources to proactively address cross-sector issues, and developing the leader-to-leader relationships that will enable the nation to more effectively respond to a major emergency. Implementation of these strategies should provide prompt, tangible value to the partnership.

Near-term Actions for the Private Sector

The NIAC believes the private sector should lead by example to fortify the partnership. The Private Sector Cross-Sector Council of the Sector Partnership Model appears to be the logical place to implement many of the private sector recommendations because it currently includes knowledgeable security experts who represent owners and operators from the 18 sectors. However, changes may be needed to this council to best accommodate CEO involvement and provide additional resources to support private sector activities. The Partnership for Critical Infrastructure Security (PCIS) is currently identified in the National Infrastructure Protection Plan as filling the role of the Private Sector Cross-Sector Council. The actions below outline strategies that PCIS should pursue to implement key NIAC recommendations.

1. Empower the Private Sector Cross-Sector Council to be a more proactive and strategic private sector body, able to engage and leverage CEO-level involvement and support as needed.

- Adopt a scalable engagement model that establishes a group of senior critical infrastructure executives to engage with and support PCIS.
- Build on PCIS's sector expertise and capabilities to guide cross-sector studies, training and exercises with government partners
- Increase state, local, and regional outreach and integration into the critical infrastructure protection partnership.
- Investigate options for establishing a permanent staff for PCIS using private-sector funds, possibly with volunteer appointments from sector companies.
- Encourage mentoring of developing sector partnerships and create a transition strategy to bring all sectors up to the same level of commitment and engagement.

The NIAC Study Group found that strong partnerships consistently had common characteristics that contributed to their success. Of the organizations reviewed by the Study Group, such as Business Executives for National Security, the Financial Services Roundtable, and the Business Roundtable, all have senior executive engagement, typically at the CEO level, as well as permanent staffs. Effective executive engagement gives the organizations an important perspective and the permanent staff enables the organization to carry out its mission.

The PCIS has notable strengths, including a committed membership, a strong value proposition in many sectors, and a good deal of flexibility. It also has an effective administrative staff in the

DHS-provided secretariat. However, the NIAC believes that PCIS could be strengthened with stronger CEO/senior executive engagement and a permanent staff, funded by the private sector that would include duties beyond the current secretariat staff activities.

CEO/Senior Executive engagement

A PCIS advisory body of senior industry executives from diverse sectors will provide the support and additional perspective needed to strengthen the sectors' abilities to establish priorities and commit resources to meet infrastructure challenges. The direct participation of the group should be modest, perhaps a quarterly phone call and a half-day meeting on an annual basis. These meetings will enable the advisory body to provide input and their perspective to PCIS on critical infrastructure protection priorities, including cross-sector interdependencies, as well as to provide their support to the PCIS. This group should be established with members drawn from several of the most highly active and engaged sectors, with the expectation that it will grow to include CEO/senior executives from all sectors over time.

The advisory body's engagement should be scalable, increasing its involvement in response to an increased threat level or if an event occurs. This group of CEOs will be able to use their relationship with PCIS to better understand the threat, provide support to PCIS if needed, and use the relationships they develop with other industry executives and senior government officials to provide additional support of company and/or industry resources. The group will also be engaged for significant policy issues.

PCIS Permanent Staff

Another important feature of successful partnerships is having adequate resources to accomplish the mission. In successful partnerships, both public and private partners each have dedicated resources and staff to carry out their partnership priorities and activities. However, in the current partnership for critical infrastructure protection, only the government side of the partnership has dedicated, permanent resources; the private-sector side of the partnership relies on volunteer staff and government-provided contractor support. This has led to some private sector concerns that the public-private partnership is implementing a government-dominated agenda. A partnership that has a more balanced set of resources should lead to a healthier relationship and result in more equal participation and results that are more satisfying to both sides of the partnership. A permanent staff, funded by the private sector, would help to address this imbalance.

2. Arrange a CEO summit with the White House and with Congress in the first quarter of 2009 to solidify the sector partnership and build senior level commitment to the partnership.

Senior industry leaders should initiative this summit with their government executive counterparts. It should be well publicized and include both private- and public-sector senior executives as well the leadership of private sector organizations engaged in critical infrastructure protection**.**

3. Support the rapid integration of the incoming Administration officials, members of Congress, and staff described in Recommendation 1.

Near-term Actions for the Next Administration

The NIAC recommends that the new Presidential administration approach supporting and re-energizing the critical infrastructure protection mission and the critical infrastructure protection partnership as a priority and demonstrates its commitment to both the public and private side of the partnership through timely and very visible actions such as those outlined below.

In the first 100 days of the new Administration, the White House should implement the following actions (contained in Recommendations 1 and 2).

- The Secretary of Homeland Security should communicate to both presidential candidates prior to the November 4th election the need to address homeland security issues as a priority during the transition period following the election, and request a meeting with appropriate members of the President-elect's transition team in November 2008.
- The DHS Assistant Secretary for Infrastructure Protection should hold a follow-up meeting in December 2008 to provide a more specific briefing for appropriate members of the transition team. Private-sector partners should also participate in these briefings.
- The leader of each Sector-Specific Agency should ensure that tailored briefing materials are prepared for the President's transition team and executive appointees covering the status of their sector's infrastructure protection issues and the role of the public-private partnership.
- DHS, in collaboration with the White House, should identify incentives to promote interagency cooperation in critical infrastructure protection.
- DHS and the Sector-Specific Agencies should encourage the Sector Coordinating Councils and the Government Coordinating Councils to fully integrate appropriate business organizations and state, local, and regional security partners into the sector partnerships.

