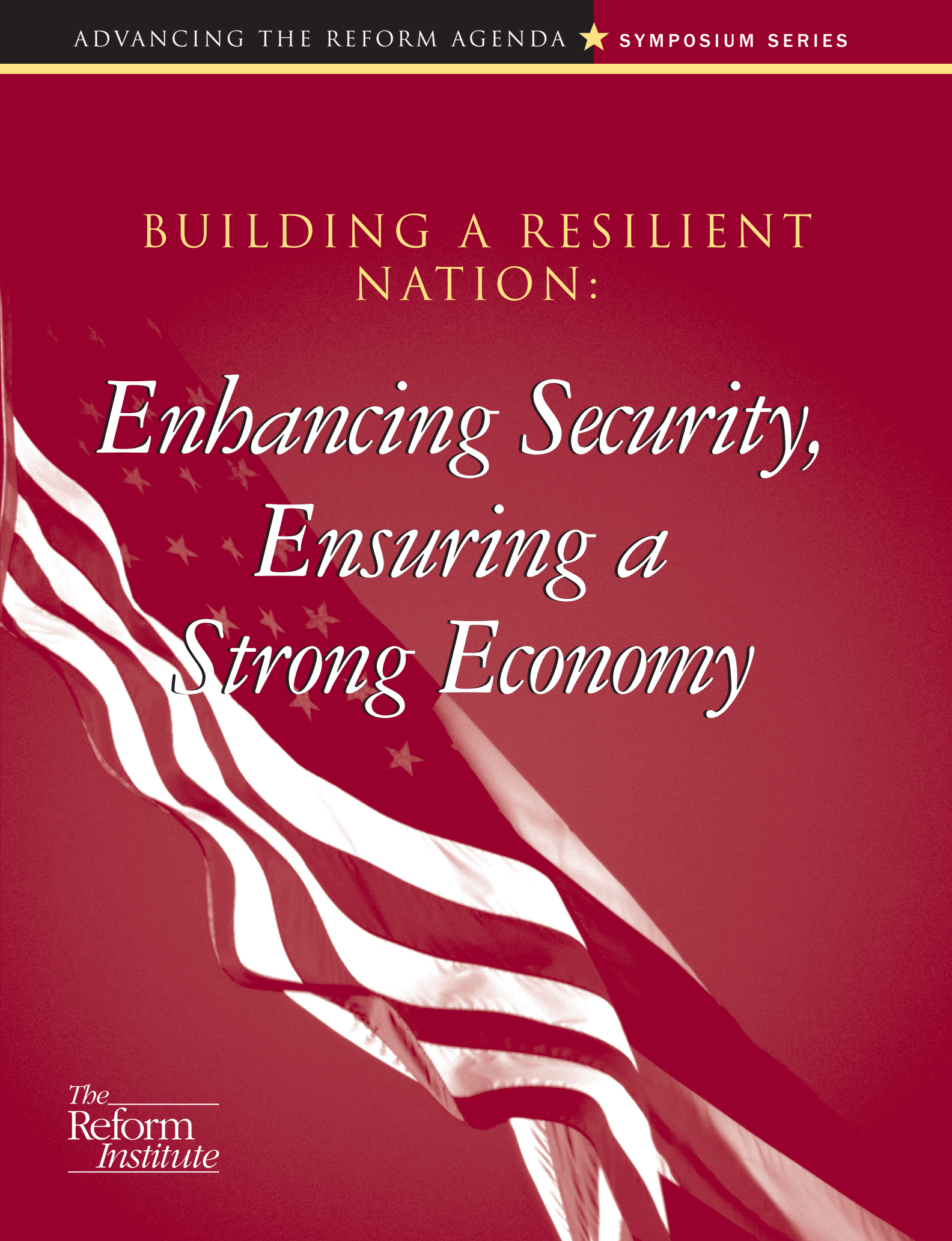
BUILDING A RESILIENT NATION:

Enhancing Security, Ensuring a Strong Economy



The Reform Institute

BUILDING A RESILIENT NATION:
ENHANCING SECURITY, ENSURING A STRONG ECONOMY

PROJECT DIRECTORS

MARK DELICH
Director of Research and Policy
Reform Institute

ROBERT W. KELLY
Managing Partner
CenTauri Solutions, LLC
Senior Advisor, Reform Institute

EDITOR
CHRIS DREIBELBIS
Communications and Economic Policy Director
Reform Institute

The *Reform* Institute
300 North Washington St, Suite 600
Alexandria, VA 22314

Tel (703) 535-6897
Fax (866) 863-5510

www.reforminstitute.org

FACILITATING A NATIONAL DIALOGUE ON RESILIENCE: A MESSAGE FROM SENIOR ADVISOR ROBERT W. KELLY

On March 27 & 28, 2008, the Reform Institute, a non-partisan, centrist think tank headquartered in the Washington, DC area hosted a two-day symposium in New York City entitled "Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy." The event, which was held in the Model Room of the historic New York Yacht Club, was funded by the McCormick Tribune Foundation of Chicago as part of the McCormick Tribune Conference Series and assembled a wide range of business leaders and leading voices on resilience. New York City was chosen as the location of the symposium for both practical and symbolic reasons.

It seems as though hardly a week goes by without a conference or meeting taking place in the Washington, DC area focused on some aspect of homeland security. The Reform Institute sought to break the mold of such affairs, which usually revolve around the various roles of government in addressing homeland security challenges. It is time for a new perspective. With some 85% of the Nation's critical infrastructure in private hands, the Reform Institute decided to highlight the role of the private sector in building resilience. The Institute also sought a fresh venue. Not only is New York City the Nation's economic capital, through its response to the attacks of September 11, 2001 it has come to embody the spirit of resilience.

The essence of resilience is the ability of the nation to withstand a catastrophic event and quickly return to a state of near normalcy. With our infrastructure and economic activity as potential targets, the business community is on the front lines of efforts to enhance our resilience. Ensuring business continuity in the event of a crisis is critical to strengthening our resilience.

Because this is still a new concept to many and implementing it will require cooperation among all segments of our society, the Reform Institute is committed to promoting a national dialogue on resilience. The symposium brought together participants with varied backgrounds to discuss their experiences in building resilience within their respective industries and to share best practices. By highlighting the innovative efforts of the private sector, we seek to identify areas for collaboration between the public and private sectors and new directions for leadership.

The Reform Institute is grateful for the generous support of the McCormick Tribune Foundation and Alcatel-Lucent, with special thanks to Ms. Marie Royce, Managing Director of Global Strategic Initiatives at Alcatel-Lucent. We also express appreciation to all the symposium's speakers and panelists. The Institute would particularly like to thank the symposium's panel moderators for their assistance in assembling and facilitating their respective panel discussions: Ms. Mary Arnold, Vice President of Government Relations, SAP America; Major General Donna Barbisch, USAR (Ret.), President of Global Deterrence Alternatives; Mr. Lawrence Hebert, Chairman Dominion Advisory Group; The Honorable Marc Spitzer, Commissioner, Federal Energy Regulatory Commission; and Mr. Grant Seiffert, President, Telecommunications Industry Association. Thanks also to Gary Gilbert of Hutchison Port Holdings for helping us to secure the New York Yacht Club as our venue.

Robert W. Kelly
Managing Partner
CenTuari Solutions, LLC
Senior Advisor, Reform Institute

ACKNOWLEDGEMENTS

From the Reform Institute—**Cecilia Martinez, Mark Delich, Chris Dreibelbis, Nichole Remmert, Kerry Buker, Pam Pryor, Sarah Wambaugh, Matt Patton**

McCormick Tribune Foundation; New York Yacht Club; Marie Royce, Managing Director, Global Strategic Initiatives, Global Government & Public Affairs, **Alcatel-Lucent**; **Suzanne Luft**, Blue Guitar Design

Symposium Advisory Committee—**Robert Kelly**, CenTauri Solutions, LLC; **Paul Bateman**, Klein & Saks Group; **Stephen Flynn**, Council on Foreign Relations; **Charles Kolb**, Committee for Economic Development