Appendix A: Summary of the Sector Partnership Model

The National Infrastructure Protection Plan (NIPP) establishes a framework for government and the private sector to collaborate on critical infrastructure and key resources (CIKR) issues. To this end, the NIPP offers a comprehensive risk management framework with defined roles and responsibilities for the Department of Homeland Security (DHS), federal Sector-Specific Agencies (SSA) and other federal, state, local, tribal, and private sector security partners. This approach is facilitated by the Critical Infrastructure Partnership Advisory Council (CIPAC), Sector Coordinating Councils (SCC), and Government Coordinating Councils (GCC).

HSPD-7

Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, provides for a central source in coordinating uniform security practices and harmonizing security programs across and within government agencies. The directive identifies 17 CIKR sectors. It directs DHS and other federal agencies to "collaborate with the private sector and continue to support sector-coordinating mechanisms: (a) to identify, prioritize, and coordinate the protection of CIKR; and (b) to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." Exercising the authority given to the Homeland Security Secretary in HSPD-7, Secretary Chertoff established the Critical Manufacturing Sector as the 18th sector in 2008.

Under HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall effort to enhance CIKR protection, including collaborative development of the NIPP. The primary organizational structure relied upon by the NIPP for this purpose is the Sector Partnership Model.

Sector Partners

DHS developed a Sector Partnership Model to facilitate an unprecedented level of cooperation throughout all levels of government, industry, and institutions for protection of CIKR. Under the Sector Partnership Model, each of the 17 sectors identified in HSPD-7 as CIKR is designated to a corresponding federal partner or SSA.

The partnership structure establishes a private SCC and a corresponding GCC for each sector. CIPAC enables SCC and GCC members to engage in intra-government and public-private cooperation and information sharing across the entire range of CIKR activities.

Partner Roles and Responsibilities

Federal. According to HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall effort to enhance CIKR protection. SSAs work with DHS to implement the NIPP Sector Partnership Model, develop protective programs and related requirements, provide sector-level CIKR protection guidance, and encourage sharing of security-related information, when appropriate, among private entities within the sector and between the public and private sectors. Additionally, SSAs collaborate with security partners to develop Sector-Specific Plans (SSPs)

and sector-level performance feedback to DHS for cross-sector gap analysis assessments. DHS serves as the SSA for 11 of the 18 CIKR sectors[3].

Sector-Specific Agencies

Sector	Sector-Specific Agency (SSA)
Agriculture & Food	Departments of Agriculture, Health and Human Services and the Food and Drug Administration
Banking and Finance	Department of the Treasury
Chemical	Department of Homeland Security, Infrastructure Protection
Commercial Facilities	Department of Homeland Security, Infrastructure Protection
Communications	Department of Homeland Security, Cyber Security and Communications
Critical Manufacturing	Department of Homeland Security, Infrastructure Protection
Dams	Department of Homeland Security, Infrastructure Protection
Defense Industrial Base	Department of Defense
Drinking Water & Water Treatment Systems	Environmental Protection Agency
Energy	Department of Energy
Emergency Services	Department of Homeland Security, Infrastructure Protection
Government Facilities	Department of Homeland Security, Immigration and Customs Enforcement and the Federal Protective Service
Information Technology	Department of Homeland Security, Cyber Security and Communications
National Monuments and Icons	Department of the Interior
Nuclear Reactors, Materials, and Waste	Department of Homeland Security, Infrastructure Protection
Postal and Shipping	Department of Homeland Security, Transportation Security Administration
Public Health & Healthcare	Department of Health and Human Services
Transportation Systems	Department of Homeland Security, Transportation Security Administration and the U.S. Coast Guard

State. As outlined in the NIPP, states are primarily responsible for developing and implementing statewide/regional CIKR protection programs. To effectively implement these programs, states should establish security partnerships, facilitate coordinated information sharing, coordinate regional and local efforts with the private sector, and cut across all sectors present within the state to support national, state, and local priorities.

Local. Local entities provide critical public services in conjunction with private sector owners and operators, and thus they drive emergency preparedness and local participation in NIPP and SSP implementation. As a NIPP partner, local governments:

- Facilitate the exchange of information among and between public and private entities
- Apply documented lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents to CIKR protection
- Act as a focal point for protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens

[3] In 2008, Critical Manufacturing was added as an 18th sector

Examples of Successful State, Regional, and Local Partnership Efforts

ChicagoFIRST

In 2003, Chicago's leading financial services institutions came together to form ChicagoFIRST, a not-for-profit association dedicated to addressing homeland security and emergency management issues requiring a coordinated response. Since its foundation, ChicagoFIRST has worked to enhance the resiliency of the Chicago financial community by building and maintaining relationships with government at all levels in order to better understand successful approaches to various crises, including evacuations, sheltering in place, and credentialing. Under the leadership of Executive Director Brian Tishuk, ChicagoFIRST has obtained support from the City of Chicago's Office of Emergency Management and Communications, the Illinois Terrorism Task Force, and the U.S. Department of Treasury. Mr. Tishuk has also played a leading role in helping to establish similar organizations across the country. Some 12 other regional partnerships have formed using the basic ChicagoFIRST model.

State, Local, Tribal, and Territorial Government Coordinating Council

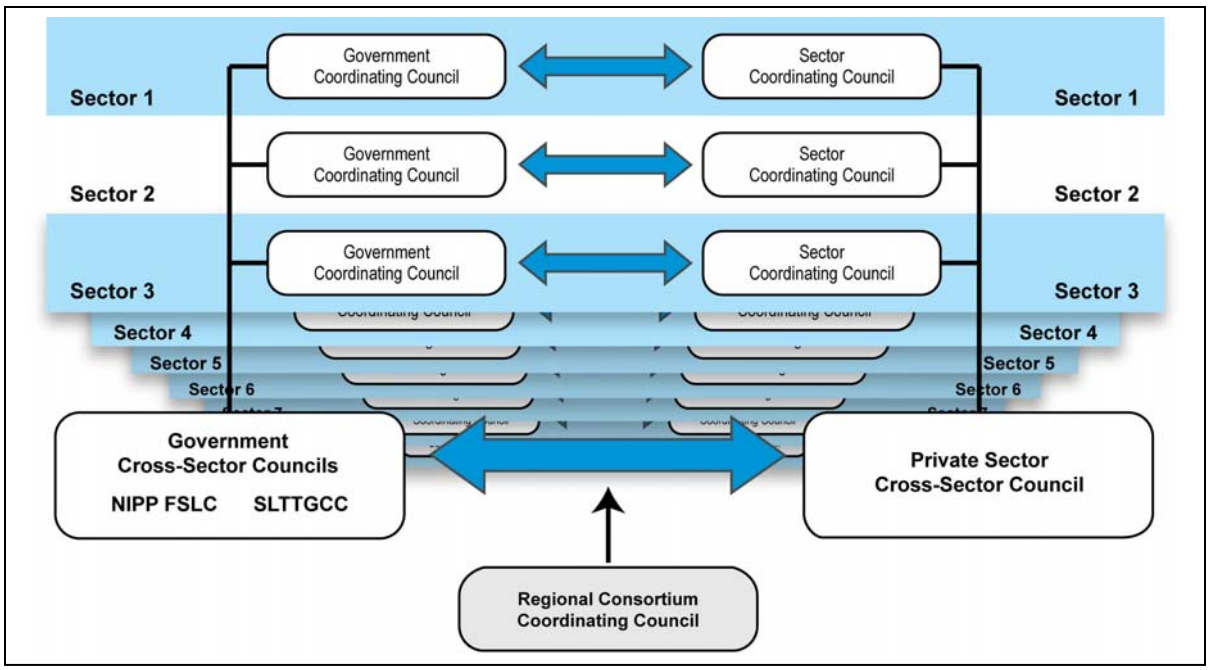
The Department of Homeland Security established the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) in order to bring together CIKR protection experts from the private sector and all levels of government. SLTTGCC functions as a forum for state, local, tribal, and territorial government representatives to engage with the Federal government and the CIKR owners and operators within the sector partnership framework, to achieve the homeland security mission of protecting the nation's critical infrastructure. Michael McDaniel, Homeland Security Advisor and Assistant Adjutant General for Homeland Security for the State of Michigan, serves as the current chair of the SLTTGCC. Under McDaniel's leadership the SLTTGCC has actively engaged all 50 states, coordinating outreach efforts, information sharing and more.

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative organization with participation from all 50 states, the District of Columbia, local governments and U.S. Territories. The mission of the MS-ISAC, consistent with the objectives of the National Strategy to Secure Cyberspace, is to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. It provides a central resource for gathering information on cyber threats to critical infrastructure and provides for two-way sharing of information between the states and local government.

Regional. Regional security partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Regional partners collaborate to implement NIPP-related CIKR risk assessment and protection activities, promote education and awareness of CIKR protection efforts occurring within their region, and coordinate regional exercise and training programs.

Private Sector. Private-sector owners and operators are responsible for supporting risk-management planning and investments in security as a necessary component of prudent business planning and operations. The CIKR protection responsibilities of specific owners and operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private-sector security operations within the sector; however, most sectors are guided by voluntary security regimes or adherence to industry-promoted best practices. Fortifying CIKR security within this diverse sector requires implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented; developing and



coordinating CIKR protective and emergency response actions, plans, and programs with appropriate federal, state, and local governments; and participating in the NIPP Sector Partnership Model including SCCs and information-sharing mechanisms, among others.

Sector Coordinating Councils

SCCs are self-organized, representative bodies that include a broad range inclusive of owners, operators, and trade associations within a particular sector. They are tasked with coordinating sector-wide activities and initiatives focused on improving homeland security and critical infrastructure protection. While DHS prefers that each SCC be chaired by an owner and/or operator, it is the responsibility of each SCC to establish the criteria for membership, governance structure, business case, and work process for that body.

According to the NIPP, SCCs are also a primary point of entry into their respective sectors, providing a communication and coordination channel between the sector and DHS, the SSAs, and the GCCs. This range of coordination is designed to facilitate:

- National planning on protection and resiliency
- Identification and prioritization of sector risk-management activities
- Information sharing related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and effective security practices
- Collaboration among and between public- and private-sector CIKR security partners on strategic communication, coordination, and procedures during response and recovery activities.

Cross-sector issues and interdependencies between the SCCs are addressed through a Private Sector Cross-Sector Council, such as the Partnership for Critical Infrastructure Security (PCIS).

The PCIS provides senior-level strategic coordination through partnership with DHS and the SSAs.

Government Coordinating Councils

GCCs serve as a counterpart to the SCC for each CIKR sector. They bring together diverse federal, state, local, and tribal interests to identify and develop collaborative strategies for the advancement of CIKR protection. GCCs support the efforts of SCCs to plan, implement, and execute sector-wide security initiatives, leveraging complementary resources within government and between CIKR owners and operators to enhance sector security.