Symposium participants—**Valerie Abend**, Deputy Assistant Secretary, Critical Infrastructure Protection & Compliance Policy, U.S. Department of the Treasury; **Mary Arnold**, Vice President of Government Relations, SAP America; **Susan Bailey**, VP, Operations, Planning & Support for AT&T's Global Network Operations; Major General (Retired) **Donna Barbisch**, President, Global Deterrence Alternatives; **Paul Bates**, Vice President of Global Enterprise Solutions, Verizon; **Joseph Bruno**, Commissioner of the New York City Office of Emergency Management; **Michael Claes**, Executive Vice President/Managing Director, Burson-Marsteller; **Jack Devine**, President & Founding Partner, The Arkin Group LLC; **Thomas Von Essen**, former Fire Commissioner, New York City Fire Department; **Timothy Farrell**, Senior Vice President, Business Continuity Manager – Corporate, Bank of America; **Shaun Flynn**, Chief Risk Officer, QBE the Americas; **Stephen Flynn**, Ira Lipman Senior Fellow for Counterterrorism and National Security Studies, Council on Foreign Relations; **Gary Gilbert**, Senior Vice President of Hutchison Port Holdings; **Chris Hackett**, Vice President of Public Sector Sales Programs, Sprint; **Lawrence Hebert**, Chairman, Dominion Advisory Group; **Reynold Hoover**, Assistant Vice President for Police and Infrastructure Protection, CSX; **Shawn Johnson**, Director of Institutional Financial Services, State Street Global Advisors; **John Kneuer**, Sr. Vice President for Strategic Planning and External Affairs, Rivada Networks; **Michael Kormos**, Senior Vice President of Operations, PJM Interconnection; Colonel **Randall Larsen**, USAF (Ret), Founding Director, Institute for Homeland Security; **Phil Marie**, Senior Vice President, Infrastructure Services, The NASDAQ-OMX Group, Inc.; **Jerry Napolitano**, Solutions Architect for Public Safety Communications, Government & Public Safety, Motorola; **Ted O'Brien**, Vice President & General Manager, Americas, Iridium Satellite, LLC; **Cindy Ortega**, Senior Vice President for MGM MIRAGE Energy and Environmental Services; **Martin Padilla**, Shell Energy North America; **Karl Rauscher**, Bell Labs Fellow, and Executive Director, Bell Labs Network Reliability & Security Office, Alcatel-Lucent; **Grant Seiffert**, President, Telecommunications Industry Association; **Marc Spitzer**, Commissioner, Federal Energy Regulatory Commission; **Edward Stern**, President & CEO, Neptune RTS; **Bill Tenney**, Group Manager, International Assets Protection, Target; **Caren Wilcox**, Executive Director of the Organic Trade Association; **Leigh Williams**, President, BITS, Financial Services Roundtable

TABLE OF CONTENTS

INTRODUCTION

MAKING RESILIENCE *a National Priority*

We live in an information age where society is constantly confronted with disruptive, indeed catastrophic events that seemingly occur with more frequency and tend to affect us even when they occur in remote parts of the globe. Whether it is a tsunami in Southeast Asia, a hurricane in the U.S. Gulf Coast, terrorist attacks in New York, London and Madrid, geopolitical turmoil in Sub-Saharan Africa or a longshoreman's strike along the U.S Pacific Coast, both humans and nature wreaking havoc on people, property, institutions, states and the global economy is becoming more prevalent and more significant in our increasingly interconnected world. The circumstances dictate a new direction in security policy where governments, industry, institutions and individuals acknowledge the simple fact that catastrophic events are going to happen and work together to mitigate their effects.

Regardless of our best efforts, we cannot prevent the unpreventable. Natural disasters, industrial accidents, labor disputes and the vile acts of determined terrorist organizations represent ongoing threats that possess the potential to inflict great harm and severely damage our economy and global leadership. The simple fact is that not all these hazards can be averted. Certainly we can reduce the likelihood of terrorist attacks through the use of competent intelligence systems and reasonable security measures. Likewise we can decrease the incidence of industrial accidents and labor disputes through sound management practices. Nevertheless, devastating incidents will occur. What is within our power, however, is to better prepare our nation and its critical infrastructure to absorb the blows of catastrophes in order to prevent them from seriously disrupting critical activities and destabilizing the Nation. Adopting a national mindset of resilience[1] must be become a priority.

THE PAPER HIGHLIGHTS FOUR AREAS THAT DURING THE COURSE OF THE PROCEEDINGS IDENTIFIED THEMSELVES AS THE CRITICAL ELEMENTS OF RESILIENCE: PREPAREDNESS, PROTECTION, RESPONSE, AND RECOVERY.

Placing resilience at the heart of our homeland security policy will bring a much-needed overarching focus to the work of government agencies, particularly the U.S. Department of Homeland Security (DHS). It will also engage the populace and promote more cooperation between the public and private sectors.

Brittle units tend to shatter when confronted with catastrophic shocks while flexible and reinforced entities are poised to bounce back when subjected to the same forces. A resilient nation is one that is not overwhelmed or immobilized by a calamitous event. Resilience is about mitigating the cascading adverse effects of a terrorist attack or natural disaster so that the nation can quickly recover and resume normal activity after such an episode.

"THE VERY PROCESS OF ENGAGING ALL OF US IN MAKING RESILIENCE AN ACTIVE PRIORITY…CAN BE ONE OF THE BEST MEDICINES FOR DEALING WITH THE LEVEL OF PARTISANSHIP IN THIS COUNTRY…"

— DR. STEPHEN FLYNN
COUNCIL ON FOREIGN RELATIONS

Embracing national resilience in this age of peril has three significant benefits. It can serve to mobilize perhaps America's greatest asset – her people – through individual effort or collective action within the private and non-profit sectors. It will also strengthen our economy by reinforcing our critical infrastructure, mitigating the possibility of a severe disruption in economic activity and providing American firms with a competitive advantage. Finally, it will enhance our security – including homeland, energy and financial – by making the country less vulnerable to the continuing threat of terrorism.

Viewing Americans as assets, instead of potential victims, would revolutionize our homeland security policy and unleash the determination, spirit and ingenuity of Americans in overcoming our greatest challenges. Dr. **Stephen Flynn** of the **Council on Foreign Relations** stressed how building resilience could be a unifying endeavor in the symposium's opening keynote address, "The very process of engaging all of us in making resilience an active priority, I think, can be one of the best medicines we could have for dealing with the level of partisanship in this country and the levels of self-destructive meism that seems to be across the land."

Thanks to the efforts of advocates such as Dr. Flynn, resilience is gaining prominence on the national agenda.[2] The Homeland Security Committee of the U.S. House of Representatives proclaimed May 2008 as "Resilience Month" and held a series of hearings to examine the issue and identify reforms to bring about resilience.[3] A report released on September 11, 2008 by the Homeland Security Advisory Council, which advises the Secretary of Homeland Security, acknowledged "Lead the building of a resilient America" as one of the *Top Ten Challenges Facing The Next Secretary of Homeland Security*.[4] While the need for making America more resilient is becoming evident, there is of yet no consensus on what precisely constitutes resilience and no clear blueprint for how to achieve it. Defining the concept and developing a comprehensive resilience strategy will require a national dialogue that brings together government authorities, the private and non-profit sectors, as well as the general public in discussing what resilience means to them and how they can work together to realize it. In March of 2008 the Reform Institute brought together experts and leaders from disparate industries and government agencies to launch such a dialogue at the national symposium, "Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy."[5]

Presentations at the symposium vividly revealed the groundbreaking work already underway within the private sector towards resilience. Risk management and business continuity are critical aspects of virtually every enterprise. Firms recognize that it is imperative to their respective bottom lines to assess potential threats and to ensure their venture continues operating in the face of a crisis. This ability is critical to U.S. economic growth and international competitiveness. With some 85% of U.S. critical infrastructure is in the hands of the private sector and commercial activity the

critical lifeline of the country in the age of globalization, the U.S. economy is a potential target for terrorists. As such, the private sector has an essential role to play and many companies are already leading the way. Fostering an exchange of ideas on what has been successful and what more needs to be done is the first step to charting a course for future action.

This report is a compilation of the ideas, anecdotes, experiences, and recommendations provided by the panelists and speakers at the symposium with two goals: first, to capture the substance of the ideas shared at this event and second – and perhaps more importantly – to identify what resilience is and provide concrete examples of when the concept has been deployed into actionable steps by both the private and public sectors. The paper highlights four areas that during the course of the proceedings identified themselves as the critical elements of resilience: preparedness, protection, response, and recovery.

CHAPTER 1

PREPARING *for Resilience*

Preparation and planning are the foundation for building resilience. Communities and businesses run the risk of a much more difficult recovery process by failing to adequately plan, conduct a full risk assessment, and provide preparedness-based education to their constituents or employees. The essential need for community and business preparedness came into stark display during the 9-11 attacks and Hurricanes Katrina and Rita. While great strides have been made in improving preparedness, much more work still has to be done to promote preparedness among American families, communities and businesses. Many firms are ahead of the curve in recognizing the importance of being prepared for catastrophic events to their bottom lines and the future of their ventures. Their efforts can serve as models for governments, communities, and other companies. The experiences of locales that have dealt with crises, such as New York City, are also very informative.

The first critical aspect of preparedness involves the development of emergency and continuity planning, including the preparation of an emergency supply kit and the dissemination of information about emergency plans developed by state and local governments and employers. It is essential that such plans be tested through exercises that simulate potential scenarios. Joint exercises involving companies and government authorities are especially effective and serve to encourage valuable public-private collaboration. Secondly, it is necessary for governments and businesses to acquire a full understanding of possible risks and to undertake long-term planning towards confronting them.