According to the NIPP, GCCs further CIKR sector security by supporting:

- Interagency coordination for CIKR strategies, programs, initiatives, activities, policies, and communications
- SCC planning, implementation, and execution of sector-wide security initiatives
- Identification of gaps in plans, programs, policies, procedures, and strategies
- Forums with the private sector to develop, implement, and maintain SSPs and programs
- Information sharing and coordination during events of national emergency or significance and augmentation of existing emergency operation channels within federal, state, local, territorial, and tribal governments and with industry

Cross-sector issues and interdependencies between the GCCs are addressed through the Government Cross-Sector Council and its two subcouncils. The NIPP Federal Senior Leadership Council (FSLC) drives enhanced communications and coordination between and among federal departments and agencies with a role in implementing the NIPP and HSPD-7. The State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) provides an organizational structure to coordinate across jurisdictions on state and local levels.

Critical Infrastructure Partnership Advisory Council (CIPAC)

CIPAC is a non-decisional body, tasked with determining national priorities and resource requirements for the protection of CIKR against threats, as well as providing recommendations to DHS, SSAs, and other federal departments directly related to the critical infrastructure areas outlined in HSPD-7.

CIPAC provides a forum for government and private sector security partners to engage in a wide range of activities including: planning, coordination, implementation, and operational issues; implementation of security programs; operational activities related to CIKR protection including incident response, recovery, and reconstitution; and development and support of national plans, including the NIPP and Sector-Specific Plans.

Due to the sensitive nature of CIKR, it is necessary for owners and operators to, in confidence, share information and advice regarding threats, vulnerabilities, protective measures, and lessons learned. CIPAC serves as the legal framework by which members of the SCCs and GCCs engage

in joint CIKR protection-related activities. CIPAC, which has been exempted from the requirements of the Federal Advisory Committee Act (FACA), is designed to allow meaningful dialogue on CIKR protection issues while facilitating mutual action between government entities and owners and operators.

Another component of CIPAC is Joint Sector Committees, which are composed of eligible SCC members from each sector and GCC members. Eligible SCC members include CIKR owners and operators and members of representative trade associations. Eligible GCC members include government representatives from federal, state, local, territorial, and tribal government agencies (or their representative bodies). CIPAC also includes a joint cross-sector committee that consists of designated private sector and agency leads from each joint sector committee.

Appendix B: Summary of Previous NIAC Recommendations on Partnerships

The NIAC Study Group reviewed the recommendations related to the public-private partnership contained in previous NIAC studies and their respective letters of transmittal to the President. This review provided a useful foundation for developing our current recommendations. This appendix summarizes key recommendations from five previous studies:

- *Sector Partnership Model Implementation* (October 11, 2005)
- *Risk Management Approaches to Protection* (October 11, 2005)
- *Workforce Preparation, Education and Research* (April 11, 2006)
- *Public-Private Sector Intelligence Coordination* (July 11, 2006)
- *Convergence of Physical and Cyber Technologies and Related Security Management Challenges* (January 16, 2007)

Sector Partnership Model Implementation

The Sector Partnership Model was based in part on NIAC recommendations dating back to April 2003. The model was formalized in the Interim National Infrastructure Protection Plan in February 2005, and shortly thereafter DHS asked the NIAC to assess the validity of the model and to make any recommendations it thought appropriate. The report firmly supports the model, concluding that "the public-private partnership is vital to the protection of our nation's critical infrastructure as well as the ability of the United States to respond to disasters." The NIAC cautions, however, that "a true partnership is possible only if we establish the sovereignty and equality of all stakeholders."

Key recommendations from this study include:

- **Government should implement the Sector Partnership Model immediately.** Stakeholders should develop a true partnership based on the principle of collaboration of equals in which all partners bring value: "For implementation of the model to be effective, public and private sector stakeholders must have adequate and legitimate opportunities for meaningful participation."

- **Partners should work together to clearly define the roles and responsibilities of the Sector Partnership Model.** "Each partner, as an independent organizational entity, has sovereignty of its own and brings unique capabilities to the table. The model generates true value when all partners work together effectively and efficiently. The partnership needs to be rooted in robust collaboration between government and the sectors as well as between the sectors."

- **The Sector Coordinating Councils (SCC) and the Private Sector Cross-Sector Council should be given certain privileges.** "All SCCs and the Private Sector Cross-Sector Council should be self-organized, recognized as advisory committees on critical infrastructure protection and response/recovery matters, and be exempted from all requirements of the FACA [Federal Advisory Committee Act]."

- **DHS and the Sector-Specific Agencies (SSA) must embrace the role of owners and operators in protecting critical infrastructure.** "Given that the private sector owns 85 percent of the critical infrastructure, DHS and other Sector Specific Agencies must embrace the integral role of the owners and operators in this critical endeavor to protect our nation's critical infrastructure and meet the challenges of large-scale disaster preparation, response and recovery….The sobering scope and widespread impact of Hurricanes Katrina and Rita among multiple sectors demonstrate the need for joint action and fully integrated partnerships….[A] more capable national protection and preparedness enterprise can be firmly established through the Sector Partnership Model."

Risk Management Approaches to Protection

Risk management is a complex endeavor and expansion of its use in government will not be achieved without recalibrations, lessons learned and continuous improvement. The Risk Management report emphasizes that government should look to the private sector for guidance on this task because of its long-standing and matured processes in risk management. It also asserts that government can learn from the private sector and the private sector is willing to cooperate with government to help it become more efficient.

Key recommendations from this study include:

- **Government should establish risk-management leadership functions within all federal agencies.** This will provide greater focus and accountability at senior levels of government and will help to drive risk-management structure and practice throughout government. To achieve this, cabinet-level departments should establish a Chief Risk Officer (CRO), a common element of successful risk management in the private sector.
- **Government should establish oversight structure similar to the private sector's.** In the private sector, risk management is most effective when corporate governance structures oversee the process in order to ensure accountability, promote standards, and prioritize resources against threats and vulnerabilities. Government would benefit from establishing similar risk management accountability and oversight structures.