New York City's preparation for the "Y2K" dilemma provides many positive lessons in how to best prepare a community for a possible event. After the Y2K problem was identified the City of New York began preparations in 1996 by spending over $350 million to test, fix, and replace the city's critical computer systems. Beginning in 1998 the city's Office of Emergency Management (OEM) developed plans to ensure that critical public safety services provided by the City of New York continued to function in any eventuality. The city government established a task force that coordinated plans with other governments in the tri-state area and opened a 24 hours-a-day command center to coordinate any potential response by working with representatives from utilities, transportation authorities, the securities and banking industry and technology vendors. Town hall events were held, a website and phone number were established and palm cards printed in multiple languages were created to educate the public on preparation for Y2K. This level of planning, coordination and education fully prepared the New York City community for a potentially

negative situation and can be used as a model for communities and businesses to prepare for threats both known and unknown.

There are many facets to preparedness. Symposium presentations highlighted crucial issues such as planning, education, cooperation and engagement at all levels.

IN ORDER TO BE PROPERLY REGARDED AND VALUED BY EMPLOYEES, CORPORATE PREPRAREDNESS PLANS MUST HAVE INPUT FROM ALL QUARTERS OF THE ORGANIZATION AND BUY-IN AT ALL LEVELS.

In providing insight from the government perspective, Commissioner **Joseph Bruno**, Commissioner of the **New York City Office of Emergency Management** (OEM), outlined how the OEM develops all types of plans including those that are hazard-specific such as strikes, power disruptions, fires, water main breaks, air traffic issues, avian flu and weather emergencies. Its emergency plans are based in the City-Wide Incident Management System (CIMs) which determines who is in charge and their related responsibilities. The OEM's Watch Command monitors everything that is happening in the city including 911, and police, fire and EMS dispatch and breaking news of every type across the city, country and the globe. Based on its assessment of what is happening, it may dispatch other agencies to the scene of an emergency.

Private initiatives can complement and inform public preparedness efforts. Underlining the importance of private firms having proper preparedness planning in place Colonel **Randy Larsen** (Ret.), Founding Director of the **Institute for Homeland Security**, discussed how Con-Way Trucking, a $6 billion company with 26,000 employees, pulled together a pandemic flu business continuity plan. Colonel Larsen stated that their aggressive plan includes the staging of 500,000 M95 masks, operations plans for periods of quarantine and HR policies for the pooling and distribution of sick leave. However, he noted that the aspect of the plan that has already proven to be most beneficial is the employee training on health etiquette (frequent hand washing and coughing on sleeve rather than hand) which company officials believe has already reduced routine sick leave. Sometimes the smallest details can have a big impact. This account demonstrates how preparedness efforts can have benefits beyond those intended.

Preparedness plans are most effective when they have been tested through exercises. Many of the participating speakers on the "Securing the Financial Markets" panel, moderated by Mr. **Lawrence Hebert**, Chairman of **Dominion Advisory Group**, expressed how important disaster planning and exercising are in the financial services sector's efforts to ensure industry-wide resiliency. Most organizations schedule quarterly tests on crisis management and go to great lengths to ensure maximum participation of senior management. Many firms have established executive response teams that are comprised of the CEO as well as all executive, senior and key vice presidents. It is not unusual for each to be furnished with multiple mobile phones from different carriers and to have both their homes and offices equipped with Internet Protocol (IP) phones to ensure maximum mobility. Some firms conduct scenario planning or similar activities as frequently as quarterly with key executives assuming responsibility for major segments.

In order to be properly regarded and valued by employees, corporate preparedness plans must have input from all quarters of the organization and buy-in at all levels. Senior executives must set the example. Mr. **Martin Padilla of Shell Energy** detailed how Shell, in the crisis management area, has adopted an incident command planning system. This guides all planning activities whether dealing with energy terminals, pipeline pump stations or multiple refineries. Shell's planning begins in the field and

permeates up to the executive leadership level, helping to develop a corporate culture. Mr. Padilla stated that ensuring that the same processes are followed at the executive leadership level facilitates better communication with the field; particularly considering the need to send additional resources in response to an isolated or widespread incident. Hurricane Katrina and its aftermath served as potent tests of Shell's systems. As a result, current crisis planning is informed by lessons learned from Katrina.

Interoperability of communications equipment is a critical component for the preparedness of first responders. Here too, planning and exercising of those plans is vital, along with developing uniform standards through public-private cooperation. Mr. **Jerry Napolitano**, Solutions Architect for Public Safety Communications at the **Motorola Corporation** argued that for the "one radio" concept of interoperability to work there are a number of underpinning requirement uniform standards that must be formulated. Where in the past standards were largely derived from the actions of equipment manufacturers, true interoperability will require the intervention of the government in identifying and codifying standards as well as requiring jurisdictions seeking grant funding to adhere to the standards as a precondition. Mr. Napolitano stated that planning and exercising are too often overlooked when addressing interoperability. As in other areas affecting readiness and response, interoperability planning and exercising must become part of the culture. He stated that greater spectrum discipline is another critical element because a coordinated response or recovery effort is not well served when the myriad players are all communicating on different radio bands and that centralized command and control is an essential requirement to true interoperability.

Just as ensuring communications is critical during a crisis, hardening the supply chain to guarantee the uninterrupted flow of goods and services is a fundamental aspect of resilience. Mr. **Reynold Hoover**, Assistant Vice President for Police and Infrastructure at **CSX Corporation**, discussed the "all hazards" approach CSX has taken to business continuity and supply chain disruption by addressing both high-likelihood sources of potential disruption such as accidents and criminal acts of vandalism and also low-likelihood disruptions such as terrorism or natural disasters. According to Mr. Hoover, CSX brings its key people together to participate in a business continuity working group that meets on a regular basis. They review and exercise continuity and succession plans to make sure that the company can respond appropriately to a variety of contingencies. CSX also partners with federal, state and local governments on a variety of issues including information sharing regarding real-time information on train location and updates on potential threats.

Knowing the risks and developing strategies for managing those risks is also crucial to preparedness and resilience. The experience and expertise of the financial industry in this area can be extremely valuable. Mr. **Shaun Flynn**, Senior Vice President and Chief Risk Office for **QBE**, the Americas, stated that currently, there is considerable pressure from state insurance regulators and from credit rating agencies on corporations to adopt credible risk management processes. He stated further that although it is a wise business practice, there are a number of obstacles, one of the main being the organizations' corporate culture. Mr. Flynn argued that for this reason it is essential that the adoption of effective risk management processes needs to start with executive management at the strategic level. The corporate management team needs to realistically address risks to the viability of the venture and to prioritize them. Insurers are particularly adept at risk analysis utilizing a variety of models including catastrophe and storm models and can serve as a valuable resource to industry. According to Mr. Flynn, once a comprehensive risk analysis has been accomplished, the next step is to determine how the entity will manage the risk. Core discussions need to take place including whether or not to accept the risk, reject it or how to

otherwise mitigate it. Risk management needs to feed into a firm's strategic planning and strategic initiatives going forward.

Engendering preparedness among the general public is perhaps the greatest challenge. Commissioner Bruno discussed how a major portion of OEM's mission is also to educate the public on emergency preparedness. This requires extensive coordination, cooperation and interaction with the private sector. In addition, Commissioner Bruno stated that his office is continually instructing people and working with the public on being prepared, "We are out there talking to people and instructing people and working with the private sector…on being prepared."

Communities and public agencies can learn a great deal from the preparedness efforts of the private sector, such as identifying and evaluating potential threats, developing and assessing comprehensive plans, educating and involving all stakeholders, and promoting cooperation at all levels. Areas for public-private partnership identified at the symposium include joint exercises for testing preparedness and continuity plans and developing industry-wide best practices for devising such plans. A common theme was the need to make preparedness an integral part of an entity's culture. This can be done through education and awareness-building and through leadership at the senior level that sets the proper example.

CHAPTER 2

PROTECTING *Against Threat*

The drive to bolster the Nation's security as a result of September 11, 2001, epitomized by the creation of the Department of Homeland Security, has been successful in making the United States more secure; most notably the absence of any major terrorist attacks on U.S. soil in the seven years since 9-11. However, the myopic focus on preventing terrorism through the traditional trilogy of guns, gates, and guards does not adequately address threats from natural or other types of disasters, as was evidenced by the government's appalling inability to effectively deal with Hurricane Katrina and its aftermath in 2005. A national strategy based on resilience encompasses all potential threats. Achieving a more resilient America requires strengthening and protecting our aging critical infrastructure, including bridges, damns, levees, communications and information technology networks, electric power grid and supply chain.

The concept of protection within resilience should not be viewed only as a responsibility of the federal government or merely a "hard" security issue. As a matter of sound strategy, businesses every day take steps to protect their employees and assets from a variety of contingencies and to prevent serious disruption to their operations. Long-term concerns such as climate change and sustaining the supply of secure and affordable energy have many businesses pursuing innovative solutions that make them more secure and resilient against outside forces.