Workforce Preparation, Education and Research

The key recommendation from this study is:

- **Government should designate a privately administered, public-private Information Assurance (IA) training certification body.** This organization would standardize IA position descriptions, including required and recommended Knowledge, Skills, and Abilities (KSAs) for government jobs and review and reform IA testing procedures. A partnership between government, industry, and educators is needed to train a workforce capable of servicing the nation's critical infrastructure and cyber security and ensure U.S. competitiveness in the global marketplace.

Public-Private Sector Intelligence Coordination

Key recommendations from this study include:

- **Government should engage critical infrastructure CEOs in the intelligence-sharing process.** The government should develop a voluntary executive-level information sharing process between critical infrastructure CEOs and senior intelligence officers. This process will begin with a pilot program of volunteer chief executives of one sector and later expand to all sectors. The Attorney General should then publish a best-practices guide for employers to clarify legal issues surrounding the apparent conflict between privacy and counter-terrorism laws involving employees and to clarify the limits of private sector cooperation with the intelligence community.
- **Government should resolve private sector concerns over the legality of cooperating with the Intelligence Community (IC).**
- **Government should utilize the existing Sector Partnership Model to improve information flow between the IC and critical infrastructure.** By building on the existing partnership model, government can leverage information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector.
- **Government should improve the IC staff's understanding of the sectors.** Creating sector specialist positions, made up of civil servants at the executive and operational levels, can develop a deep understanding of government's private sector partners. The NIAC recommended that government create an ongoing training and career development program for sector specialists within intelligence agencies, and develop a formal and objectively manageable homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored to a specific sector.

Convergence of Physical and Cyber Technologies and Related Security Management Challenges

Conducted by NIAC in 2007, this study examined infrastructure risks associated with the increased use of cyber control systems to operate physical processes. As a result of this investigation, the report contains recommendations to improve the public-private partnership in the area of cyber security for critical infrastructure systems. This includes a framework and approach for improving executive leadership awareness of the cyber threat to critical infrastructure control systems, which is critical to achieving all action for needed control systems cyber security.

Key recommendations from this study include:

- **Executive leadership should work to improve their understanding and communication of information on threats, incidents, and vulnerabilities.** Properly informed executive decisions by infrastructure protection partners in the public and private sectors are dependent on clear understanding and communication of threats, incidents, and vulnerabilities. The NIAC recommended improvements in government leadership priorities for strategic planning and coordination. DHS and the SSAs, in coordination with the national laboratories, are working to develop cyber security

solutions for these systems, but strategic planning and coordination could benefit from higher-level agency coordination and private-sector feedback in the funding prioritization process

- **A sector-specific approach is needed to develop and support the appropriate market conditions to develop control systems cyber security technologies and products.** The control systems market is distinctly different from the IT market, and it is in the early stages of a transition toward developing the needed market drivers for cyber security solutions.

Appendix C: Accomplishments and Successes of the Sector Partnership

The following is a series of examples illustrating tangible accomplishments of the sector partnership. While the list is not an exhaustive recitation of each and every success, it does serve to shed light on the significant progress made by the sector partners in accomplishing the infrastructure protection mission.

- The Financial Services Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) cosponsored a three-week pandemic flu tabletop exercise for the banking and finance sector in September 2007. More than 2,700 U.S. financial services organizations participated in the voluntary exercise, which simulated a severe global pandemic flu. This exercise provided valuable insights to both government and private partners that resulted in improved preparedness for pandemic influenza.

- The Nuclear SCC partnered with the Department of Homeland Security (DHS) to pilot the Comprehensive Review of Critical Infrastructure, which assesses potential physical vulnerabilities at the nation's nuclear power plants. By 2007, all of the nation's commercial nuclear power plants had received this security review by a multi-federal agency team working with the owner-operators of the nuclear plants and with local and state agencies. Their findings provided valuable insights on how to further improve the security of some of the best-defended facilities in the United States. The Comprehensive Review has been broadened to other sectors and $25 million in grants have been provided to state and local law enforcement agencies.

- The Department of Energy (DOE), working in partnership with energy sector owners, operators, and vendors, has improved the cyber security of today's energy control systems while anticipating the needs of tomorrow. The DOE's National SCADA Test Bed (NSTB) conducted cyber security tests of sensitive control systems used throughout the energy sector to manage the flows of electricity, oil, and natural gas. When NSTB found security flaws, they notified system vendors who corrected deficiencies and provided patches to the energy system owners. The vendors also used these results to "harden" their next-generation systems. So far, 38 utilities have downloaded the security patches and several major utilities have purchased and installed the improved next-generation systems.

- DOE and DHS have trained more than 1,700 energy operators and stakeholders on how to improve cyber security of commercial control systems. The training sessions teach operators about potential vulnerabilities of specific systems and inform them about practices to help address those vulnerabilities. As a result, operators are better prepared to recognize cyber security problems and implement best practices for sustainable control systems security.

- DHS and the Idaho National Laboratory identified a potentially serious cyber vulnerability affecting critical assets in certain critical sectors. After a series of tests, a mitigation was developed. DHS quickly and efficiently engaged key SCCs to encourage owners and operators to implement the mitigation before sensitive details could be publicized. The resulting security fix has now been fully implemented throughout the nuclear sector, as well as in other sectors, thereby protecting these devices from a potential cyber threat.

- DHS launched the Technical Resource for Incident Prevention (TRIPwire) to provide a collaborative, information-sharing network for bomb squad, law enforcement, and emergency services personnel. Since its establishment in 2006, TRIPwire has grown to more than 5,000 users, including 1,000 certified bomb technicians who represent 45 federal departments and agencies, 36 military units, 750 state and local agencies, and more than 75 private-sector organizations. The TRIPwire Community Gateway, a new web portal, now provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent IED incidents in critical infrastructure sectors.