Protecting the supply chain is critical to the function of many firms.[6] As such, the corporate sector is deeply involved in areas such as rail, port, shipping, and border security. Discussing security in freight shipping, Mr. **Bill Tenney**, Group Manager of International Assets Protection for the **Target Corporation**, reinforced the idea that in order to secure the global supply chain both public and private sectors need to be fully engaged. He cited the Customs-Trade Partnership Against Terrorism (C-TPAT) as an example and noted, although C-TPAT is a voluntary public-private partnership, for companies such as Target, Home Depot, Wal-Mart and Nike given their heavy reliance on direct imports, the program can hardly be viewed as voluntary. He argued that C-TPAT provides substantial benefits to companies like Target by reducing the amount of security inspections of inbound containers, which translates into increased speed by which goods can be delivered to market as well as reduced inspection costs. In return C-TPAT members agree to deploy enhanced security measures "upstream" in the supply chain, thus reducing the need for inspections occurring within the transit cycle. Mr. Tenney noted that although forty-five percent of all U.S. trade comes through C-TPAT partners, that means

that more than half of all companies are still not participating; a gap that must be closed. He urged taking C-TPAT to the next level – "public-private partnership 2.0" – recommending even closer collaboration on issues such as sharing threat information, setting common standards, utilizing technology, and developing an "all hazards approach" to possible threats.

RESILIENCE RECOGNIZES THAT OUR CRITICAL INFRASTRUCTURE IS THE BACKBONE OF THE NATION AND THE SUPPLY CHAIN ITS LIFEBLOOD.

On the same topic, Mr. **Gary Gilbert**, Senior Vice President, **Hutchison Port Holdings** (HPH), stressed the urgency in deploying container scanning technology. He noted that HPH terminals account for about 50% of the total U.S.-bound containers. Mr. Gilbert pointed out that HPH was involved in a test of container scanning technology at one of its ports in Hong Kong. The test, which placed radiation portal monitors and X-ray scanners at the gates of the terminal, demonstrated that containers could be effectively scanned for the presence of shielded material without slowing down the flow of containers into the terminal. Mr. Gilbert observed that since about 65% of HPH containers arrive through the terminal gate and another 35% arrive on smaller ships and barges for transshipment this is a significant improvement over the current regime. Mr. Gilbert also raised the issue that under the Container Security Initiative (CSI), which uses inherently unreliable manifest data for targeting high risk containers, less than 1% of containers are scanned at foreign ports and only those posing the "very highest risk." Other containers that are considered merely "high risk" are not scanned until they arrive at a U.S. port.

Mr. Gilbert noted that there is currently much debate taking place regarding the 100% scanning requirement imposed by recent legislation. He contended that the debate should not be centered around whether or not 100% scanning is achievable, but rather what needs to be done to increase scanning from its currently unacceptable level of less than 1% to something that will have a greater impact on the overall security of our supply chain. The real questions are, he noted, as follows: What is a realistic goal? What are the benefits beyond security? What is going to be the cost?

Mr. Hoover, discussing railway security, pointed out that the reality of the technologically capable terrorist dictates that we need to think in new and creative ways regarding how we develop continuity programs and build resilience in response to the threat. He mentioned that during the past year DHS had given some $15 million to freight railroads ostensibly for infrastructure protection, but that the funding unfortunately was limited to Class 1 railroads and was further restricted to be used only for train security and not for improvements in rail infrastructure. This point illustrates the need for government agencies to seek and accept more input from the private sector in making decisions concerning policy and funding of security programs.

In addition to the security of physical assets, protecting sensitive company data is equally imperative in the information age. Mr. **Jack Devine**, President and Founding Partner of the **Akin Group** and a former senior administrator at the Central Intelligence Agency (CIA), asserted that as important as it is to prepare for the inevitable chemical, biological and radiological threats, it is equally important to understand that there is an ongoing global explosion of the collection of economic intelligence. Every business needs to understand this threat and take measures to protect its information. He stated that businesses also should have realistic business continuity and crisis management plans and should conduct periodic audits of every aspect of their critical information. Special efforts also need to be taken in the vetting of potential employees and in training all employees to be sensitive to potential threats and to safeguard company information.

Communications and information technology networks are also key components of our critical infrastructure that require protection. Predictably, telecommunications and IT companies are out in front in securing their networks. Dr. **Susan Bailey**, Vice President of Operations, Planning and Support for **AT&T** Global Network Operations, discussed how her company ensures their infrastructure remains operational through the development of an enterprise business continuity protocol that focuses on protecting three types of assets. The first is the network itself along with the associated computer architecture, fiber optic cable and connectivity carrying customer traffic. The second type of assets are the mission-critical work centers and their associated employees. Third, the protocol focuses on protecting network management tools comprising the support systems that its employees use to interact with and the databases that they need to reference in order to manage the network. Dr. Bailey stated that the enterprise continuity protocol is based on a common approach to business impact analysis, threat analysis, risk management and mitigation. The protocol recognizes the importance of conducting exercises of disaster scenarios as a critical component in the overall approach to preparedness planning.

The electric power grid is yet another element of our critical infrastructure in which the relevant actors are intensely involved in protection and security. The panel discussion on "Securing the Energy Market," moderated by Commissioner **Marc Spitzer** of the **Federal Energy Regulatory Commission** (FERC), touched on the subject. Mr. **Michael Kormos**, Senior Vice President of Operations, **PJM Interconnection**, stated that infrastructure planning is a huge issue in building resilience and protecting against energy disruptions. PJM was widely praised for maintaining operations in its section of the grid during the Northeast blackout of 2003 while surrounding areas lost power. He credited regional planning and cooperation with utilities that resulted in a robust system able to withstand the cascading blackout. However, he was not optimistic that the PJM system could withstand such an event today, given that increasing demand coupled with slow growth in generating capacity are stressing the system, thereby diminishing the flexibility and resiliency in the grid.

As houses grow bigger and consumers purchase and use greater numbers of energy consuming appliances and devices the load on electrical systems continues to grow. At the same time he pointed out that in the major metropolitan areas where the increase in demand has been the greatest there has been no increase in generation capability. According to Mr. Kormos, to plan and install a major transmission line takes about five years, to build a power generation plant takes five to ten years and the planning-to-operations horizon for a nuclear power plant is much longer still. The dichotomy that the nation finds itself in is that while consumers continue to engage in behavior that requires more generation capability most are loath to find a transmission line, generating plant or certainly a nuclear power plant located near where they live. His presentation served as a warning that the U.S. needs a comprehensive energy strategy that involves grid modernization and that deals with American's NIMBY (Not in My Back Yard) issues. Mr. Kormos sees the next-generation "smart grid"[7] as the right direction, but great care has to be taken in protecting the advanced communications and automation capabilities of the smart grid from cyber attack.

Many large-scale consumers of energy, motivated by skyrocketing energy bills that threaten their profitability and competitiveness, are taking substantive steps to improve conservation and efficiency, which also reduces stress on the grid and shields these ventures from some of the most devastating consequences of power outages. Ms. **Cindy Ortega**, Vice President, **MGM MIRAGE** Energy and Environmental Services, described how big businesses have the ability to not only transform markets but also to change behavior; particularly that of consum-

ers. In its development of City Center, the largest privately-funded construction project ever undertaken in North America, MGM MIRAGE is devoted to using only the best practices and compliance with the certification system established by the U.S. Green Building Council. More than 60% of the U.S. electricity capacity is consumed by residential and office buildings. The six large high-rise buildings sited on City Center's sixty acres will be among the most energy efficient and environmentally responsible in the world and will hopefully serve as a model for developers within the United States and around the world to adopt.

Resilience recognizes that our critical infrastructure is the backbone of the Nation and the supply chain its lifeblood. Modernizing the aging infrastructure and hardening the vulnerable supply chain will prevent severe disruptions to vital social and economic activity that could result from a catastrophic event and protect against terrorist attacks by making these entities less attractive targets. Because they are so reliant on infrastructure and the supply chain, businesses are active in protecting and reinforcing them. Employers also have a prime responsibility in protecting their employees, assets and operations in an increasingly hostile and uncertain world. Robust public-private collaboration is essential in order to optimize results and ensure that government and private security efforts are complementary.

CHAPTER 3

RESPONDING *to Crisis*

Preparedness and protection involve actions prior to a negative event taking place. Equally as important to building resilience is what immediately happens following an event as widespread as a natural disaster or one that is localized to a community or business.

The ability to quickly respond is essential to mitigate long-term negative effects of a disaster. The events following Hurricane Katrina in New Orleans demonstrate how insufficiently responding to crisis not only amplifies the difficulties faced, but can also diminish any confidence in the leadership of our elected officials. The lack of coordination and planning that led to the inadequate response on the part of federal, state and local governments after the hurricane is a catalyst for renewed efforts to improve how our Nation responds to catastrophic events.