- In an effort to reduce the all-hazards risk, Protective Security Advisors (PSAs) have established over 20,000 relationships with federal, state, local, territorial, tribal, and private-sector stakeholders. They have provided support to over 2,059 buffer zone plans (BZP) and approximately $240 million dollars in funding across the 18 sectors in 50 states and 5 U.S. territories through the Buffer Zone Protection Program (BZPP). PSAs have supported more than 516 site assistance visits, 61 nuclear comprehensive reviews (CRs), and 6 chemical CRs, and have conducted 584 Enhanced Critical Infrastructure Protection Initiative (ECIP) visits. During contingencies and domestic incidents, PSAs have supported principal federal officials and federal coordinating officers through their work at state and local emergency operations centers, where they have served as the infrastructure liaison and have provided support and expertise to the infrastructure liaison cell. Most recently, PSAs helped speed recovery efforts in the aftermath of Hurricane Gustav by coordinating with law enforcement and emergency management officials to allow owner/operators access to priority assets in the Chemical Sector.

- Multiple sectors have addressed threats, incidents, and vulnerabilities by working with the Partnership for Critical Infrastructure Security (PCIS) and DHS to form Information and Sharing and Analysis Centers (ISACs). ISACs play a key role in developing operational business continuity plans and disaster-response protocols for each sector. During events of national significance, the ISACs work closely with DHS's National Infrastructure Coordinating Center (NICC) and their respective Sector-Specific Agencies (SSAs) to obtain ground truth information that helps DHS determine the cross-sector impact of these events. This process was first utilized in the course of Hurricane Katrina, practiced during the NLE02-08 exercise, and executed successfully during the 2008 hurricane season.

- Protection and resilience in the Banking and Finance Sector has been enhanced through the establishment of regional Financial Industry Resilience through Security and Teamwork or "FIRST" organizations. These private sector groups, including ChicagoFIRST and over a dozen similar organizations, are comprised of major financial institutions serving a mission to increase the resilience of the financial community in their respective geographic areas. FIRST organizations address business continuity and homeland security issues requiring a common or coordinated response. They coordinate regularly with local, regional, and federal agencies, helping to build trusted relationships which will later allow them to move "beyond the yellow tape" in an emergency and provide timely expert assistance to first responders. During a significant bank fire in the Chicago area, the public-private relationships established by ChicagoFIRST enabled bank employees to provide critical information to first responders, which assisted the emergency response to the event. ChicagoFIRST also established the

Regional Partnership Council, or "RPCfirst," to foster collaboration among the FIRST coalitions. The mission of RPCfirst is to share best practices regarding the building of relationships with the public sector, the development of credentialing programs, how to obtain seats in emergency operations centers, and the promotion of effective and efficient information sharing before, during, and after an event.

- PCIS created the Cross-Sector Cyber Security Working Group (CSCSWG), co-chaired by PCIS and the Cyber Security and Communications Assistant Secretary for DHS. CSCSWG serves as a forum to bring government and the private sector together to address common cyber security elements across the 18 critical infrastructure and key resource sectors. The CSCSWG is a mechanism for the exchange of information on common cyber security challenges and issues, as it enhances the understanding of dependencies and interdependencies through regular and active participation from all sectors and more than 90 CSCSWG members. Through its monthly meetings, the CSCSWG provides a "one-stop-shop" for updates on cyber security activities such as the Process Control Systems Forum, Software Assurance Forum, and the ISAC Council.

- The Multi-State Information Sharing and Analysis Center (MS-ISAC) was designed as an essential central resource for gathering information on cyber threats to critical infrastructure from the states and facilitating two-way sharing of this information between and among the states and with local governments. It is a collaborative organization that is consistent with the objectives of the National Strategy to Secure Cyberspace, and it includes participants from all 50 states, the District of Columbia, local governments, and U.S. territories.

- PCIS developed a simulation cell that served as a liaison with private sector experts and delivered advice and insights to enhance response and recovery during the Top Officials 4 (TOPOFF 4) exercise. The TOPOFF exercises, mandated by Congress, offer opportunities to integrate the private and public sectors for coordinated response and recovery during a terrorist attack. Preparation for the most recent exercise, TOPOFF 4, was preceded by several months of active engagement by private sector representatives from PCIS.

- The Dams Sector partnership publications have allowed government and the Dams Sector to introduce security and protection practices and methods to the 10,000+ small dam operators across the country. They include the Dam Sector Security Awareness Guide, Dams Sector Crisis Management Handbook, and Dams Sector Protective Measures Handbook.

- The Financial Services Information Sharing and Analysis Center (FS-ISAC) has been successful in addressing Bank and Finance Sector concerns about physical and cyber security threats, vulnerabilities, and incidents. Since its formation in 1999, the FS-ISAC has grown to its current membership of over 4,300 banks, credit unions, securities firms, and insurance companies. The FS-ISAC led industry efforts to implement mitigation strategies around cyber attacks, including "spear phishing" account theft, "pump and dump" securities fraud, DNS server-cache poisoning vulnerabilities, keylogging, and Chinese brute force attacks, among others. The FS-ISAC works closely with its member financial institutions and its SSA, the U.S. Department of Treasury, to address these threats. The FS-ISAC also supported the Treasury and Financial Services SCC's (FSSCC) efforts in 2007 to conduct an industry-wide pandemic flu exercise, drawing participation from over 2,700 financial institutions.

- The American Water Works Association (AWWA) has provided updated guidance on the development of business continuity plans for the Water Sector. AWWA is sponsoring a series of seminars presenting a step-by-step approach to developing the core elements of a business continuity plan for any water utility.

- Chemical Sector collaboration and feedback during the development of the Chemical Facility Anti-Terrorism Standards (CFATS) allowed DHS to create a more focused and efficient set of standards while achieving needed security in a broadly diverse sector. When fully operational, these regulations will establish a baseline for security and protection of all chemical facilities across the country.

- EPA is enhancing the security of drinking water utilities through development of a laboratory network known as the Water Laboratory Alliance (WLA). EPA will establish a nationwide network of federal, state, local, and commercial laboratories capable of analyzing drinking water for chemical, biological, and radiological contaminants resulting from terrorist attacks, other intentional acts, natural disasters, and other hazards. In the first step toward building the WLA, EPA and its partners have established regional laboratory response plans in all 10 EPA regions.

- The Chemical Sector partnership has undertaken the Security Outreach and Awareness Program (SOAP), which provides critically important information to chemical facility managers, control engineers, and IT administrators dealing with cyber-security management. Working in partnership with both the National Cyber Security Division and the private sector, the Chemical SSA was instrumental in developing this program. Its aim is to provide a review of policies and procedures regarding process control systems at medium- to small-sized facilities. A successful pilot study of SOAP was conducted in June 2008 and additional pilot visits are scheduled for fall 2008.

- The Water Sector established the Water/Wastewater Agency Response Network (WARN), which provides a method for water/wastewater utilities that have sustained damage from natural or manmade events to obtain emergency assistance in the form of personnel, equipment, materials, and other associated services from other Water Sector utilities. A total of 10 states have now established networks and plans are currently being developed to broaden this effort to include interstate mutual aid. The WARN networks were active during the Hurricane Gustav recovery.

- The Cyber Security Working Group of the Water SCC developed a unified security strategy to mitigate the risks associated with cyber systems in the form of the *Roadmap to Secure Control Systems in the Water Sector*. The Roadmap provides a 10-year broad-based plan for improving security preparedness, resilience, and response/recovery of industrial control systems.

- The web-based Chemical Security Awareness Training Program was designed to increase security awareness in chemical facilities nationwide. Based on industry best practices, this interactive program is designed to augment existing corporate security training programs. Its

goal is to reach approximately 400,000 employees directly involved in the manufacture, transportation, and storage of chemicals.

- The Water Sector participated in the Critical Foreign Dependencies Initiative, a process developed by DHS working in coordination with the U.S. Department of State. Under this initiative, the Water Sector is developing a comprehensive inventory of infrastructure located outside the United States which, if disrupted or destroyed, would lead to loss of life in the United States or critically affect the nation's economic, industrial, and/or defensive capabilities.

- The Dams Sector has produced an enhanced risk-assessment methodology for dam operators that combines the systems and asset knowledge of Dam Sector operators with government understanding and knowledge of potential threats. This jointly developed risk-assessment methodology has given dam operators a better understanding of the risks that they face, allowing them to more realistically manage their risks and make more efficient allocations of security and protection spending.

- The security of the Banking and Finance Sector has been strengthened through strong public-private interaction in developing and communicating best practices. After the attack on September 11, 2001, the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and the Securities and Exchange Commission developed the interagency whitepaper, *Sound Practices to Strengthen the Resilience of the U.S. Financial System*. The paper includes a series of sound practices that were identified by industry experts during interviews and meetings with the agencies. More than 90 comments were submitted by industry and addressed by the agencies before the writers issued the final paper. Firms that play significant roles in critical financial markets were expected to substantially achieve the implementation of the sound practices in a specified time period, and the SCC monitored and promoted progress on these efforts. Other financial sector entities implemented the practices as appropriate for their businesses.

- The Comprehensive Review Outcomes Working Network (CROWN) pilot process has been established to systematically follow up on improvement opportunities identified during Nuclear Sector Comprehensive Reviews of Critical Infrastructure (CRs). In addition to tangible improvements in security at commercial nuclear reactor sites, the process has enabled the Nuclear SSA to cultivate new working relationships with the Office of Bombing Prevention, the Office of Emergency Communications, FEMA REP, and the NIMS Integration Office.

- Physical security enhancements have been completed at the Universities of Missouri, Columbia, and Oregon State University nuclear research and test reactors. The security enhancement program originated in the Nuclear SCC and was implemented through partnership among the Nuclear Regulatory Commission, DOE, and DHS. Improvements include installing additional access doors, new alarm communication and display with CCTV recording capability, airlock door enhancements, and hardened entry gates and access points. Due to the success of these first two pilot projects, the program will be expanded to include approximately eight additional facilities in FY09.

Appendix D: References

Bush, George W. 2003. "Critical Infrastructure Identification, Prioritization, and Protection." *Homeland Security Presidential Directive/Hspd-7* (December 17). Washington, D.C.: The White House. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (accessed September 2008).

Business Response Task Force. 2007. *Getting Down to Business: An Action Plan for Public-Private Disaster Response Coordination* (January). Washington, D.C.: Business Executives for National Security. http://www.bens.org/mis_support/Getting-Down-To-Business.pdf (accessed September 2008).

Cavanagh, Thomas E. 2008. "Coordinating Business Preparedness: Managing Public and Private Efforts." *Executive Action Serie*s, no. 266 (April). New York: The Conference Board.

Cavanagh, Thomas E. 2006. *Navigating Risk: The Business Case for Security*. New York: The Conference Board.

Clinton, William J. 1998. "Critical Infrastructure Protection." *Presidential Decision Directive/NSC-63* (May 22). Washington, D.C.: The White House.