A key element to response is communications, both internal and external. First responders must be able to communicate with each other; government authorities must communicate with the general public, as well as with businesses and other organizations in order to coordinate activities; and all these actors must communicate internally. Mr. **John Kneuer**, Senior Vice President for Strategic Planning and External Affairs at **Rivada Networks** and former Administrator of the National Telecommunications and Information Administration (NTIA), highlighted the pivotal role of telecommunications in building a resilient nation, "communications is the underpinning of any concept of resilience." He noted that in responding, reacting, recovering or rebuilding from a catastrophic event, robust and reliable communications are an absolute necessity. He credited the diversity of communications channels, such as cell phones, land lines, broadband, and satellite – all enabled by competition – in creating a robust and redundant communications infrastructure. The ability to access critical information across a broad spectrum – whether in a pre-incident or post-incident environment – is critical to resilience.

In that vein, Mr. **Ted O'Brien**, Vice President and General Manager, Americas, **Iridium Satellite**, discussed how Iridium and similar systems are well-suited in providing immediate, real-time, two-way voice communications services to first responders anywhere in the world. He stated that they are particularly valuable in those areas where a catastrophic event may have partially or completely taken out the existing terrestrial-based communications services. He remarked that the challenge is in doing a better job as an industry in educating first responders about what systems are best for each circumstance. Since many first responders are unfamiliar with systems such as Iridium they rarely have Iridium units in place prior to a catastrophic event. Mr. O'Brien argued that the obvious problem is that once a cata-

strophic event takes place, degraded transportation infrastructure often makes it difficult, if not impossible, to get handsets delivered to the people that need them. This was a lesson of Katrina, where there was no pre-positioning of equipment.

A COMMON THEME AMONG THE SYMPOSIUM'S SPEAKERS WAS THE IMPORTANCE OF FIRST RESPONDERS AND THE CRUCIAL ROLE OF LOCAL COMMUNITIES.

A common theme among the symposium's speakers was the importance of first responders and the crucial role of local communities. Discussing how some small communities respond during a crisis Colonel Larsen told the story of the sheriff of Grimes County, Texas who when asked what he does in the event of a crisis (given that he only had nine deputies) responded "Son, you just posse up." He stated, for example, when Hurricane Rita sent 400,000 ill-prepared evacuees through Grimes County, the sheriff made a deal with Texas Sheriff's Association, who coordinated the supplying of extra officers from other counties. He also called in his reserve officers and was able to pick up sixty-three sworn officers from the Fish and Wildlife Commission. Delaware and other states employ this concept on a broader scale. They have created state militias and recruited physicians, nurses, and EMTs to respond in emergencies. Colonel Larsen cited a number of other instances where communities and businesses have managed to "posse up" to handle contingencies. The point was driven home that responding to catastrophic events, particularly initially, will rest on individuals and communities. Corporate America has an important role within this context.

To highlight how proper planning and response can build resilience into a community and company Ms. **Caren Wilcox** discussed her time working for the **Hershey Corporation** during the Three Mile Island incident in 1979. According to Ms. Wilcox the baseline in the food industry for providing resilience in the area of potential threats to the food supply is the Hazard Analysis and Critical Control Point System (HACCP). The HACCP is a systemic approach to the identification, evaluation and control of food safety hazards based on a number of principles including a hazard analysis of the likely-to-occur hazards such as toxins, pathogens, metals, glass, chemicals, pesticides, disease, parasites and occasional spoilage. During the Three Mile Island emergency, a number of Hershey's nearby plants and dairy farms were threatened by possible radiation contamination.

Ms. Wilcox relayed how the company had a HACCP in place at all three of its affected plants when on the morning of the incident the entire telephone system in Central Pennsylvania failed. Since Hershey's senior managers could not communicate telephonically they all gathered in the plant manager's office of the world's largest chocolate plant and decided what to do in accordance with HACCP principles to protect the product – and thereby protect the company. A number of actions were taken immediately such as shutting off the air intakes of all buildings and asking all local dairy suppliers to move their herds indoors and feed them only internal feed. They also acquired and deployed radiological testing equipment to determine whether or not there had been any exposure to radiation and, if so, how much. Ms. Wilcox said that with a media anxious to report that Hershey Kisses would "soon be glowing in the dark" the company's swift and decisive action assured that it recovered very rapidly from the event.

Whereas a swift and effective response can largely neutralize the adverse consequences of a catastrophic event, a poor response can have the opposite effect – exacerbating the situation. An insufficient response is not the only concern. Mr. Tenney stated that a prime anxiety

for companies such as Target revolves around how the United States might overreact to the detonation of a weapon within the global supply chain, thereby bringing commerce to a virtual halt and severely damaging the economy. This concern is based, in part, on the results of a highly-publicized exercise conducted by the consulting firm Booz Allen in 2002. The scenario employed a "dirty bomb" that detonated in a container. The exercise estimated that even a brief subsequent port shutdown would produce a backlog of containers that would take 50 days to clear, with a resultant $60 billion hit to the national economy. The West Coast dock strike of 2002 provides additional evidence in that the ten day stoppage, which was widely known about in advance, caused months to recover from and an estimated $20 billion in damages to the economy.

The ability to rapidly respond to a crisis is a major aspect of resilience. As was witnessed by the colossal failures in the wake of Hurricane Katrina, a deficient response can turn an emergency into a calamity of epic proportions. Factors contributing to a successful response identified by symposium participants include advanced planning, reliable communications among first responders, government agencies and all affected parties, engagement on the part of communities and corporations, and accurately assessing the situation so as not to overreach.

CHAPTER 4

RECOVERING *from Disaster*

The ultimate point of resilience is recovery. The ability to quickly return to a state of near normalcy following a catastrophe is the hallmark of a resilient nation. Symposium panelists agreed that nongovernmental organizations play a critical role in disaster recovery efforts. Americans routinely utilize the wide network of private groups and charities to immediately assist their fellow citizens in need. This community-based activism is extremely important to building resilience and is often critical to the first phase of families recovering from a disastrous event.

The ability of the United States to emerge from adversity as a stronger nation has defined us and contributed immensely to America's ascent as a global leader. The fortitude and conviction of Americans is no more evident than in our ability to rebuild after disaster. We, as a nation, must continue to nurture the indomitable human spirit during the darkest times and mobilize Americans in recovery efforts. While there is an important role for federal agencies in supporting and coordinating long-term rebuilding, the most successful efforts will be where families and communities band together. In asserting the importance of local authorities and the role of the citizenry in recovering from a disaster Colonel Randy Larson quoted a former secretary of the Department of Health and Human Services who traveled around the country talking about pandemic flu. What the secretary said in all fifty states was that "Any community that prepares with an expectation that the federal government will come to the rescue will be sadly disappointed."

In describing the difficulties of responding to and recovering from a disastrous event, Mr. **Thomas Von Essen**, New York City Fire Commissioner on September 11, 2001, recalled what a watershed event 9-11 was not just for New York City, but for the whole nation. He noted how woefully unprepared we were for such an event at the time, how we have made limited progress in the interim and how far we have yet to go. Although the city had a wide range of contingency plans, many put in place as a result of deficiencies that were identified in the run up to the "Y2K issue," they had nothing in place that could remotely address a situation where Lower Manhattan had been essentially shut down, thousands of people including hundred of firefighters had lost their lives, the fire department's fleet of trucks had been decimated, the stock exchange was shut down, and there was an immediate need to remove millions of tons of steel from Lower Manhattan.

Mr. Von Essen described the army of construction workers and other volunteers who showed up on their own initiative to assist with

the cleanup and recovery process. He also remarked how private companies provided supplies such as radios and vehicles. All this was done without any contracts or advanced planning in place. He went to state, "What I saw after September 11th was that the greatest resource we have as a nation is us – is our people – is our ability to volunteer, our ability to sit down, put our heads together, and fix things and solve things. And that collaboration, I believe, between the private sector and the public sector is critical to make that happen. It's not going to happen with just relying on the government." He suggested that companies with logistical expertise, such as Wal-Mart, Microsoft, FedEx, UPS, Lowe's and Home Depot, work much more closely with agencies such as the Federal Emergency Management Agency (FEMA) in managing the flow of supplies to areas recovering from a disaster.

Encouraging the spirit of community and cooperation must extend beyond individuals and families and towards companies. Collaboration among otherwise competing firms within an industry is vital to the ability of that industry to quickly recover and resume its critical operations. Speakers on the financial market panel noted that following the events of 9-11 the financial services industry collectively recognized the need to significantly enhance resilience in a sector that was already ahead of the curve compared to other industries in terms of its ability to rapidly recover from a catastrophic event. The events of 9-11, Hurricane Katrina, the 2003 Northeast power blackout, the continued threat of radical Islam, and the emergence of new threats such as pandemic influenza hardened the resolve of the industry to adopt wide-ranging measures to ensure operational continuity in an "all-threats" environment. Many symposium panelists pointed to the financial services sector as a great model for other industries seeking to become more resilient. Their widespread adoption of redundant technologies, robust business continuity plans, energetic test and exercise protocols, willingness to put competitive issues aside, and near-universal mindset that failure is not an option has done much to ensure that our financial institutions can absorb a catastrophic blow – regardless of its type and source – and bounce back rapidly.