Council on Competitiveness. 2007. *The Resilient Economy: Integrating Competitiveness and Security*. Washington, D.C.: Council on Competitiveness.

Department of Homeland Security 2008, *Critical Infrastructure Key Resources Sector Partnership Ethics Guidelines.*

Flynn, Stephen E. 2008, "America the Resilient: Defying Terrorism and Mitigating Natural Disasters." *Foreign Affairs*, vol. 83, no. 2, (March/April). http://www.foreignaffairs.org/20080301faessay87201-p0/stephen-e-flynn/america-the-resilient.html (accessed September 2008)

Moteff, John D. 2008. *Critical Infrastructures: Background, Policy, and Implementation* (January 15). Washington, D.C.: Congressional Research Service. RL30153.

National Infrastructure Advisory Council. 2007. *Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group: Final Report and Recommendations by the Council* (January 16). Washington, D.C.: U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf (accessed September 2008).

National Infrastructure Advisory Council. 2006. *Public-Private Sector Intelligence Coordination Recommendations: Final Report and Recommendations by the Council* (July 11). Washington, D.C.: U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf (accessed September 2008).

National Infrastructure Advisory Council. 2006. *Workforce Preparation, Education and Research Working Group: Final Report and Recommendations by the Council* (April 11). Washington, D.C.: U.S. Department of Homeland Security.

http://www.dhs.gov/xlibrary/assets/niac/niac_workforcereport_april06.pdf (accessed September 2008).

National Infrastructure Advisory Council. 2005. *Risk Management Approaches to Protection: Final Report and Recommendations by the Council* (October 11). Washington, D.C.: U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf (accessed September 2008).

National Infrastructure Advisory Council. 2004. *Best Practices for Government to Enhance the Security of National Critical Infrastructures* (April 13). Washington, D.C.: U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf (accessed September 2008)

Silverleib, Alan. 2008. "Poll: Terrorism fears are fading" (July 2). CNN.com. http://www.cnn.com/2008/POLITICS/07/02/terrorism.poll (accessed September 2008).

Stockton, Paul N. and Patrick S. Roberts. 2008. "Findings from the Forum on Homeland Security After the Bush Administration: Next Steps in Building Unity of Effort." *Homeland Security Affairs* IV, no. 2 (June). http://www.hsaj.org/?article=4.2.4 (accessed September 2008).

United Kingdom. Controller of Her Majesty's Stationary Office. 2000. *Public Private Partnerships: The Government's Approach*. London: Her Majesty's Stationary Office. http://www.hm-treasury.gov.uk/mediastore/otherfiles/ppp2000.pdf (accessed September 2008).

U.S. Congress. House. Subcommittee on Transportation Security and Infrastructure Protections, Committee on Homeland Security. 2007. "Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Base Approach?" *Statement for the Record: Robert Stephan, Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate, Department of Homeland Security*. 110th Cong., 1st sess. (May 14).

U.S. Congress. Senate. Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs. 2007. "Sector Plans Complete and Sector Councils Evolving." *Statement for the Record: Eileen R. Larence, Director Homeland Security and Justice Issues*. 110th Cong., 1st sess. (July 12).

U.S. Congress. Senate. Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs. 2007. *Statement for the Record: Robert Stephan, Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate, Department of Homeland Security*. 110th Cong., 1st sess. (July 12).

U.S. Department of Homeland Security. 2008. "Critical Infrastructure and Key Resource Support Annex." *National Response Framework* (January): CIKR-1–CIKR-21. Washington, D.C.: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. 2008. "Private-Sector Coordination Support Annex." *National Response Framework* (January): PRV-1–PRV-12. Washington, D.C.: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan*. Washington, D.C.: U.S. Department of Homeland Security. http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm (accessed September 2008).

U.S. Department of Homeland Security. 2005. *Interim National Infrastructure Protection Plan* (February). Washington, D.C.: U.S. Department of Homeland Security. http://www.deq.state.mi.us/documents/deq-wb-wws-interim-nipp.pdf (accessed September 2008).

U.S. Department of Homeland Security Office of Inspector General. 2008. *Major Management Challenges Facing the Department of Homeland Security* (January). Washington, D.C.: U.S. Department of Homeland Security Office of Inspector General. OIG-08-11.

U.S. Government Accountability Office. 2008. *Department of Homeland Security: Progress Made in Implementation of Management and Mission Functions, but More Work Remains* (February 13). Washington, D.C.: U.S. Government Accountability Office. GAO-08-457T.

U.S. Government Accountability Office. 2007. *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve* (July 12). Washington, D.C.: U.S. Government Accountability Office. GAO-07-1075T.

U.S. Government Accountability Office. 2007. *Critical Infrastructure Protection: Sector Plan and Sector Councils Continue to Evolve* (July 10). Report to The Honorable Bennie G. Thompson and The Honorable Sheila Jackson Lee. Washington, D.C.: U.S. Government Accountability Office. GAO-07-706R.

U.S. Government Accountability Office. 2007. *Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security* (February 6). Washington, D.C.: U.S. Government Accountability Office. GAO-07-398T.

U.S. Government Accountability Office. 2007. *Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges that Require Federal and Private Sector Coordination* (October). Washington, D.C.: U.S. Government Accountability Office. GAO-08-36.

U.S. Government Accountability Office. 2006. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* (October). Washington, D.C.: U.S. Government Accountability Office. GAO-07-39.

U.S. Government Accountability Office. 2004. *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure* (July). Washington, D.C.: U.S. Government Accountability Office. GAO-04-780.

U.S. Homeland Security Council. 2007. *National Strategy for Homeland Security* (October). Washington, D.C.: The White House. http://www.whitehouse.gov/homeland/book (accessed September 2008).