> **"WHAT I SAW AFTER SEPTEMBER 11TH WAS THAT THE GREATEST RESOURCE WE HAVE AS A NATION IS US — IS OUR PEOPLE — IS OUR ABILITY TO VOLUNTEER, OUR ABILITY TO SIT DOWN, PUT OUR HEADS TOGETHER, AND FIX THINGS AND SOLVE THINGS."**
>
> **—THOMAS VON ESSEN, FORMER FDNY COMMISSIONER**

Being able to quickly recover and resume operations is not only critical to a company's viability, but also to the health of the economy as a whole. Mr. Martin Padilla noted that a principal concern for Shell is the preparation for disruptive events with an emphasis on how quickly critical systems can be brought back on line and reduce the negative impact on consumers. Taking a "from the field up" approach, Mr. Padilla said that Shell focuses on taking the necessary steps to ensure a reliable post-event fuel supply. The primary vehicle that drives all this activity is Shell's business continuity plan whether the catalyst was a national critical infrastructure event, a terrorism event, or large-scale natural disaster.

According to Mr. Padilla, Shell was successful in rebounding following Katrina and assumed a leading role in assuring that not just Shell, but that the industry in general was able to recover quickly. For example, working with pipeline operators Colonial and Plantation, Shell was able to get petroleum products flowing back through their major pipelines within 24 hours of the end of the storm.

Dr. Bailey stated that in preparation for an extreme disaster scenario, AT&T maintains a fleet of more than 500 tractor trailers and fly-away units for global implementation. These trailers are equipped with all the equipment that AT&T has installed in their production network, such as the switches, routers, multiplexers, transport gear, and all of the supporting chillers and generators. When not deployed, the equipment on the trailers remains connected to their network and monitored and managed and upgraded as a part of the network. Dr. Bailey said that if needed in a particular geographic area, they can quite literally unplug them, hook up a truck, and drive them to the site where we need to basically replicate a significant major office that was lost.

Additionally, Dr. Bailey pointed out that their disaster recovery team is HAZMAT-trained, a policy the company instituted post-9-11. Whereas historically the company had a disaster recovery program focused on natural disasters, 9-11 highlighted the fact that they need to be concerned about whole classes of threats in chemical, biological, and radiological threats that had not previously been considered.

The success of any resilience strategy will be judged on how quickly an entity can recover from an incident. Much can be learned from how businesses plan for continuity and are able to quickly resume operations after an adverse event. Ultimately, the ability of the U.S. to bounce back will rest on its capacity to marshal citizens, communities, and companies to engage in the effort.

CHAPTER 5

IMPORTANCE *of Focused Leadership*

Leadership was a theme that permeated through all symposium discussions. Effective leadership will be required to tie together the four aspects of resilience – preparedness, protection, response and recovery – into a coherent and comprehensive strategy that achieves the "resiliency revolution" that Ms. **Mary Arnold** of **SAP America** called for at the symposium. Over the course of the conference speakers discussed the importance of leadership in creating a national impetus for resilience. The Department of Homeland Security must take the lead in broadening its mission from prevention alone and towards embracing resilience. The present single-minded focus on prevention discourages public involvement in making the United States more resilient and detracts from essential efforts towards preparedness. Because we cannot prevent every catastrophic event, it is important that we prepare for such contingencies and be poised to react when the inevitable event occurs. Changes in attitude need to come from leaders in both the federal government and local communities. Making resilience a priority will ensure that we are adequately prepared for the next Hurricane Katrina or terrorist attack and that such an incident does not severely disrupt vital U.S. economic and social activity.

In arguing for a renewed focus Colonel Larsen contends that as a nation we have asked and continue to ask the wrong question. He notes that when Homeland Security Secretary Michael Chertoff asks "What do we do to prevent a terrorist from smuggling in a biological weapon into the United States?" that is the wrong question. According to Colonel Larsen, the resources to make a biological weapon are within our borders and the Al Qaeda training manual dictates that the preferred method of attack is to construct weapons of mass destruction within the borders of the target country. He stated, for example, the weapons used in the London subway bombing, the Madrid train attack and the 1993 World Trade Center bombing were all constructed within the confines of the target nation. Colonel Larsen said that the right question concerning a threat from nuclear weapons is not how we stop them from smuggling one in, but rather how do we prevent Al Qaeda or other terrorist organizations from becoming a nuclear power. In the case of chemical and biological attacks, we need to understand that there is little that we can do to prevent an attack. The right question is "How do we prepare to rapidly recognize, respond and recover?"

In pointing out the need for visionary leadership, Mr. **Karl Rauscher**, Executive Director, Bell Labs Network Reliability & Security Office, **Alcatel-Lucent**, stated that, notwithstanding the many technological advances, there remain a number of key issues that need to be addressed to adequately secure our Nation. One particularly

important concern is how prepared we are versus how much reacting we are doing. Recent history demonstrates that we often react after a threat occurs – securing cockpit doors, removing shoes for inspection, etc. He said that these are examples of vulnerabilities that existed beforehand, but where an investment to address the vulnerability was not made until after the fact.

LEADERSHIP IS FUNDAMENTAL TO GALVANIZING THE COLLABORATION AMONG ALL RELEVANT PARTIES THAT IS INDISPENSABLE TO RESILIENCE.

Further, Mr. Rauscher observed a troubling paradox concerning the 9-11 attacks. He argued that although various studies of the attacks are quick to point out that determined terrorist organizations are dedicated to doing things that we are not likely to be expecting, the same reports are equally quick to note that preceding the attacks our government displayed a failure of imagination. While we as a nation are being asked to demonstrate that we are more prepared, robust and resilient, in reality we continue to be reactive because we continue to focus on the threat rather than on the vulnerability. Mr. Rauscher emphasized that "Threat versus vulnerability is an important distinction. Threats are infinite; vulnerabilities, finite." We continue to expend precious resources focusing on reacting to threats . . . threats over which we often have no control. Vulnerabilities, on the other hand, are much more within our control. He discussed the need for the private sector to "take the initiative" in addressing vulnerabilities.

Providing an anecdote to demonstrate the importance of informed and engaged citizens to building a more resilient society, Dr. Stephen Flynn recalled the story of United Flight 93, which crashed in a field in Pennsylvania on 9-11. It was prevented from attacking our Capitol as the result of the heroic acts of many of its passengers. Unlike the passengers on the other three jets, since United 93 had departed late, its passengers had learned from frantic calls to loved ones about the true intent of the hijackers. Armed with that information they took the extraordinary measures that ultimately protected our Capitol. Dr. Flynn's point is that the likely "first preventers" and "first responders" in such a scenario are all of us.

Leadership is fundamental to galvanizing the collaboration among all relevant parties that is indispensable to resilience. The financial market panel discussed the extremely high level of resilience-focused cooperation among the various members of the financial services sector and their regulators. Panelists described how much of this is driven by the fact that, notwithstanding organic competition, there are natural interdependencies in the banking industry. Banks depend on each other for clearing and settlement processes as well as the trading of shares. Accordingly, a wide variety of federally-sponsored coordinating councils, as well as private sector-initiated groups, come together on a regular basis, put their competitive differences aside and focus on making sure that the banking and financial serves industry does not fail no matter what happens. Panelists described how the Financial Services Information Sharing and Analysis Center (F/S ISAC) operates around the clock and disseminates critical information to member financial services enterprises in both the United States and around the globe. In 2007, industry members, along with the Treasury Department and other regulators, conducted a pandemic flu exercise that involved over 2,700 financial services enterprises in the United States. This three week long exercise, which simulated a six week flu pandemic, produced many "lessons learned" that will prove to be invaluable when the industry is confronted with the real thing. The industry also participated in a national communications study on the effects of a pandemic flu on the internet and at what point it might actually grind to a halt. For 2008, industry groups are focusing on cyber security threats.

In extolling the benefits of public-private partnerships, Commissioner Joseph Bruno pointed out that private sector participation in emergency preparedness is essential. He stated that fifteen separate sectors are represented in the Emergency Operations Center (EOC) in New York City. There are representatives from the Building Owners and Managers Association, private colleges and universities, hotels, the real estate boards, banks, the security industry, food industry, business improvement districts, the advertising industry, and the Economic Development Corporation, which represents the majority of the city's major corporations. Commissioner Bruno provided a clear example of why private sector involvement is so critical. During the August 2003 blackout, automated teller machines (ATMs) didn't work and the banking industry brought large amounts of cash into the city so that people could get cash at banks if they needed to in order to continue to operate.

Further, Commissioner Bruno highlighted the key role that government agencies can play in helping firms develop, assess and improve their business continuity plans. A crucial component of a viable business continuity program is to exercise the plans to make sure that they work and to identify deficiencies. OEM has begun to assist the private sector in exercising their business continuity plans by conducting tabletop exercises. Commissioner Bruno described how OEM also goes out and provides instruction to corporate emergency management personnel and security personnel on how to run an effective tabletop exercise and how to test their plans. As part of its "Ready New York" program OEM publishes a *Ready New York Guide for Small Business*. He stated that since very few small businesses have the capability of having an emergency management staff, the guide provides practical advice for how small businesses can better prepare for emergencies.

According to Commissioner Bruno, the OEM has high involvement levels and positive relationships with other agencies; so that when a multi-agency situation arises there is a highly effective means of communication available. The OEM has a major role in bringing together a broad range of constituencies at its Emergency Operations Center. Some 130 entities are called together and they all get a seat at the table, including city, state and federal agencies, not-for-profits, utilities and a wide array of private sector participants. He said that there is no "fire-walling" of information. Private sector participants sit directly next to the OEM Commissioner and get the same information that he gets.

Mr. Padilla commented that in the hurricane-prone Gulf Coast, Shell is actively engaged in multiple-state operation centers where early exchange of information and coordination can facilitate better public-private communication. For example, in the state of Texas, Shell has a seat at the state's Emergency Operations Center where their Fuels Operations Team closely monitors the regional supply of product. Mr. Padilla noted, however, that Shell, as well as all the other oil companies, need to work closer with their federal partners to help them better understand that seemingly local events in the Gulf Coast region could easily have national implications. Working with state operations centers is critically important when dealing with mandatory evacuation orders. By participating in the operations centers, oil companies can typically learn of the issuance of mandatory evacuation orders some twenty-four to thirty-six hours in advance. This helps the suppliers to ensure that service stations along various evacuation routes are topped off ahead of the surge of traffic. Being embedded in the operations centers also facilitates the oil companies' participation in state-sponsored readiness exercises, which enhances the competencies of both public and private sector participants.

Resilience requires a new vision of leadership. As opposed to the current top-down approach – where federal agencies such as DHS issue orders with little input from the private sector or state and local authorities – resiliency stimulates collaboration.

CHAPTER 6

CONCLUSION *and Recommendations*

The two days of the symposium vividly illustrated several points. It demonstrated the commitment toward building a more resilient nation by many major components of U.S. industry. It also revealed how much progress we have made during the past seven years – particularly in the private sector – toward building greater resilience. Yet it also highlighted how much farther we have yet to go. For as much as has been achieved in making large segments of our critical infrastructure less vulnerable to the disruptive impact of catastrophic events, we have yet, as a nation, come together to make resilience a top national priority. This needs to change now.

The challenge for America in building a more resilient nation is to change the national mindset from viewing resilience purely through the prism of reacting to unknown and diabolical external forces and refocus it on doing the kinds of things we should have been doing all along…had there been no 9-11. Catastrophic, disruptive events have always been with us and they always will be. What has changed, however, is our vulnerability to disruptive events. There is no small sense of irony when one considers that in many instances society's increased vulnerability has to some degree been brought about as a result of our adoption of, and ultimate reliance on, technology. It is a simple fact that citizens of industrialized nations are far less self-reliant and able to withstand catastrophic events than they once were.

Examples abound. Technological advances in shipping and the development of sophisticated intermodal transportation systems led to the creation of a global supply chain premised on just-in-time delivery, yet which is highly susceptible to disruption. Local power companies are now largely things of the past and the development of highly-networked power grids have made the delivery of electrical power much more efficient and less costly, yet more susceptible to widespread outages when disruptions occur. Although our automobiles are safer, more efficient, more reliable and more comfortable than ever; many motorists in urban and suburban areas find themselves spending increasingly greater periods of time stuck in horrendous traffic.

At the same time, we as Americans, find ourselves bombarded with messages – some more subtle than others – alerting us to the many threats to our national and personal security. One cannot enter an airport, ball game, rock concert, political rally, military base or office building without going through a security cordon. Color-coded threat levels greet us as we arrive at the airport. Random bag checks are being conducted on Amtrak. There is little evidence that any of these actions will make us safer, but no public official wants to answer painful questions about prevention, preparedness and countermeasures on that presumed awful "morning after" some point in the future.

A truly resilient nation places equal emphasis on preparedness, protection, response, and recovery so that it can withstand disruptive events that it knows are inevitable irrespective of their origin. A truly resilient nation can take a punch and can bounce back to a state of near normalcy in a relatively brief period of time. It faces up to the fact that catastrophes are inevitable and that its national focus should be on putting in place or reinforcing systems and programs that will help to ensure that its critical infrastructure can endure the worst of what nature and mankind have to offer. This is where we need to get.

A TRULY RESILIENT NATION CAN TAKE A PUNCH AND CAN BOUNCE BACK TO A STATE OF NEAR NORMALCY IN A RELATIVELY BRIEF PERIOD OF TIME.

American industries of all types are heavily reliant on the global supply chain. Because of the wide ranging economic consequences of a catastrophic disruption, the global supply chain is a particularly attractive target for a terrorist attack. Industry needs to take a clear-eyed look at how a potential supply chain disruption would impact their ability to continue to operate and develop contingency plans that would see them through a temporary disruption. Industry and the American public also need to recognize that the current system for targeting potentially hazardous shipping containers (the ubiquitous lifeblood of the global supply chain) is seriously flawed. As long as programs such as the Container Security Initiative continue to base targeting decisions on inherently suspect cargo manifest data, any sense of increased security is merely illusory.

Recommendations

Based on suggestions provided by symposium participants and its own findings, the Reform Institute has identified several recommendations for building a more resilient America.

The next Administration and Congress must refocus the Nation's homeland security policy with resilience at its core. A comprehensive strategy that encompasses preparedness, protection, response, and recovery will better prepare the United States for the threats of the 21st century. Resilience is a non-partisan concept that can provide a unifying mission to the disparate agencies of the Department of Homeland Security (DHS), encourage bipartisan reform towards making America safer, and unleash the resolve, energy and enterprise of the American people in strengthening the country.

Public-private cooperation is vital to enhancing America's resilience. There is much that the public sector can learn from the efforts of some pioneering companies in assessing the risks and strengthening their ability to function in the face of crisis. Public-private collaboration is key to applying these innovative concepts to government, communities, and other employers. The facts that the vast majority of America's critical infrastructure in the hands of the private sector and that our economic activity is a major target for terrorists dictate solid public-private partnerships.

Strong leadership will be the catalyst for making America more resilient. As a case in point, nothing will better prepare U.S. industry for withstanding and prevailing over a catastrophic event than the widespread adoption and deployment of workable, realistic, business continuity plans. This is particularly true for small and medium sized businesses. There is an important, and heretofore untapped, role for DHS here. DHS needs to be a national resource – a clearinghouse – charged with: conducting an extensive public awareness campaign targeting U.S. industry and emphasizing the criticality of developing workable and practical business continuity plans; assisting U.S. industry in developing business continuity plans by providing templates, advice, best practices and general "help desk" like services; and taking a leadership role

in the development and implementation of national, regional and local exercises with private sector interests focused on the testing of business continuity plans.

Innovation, collaboration and leadership must also be applied to hardening our vulnerable supply chain. Congress and the Administration need to refocus the efforts of DHS and its Customs and Border Protection on working with major shippers, importers, terminal operators and ocean carriers to identify better ways of identifying potential threats to the global supply chain. Specifically, DHS needs to do more to work with the private sector in the adoption of more effective container screening technologies and the widespread deployment of "smart containers."

Strengthening our crumbling infrastructure is also a major priority for attaining resilience. This will be a major undertaking that will necessitate visionary leadership, bipartisan cooperation in Washington, and intense coordination among the public and private sectors. A commitment to public outreach and education will also be required to effectively engage the public in the resilience effort.

Appendix—Program for "Building a Resilient Nation" Symposium

Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy
A National Symposium to Explore the Private Sector's Role in Resilience to our Security and Economy

Hosted by the **Reform Institute** *and Sponsored by the* **McCormick Tribune Foundation**
March 27–28, 2008
New York Yacht Club
37 West 44th Street
New York, NY 10036

Symposium Advisory Committee:
Robert W. Kelly,
CenTauri Solutions, Symposium Chairman
Paul W. Bateman,
President, The Klein & Saks Group
Stephen E. Flynn,
Council on Foreign Relations
Charles E.M. Kolb,
President, Committee for Economic Development

March 27

Welcome & Opening Remarks
Cecilia Martinez, *Executive Director, the Reform Institute*
Robert Kelly, *Founder and Managing Partner for CenTauri Solutions, LLC, Symposium Chair*

Opening Keynote Address
Stephen E. Flynn, *Ira A. Lipman Senior Fellow for Counterterrorism and National Security Studies, Council on Foreign Relations, Author of The Edge of Disaster: Rebuilding a Resilient Nation*

Session 1: Resilience Model
Gary D. Gilbert, *Senior Vice President of Hutchison Port Holdings (HPH) and Chairman of the HPH Security Committee*
Bill Tenney, *Group Manager, International Assets Protection, Target Corp.*
Reynold Hoover, *Assistant Vice President for Police and Infrastructure Protection, CSX*
Moderator: Mary Arnold, *Vice President of Government Relations, SAP America*

Luncheon Keynote Address
Colonel Randall Larsen, *USAF (Ret), Founding Director, Institute for Homeland Security, National Security Advisor to the Center for Biosecurity of the University of Pittsburgh Medical Center*

Session 2: Risk & Threat Assessment and Mitigation
Jack Devine, *President & Founding Partner, The Arkin Group LLC, former Acting Director and Associate Director, CIA Directorate of Operations*
Caren Wilcox, *Executive Director of the Organic Trade Association, Former Deputy Under Secretary for Food Safety at the U.S., Department of Agriculture*
Shaun Flynn, *Chief Risk Officer, QBE the Americas*
Michael Claes, *Executive Vice President/Managing Director, Burson-Marsteller*
Moderator: Major General (Retired) Donna Barbisch, President, Global Deterrence Alternatives

Session 3: Securing the Financial Markets Post 9/11
Timothy P. Farrell, *Senior Vice President, Business Continuity Manager – Corporate, Bank of America*
Phil Marie, *Senior Vice President, Infrastructure Services, The NASDAQ-OMX Group, Inc.*
Leigh Williams, *President, BITS, Financial Services Roundtable*
Shawn C.D. Johnson, *Chairman of the State Street Global Advisors Investment Committee, Director of Institutional Financial Services, Vice Chairman of Financial Services Sector Coordinating Council*
Valerie Abend, *Deputy Assistant Secretary, Critical Infrastructure Protection & Compliance Policy, U.S. Department of the Treasury*
Moderator: Lawrence I. Hebert, *Chairman Dominion Advisory Group, Former President & CEO of Riggs Bank and former Chairman & CEO of Allbritton Communications Company*

Day 1 Closing Remarks
Thomas Von Essen, *former Fire Commissioner, New York City Fire Department*

March 28

Day 2 Opening Keynote Address
Joseph F. Bruno, *Commissioner of the New York City Office of Emergency Management*

Session 4: Securing the Energy Market
Cindy Ortega, *Senior Vice President for MGM MIRAGE Energy and Environmental Services*
Michael J. Kormos, *Senior Vice President of Operations, PJM Interconnection*
Edward M. Stern, *President & CEO, Neptune RTS*
Martin Padilla, *Manager, HSE and Emergency Management*, *Shell Energy North America*
Moderator: Marc Spitzer, *Commissioner, Federal Energy Regulatory Commission*

Session 5: The Role of Telecom
Honorable John Kneuer, Sr. *Vice President for Strategic Planning and External Affairs, Rivada Networks & former Administrator of the National Telecommunications and Information Administration (NTIA)*
Ted O'Brien, *Vice President & General Manager, Americas, Iridium Satellite, LLC*
Karl Rauscher, *Bell Labs Fellow, and Executive Director, Bell Labs Network Reliability & Security Office, Alcatel-Lucent*
Susan (Bobbi) Bailey, *Vice President, Operations, Planning & Support for AT&T's Global Network Operations*
Chris Hackett, *Vice President of Public Sector Sales Programs, Sprint*
Jerry Napolitano, *Solutions Architect for Public Safety Communications, Government & Public Safety, Motorola*
Paul Bates, *Vice President of Global Enterprise Solutions, Verizon*
Moderator: Grant Seiffert, *President, Telecommunications Industry Association*

Symposium materials, such as agenda, participant bios, and summaries of speeches and panel discussions are available on the Reform Institute's website at *http://www.reforminstitute.org/DetailNews.aspx?nid=1322&cid=*

Endnotes

1. References on resilience are available from the Reform Institute website at http://www.reforminstitute.org/DetailPublications.aspx?pid=119&cid=3.
2. See Stephen E. Flynn, The Edge of Disaster: Rebuilding a Resilient Nation (New York, NY: Random House, a Council on Foreign Relations book, February 2007); Yossi Sheffi, The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage (Cambridge, MA: MIT Press, October 2005); Zack Phillips, "Snapping Back," Government Executive, June 15, 2007, p. 36.
3. "Chairman Thompson Announces Key Hearings to Promote a Resilient Homeland," Press Release, House Committee on Homeland Security, May 5, 2008.
4. Homeland Security Advisory Council, Top Ten Challenges Facing The Next Secretary of Homeland Security (Washington, DC: U.S. Department of Homeland Security, September 11, 2008).
5. Symposium materials, including agenda, participant bios, and summaries of remarks and panel discussions, are available from the Reform Institute website at http://www.reforminstitute.org/DetailNews.aspx?nid=1322&cid=.
6. See Robert Kelly, Chain of Perils: Hardening the Global Supply Chain And Strengthening America's Resilience (Alexandria, VA: Reform Institute, March 6, 2008).
7. See Kenneth Nahigian, The Smart Alternative: Securing and Strengthening Our Nation's Vulnerable Electric Grid (Alexandria, VA: Reform Institute, June 20, 2008); see also resources on the Reform Institute website at http://www.reforminstitute.org/DetailPublications.aspx?pid=191&cid=6.

THE REFORM INSTITUTE:
BUILDING A RESILIENT SOCIETY THROUGH FUNDAMENTAL REFORM

The Reform Institute is a nonpartisan, not-for-profit educational organization working to strengthen the foundations of our democracy and build a resilient society. The Institute formulates and advocates valuable, solutions-based reform in vital areas of public policy, including **homeland and national security, energy and environmental progress, economic opportunity and competitiveness, immigration policy, and governance** and **election reform.**

A defining characteristic of the United States has been our resilience – the ability to prevail in the face of seemingly insurmountable adversity and to emerge as a stronger nation. This was accomplished by tapping into the unrivaled resources of the nation, the American people being chief among these, and uniting the public in a common cause. Such resilience, though, cannot be taken for granted. It must be nurtured by strengthening the economy, infrastructure and democratic institutions of the U.S. and empowering her citizens in order to be prepared to confront the next challenge. Allowing every American to realize their full potential will make the U.S. the strong, resilient nation it must be to confront the challenges that lie ahead.

As an independent 501(c)3 public policy organization, the Institute is committed to advancing a policy agenda that engages Americans, especially centrists and independent-minded voters repelled by the partisan gridlock in Washington, in building a more resilient America. The most complex and persistent issues facing the U.S. include establishing a true focus to our homeland security policy that places a premium on enhancing our ability to rapidly respond to and recover from catastrophes while fostering a quick return to a state of near normalcy; developing a comprehensive energy strategy that promotes energy resilience and long-term sustainability; strengthening our economy so that it can continue to be an engine for growth and opportunity in the face of a changing global economy, intensified foreign competition and the aging of the populace; fixing the dysfunctional immigration system through comprehensive immigration reform that balances improving security with acknowledging the importance of immigration to our economy and society; and instituting reforms to the political process that restore Americans' confidence in their government and create an environment conducive to the bipartisan cooperation and leadership that the nation needs.

Political reform is essential to achieving national resilience. Since its founding in 2001, the Institute has been a leader in promoting governance and election reform, recognizing that resolving the most intractable problems confronting our society will require fundamental reform at the core of our democratic system. Such an agenda includes promoting open, fair and competitive elections; reducing the influence of special interests in our politics; advancing accountability and transparency in government; and encouraging a political discourse that rises above blatant partisanship at the federal, state and local levels. Such reforms will encourage more active political participation on the part of the citizenry and produce a more effective government capable of dealing with critical issues.

Governance reform must also encourage significant change in how the public sector interacts with other sectors of society. The challenges of the new century will require a government that is able to serve as a catalyst for focusing the spirit and industriousness of the American people towards overcoming crucial problems. This will require an efficient and responsible government that inspires the populace and supports rather than constrains innovation and enterprise. Effective leadership, combined with more openness with the public and increased collaboration with the private and non-profit sectors, will make America more resilient.

The Institute's work is informed and advanced by a broad base of reformers from across the ideological spectrum, including business leaders, policy experts, and retired and current elected officials and, most importantly, average Americans who are tired of politics as usual. The Institute's distinctive network is reflected in the members of our Advisory Committee – a bipartisan group of notable academics, experts, business leaders and public officials. The Advisory Committee is a "sounding board" for the Institute in its research and development of policy solutions. The committee does not have a governing role with the organization.

The Reform Institute's Board of Directors is chaired by **Paul Bateman** (Klein & Saks Group) and includes **Charles Kolb** (Committee for Economic Development), **Lawrence Hebert** (Dominion Advisory Group), and **Pam Pryor** (Republican National Committee). In addition, **Cecilia Martinez** serves as Executive Director.

The Reform Institute
300 North Washington Street, Suite 600
Alexandria, VA 22314

Tel (703) 535-6897 ★ Fax (866) 863-5510

www.reforminstitute.org