U.S. Resilience Project

RESILIENCE ROUNDTABLE
October 31, 2011
Washington, D.C.

Priorities for America's **Preparedness:** Best Practices from the Private Sector

SPONSORED BY

GEORGETOWN UNIVERSITY
School of Continuing Studies
Center for Continuing and Professional Education

RICHARD LOUNSBERY FOUNDATION

Table of Contents

Overview

On October 31st, the U.S. Resilience Project brought together public and private sector executives in two roundtables. Private sector participants used their own experiences and insights to offer guidance on how private sector best practices and processes can contribute to national preparedness, principles for strengthening public-private partnerships and areas for action.

The Business Case for Resilience
The first decade of the new millennium ushered in two tectonic shifts. The first was intensely visible: multiple attacks on the homeland, which shattered the perception that America could maintain its distance from global terrorism. During the decade, the nation spent an estimated $700 billion — a combined total of federal, state, local and business investment — to protect critical assets and infrastructures against malicious attack, natural disasters and other hazards.

Concurrently, a less visible shift was occurring in the private sector: greater focus on operational risk management in global enterprises. The multinational organizations of the 20th century typically cloned themselves, transplanting their operations as self-contained businesses to foreign shores. The impact of disruptions — whether accidental or man made — remained largely localized. By contrast, leading global enterprises spliced their operations across different geographies, networking them together through communication systems and transportation and energy networks. Disruptions in any part of the value chain could amplify across the network. Driven both by market forces and security concerns, America's corporate leaders have been investing in new processes, tools, technologies, and governance structures to cope with a new spectrum of risk and uncertainty.

Even as the impact of disruptions was growing, so too was their frequency, velocity and unpredictability. Who anticipated a Japanese reactor meltdown, a deep water oil spill or an Icelandic volcano that closed trans-Atlantic traffic? In the age of volatility, companies must develop the capacity to manage the outcomes of disruption, irrespective of trigger.

Over the past decade, America's business leaders have invested in new processes, tools, technologies and governance structures to manage operational risk and create a capacity for resilience.

Connecting the Dots: The tools and processes that companies have developed to manage risk can inform and shape national preparedness and resilience strategies. But, these best practices are not well known or well integrated into national response plans. Greater reliance on existing industry best practices can achieve competitiveness and security simultaneously and free up government resources to safeguard areas that commercial best practices do not and often cannot address.

Private Sector Principles for National Preparedness

Prepare for Volatility and Constant Crises

For the private sector, the challenge is not just coping with hazards; it's coping with constant crises. Global enterprises find themselves simultaneously managing multiple major business disruptions in different parts of the world on the same day.

No Downtime for Risk Management

The drought, floods, tornadoes, earthquake, hurricane, protest demonstrations and intercepted terror attacks that we experienced here in the United States were only part of HP's risk management challenges in 2011. Just touching on the headlines...We dealt with the fallout from civil unrest in Tunisia and Egypt at the beginning of the year, followed by the Christchurch earthquake in February, the Japan disaster and a state of emergency in Bahrain in March. In May, the capture of Osama bin Laden raised the possibility of retaliation. In June, there was an E-coli outbreak in Germany and unrest in Greece and Spain. In July, there were attacks in India and Norway followed by successive typhoons in the Philippines and flooding in Thailand. The bottom line is that no company can take 'time off' when it comes to crisis management and business continuity planning.

Robert Moore
Vice President of Global Security Services
Hewlett-Packard

Build on Private Sector Best Practices

Volatility and uncertainty have created a strong business rationale for resilience — and existing best practices in enterprise resilience already go a long way toward serving national mission needs. Resilience has become a strategic competency and competitive differentiator for American companies. The tools and strategies that private sector companies have created could contribute to national preparedness strategies.

Resilience as a Strategic Competency

The Coca-Cola Company and their bottling partners operate in over 200 countries around the globe and include over 800,000 people producing and marketing over 500 beverage brands of nonalcoholic ready-to-drink beverages that are served over 1.7 billion times a day. This expansive global market place, workforce, and range of beverages present an infinite number of conditions that could potentially disrupt our business. This operating reality mandates that our business possess a globally consistent capability for managing major disruptive events. Resilience not only protects our business viability, it contributes to our competitiveness.

Our strategic approach equips our business system to effectively prepare, respond, recover and restore its operations anywhere in the world, and constitutes the core of our global "resilience capability". This approach integrates five processes — Enterprise Risk Management (ERM), Incident Management and Crisis Resolution (IMCR), Emergency Planning (EP), Business Continuity Planning (BCP), and Disaster Recovery (DR) to deliver our resilience capability. In addition to the formalized global process framework outlined above, guiding principles such as collaboration and transparency by all stakeholders, alignment on strategies, process objectives, and the picture of success are critical to achieving global consistency in our resilience capability.

James Hush
Vice President, Strategic Security and Aviation
The Coca-Cola Company

Adopt a Capabilities-based Approach

Plans are useful, but they are not a panacea. There was no plan to rescue 155 people from the wings of a sinking aircraft in the middle of the Hudson River in January. In an age of turbulence, a strategy that focuses solely on predicting and preparing for specific events is…well, risky. There are an infinite number of potential disruption paths — and a growing number of "black swan" events, which are impossible to predict. Instead, leading companies focus on creating a capacity for resilience: an ability to adapt to the unexpected, respond quickly and mitigate the impacts of disruption.

The Capacity to Manage Unknown Risks

Cisco's perspective on risk is agnostic. We can identify and prepare to deal with known risks. Actuarial data predicts that there will be floods in Thailand and hurricanes in the Gulf of Mexico. But, predictive analytics can't anticipate an ash cloud that shuts down transatlantic air traffic or an earthquake in Chengdu, China. They may predict a tsunami in Japan, but not the shortages of electric power that disrupted production with rolling blackouts.

When you're agnostic to risk, you focus on response capabilities to prepare for risks that have unknown durations and unknown impacts. In those cases, you need to work with response playbooks that identify critical infrastructures and stakeholders. Information and visibility are the backbones of incident response and these tools have to be in place prior to the crisis.

John O'Connor
Senior Director, Supply Chain Operations Cisco Systems, Inc.

Preparedness is a combination of:

- **Adaptability:** creating diverse sets of skills to make sure that you can deal with whatever comes along;
- **Agility:** developing capabilities to respond, irrespective of risk trigger; and
- **Mitigation:** reducing the impact of disruption through system design and smart processes.

Manage Globally, Execute Locally

Company best practices and processes are honed globally, but applied locally with considerable latitude given to the professionals on the ground managing the crisis. If known by and coordinated with the government, these operating practices could create much greater predictability about the capabilities companies are prepared to deploy and help to operationalize public-private partnerships.

Respond Locally with Global Best Practices

Prior to 9-11 there was a lack of consistency and clear lines of authority, support, and communications in John Deere's crisis planning. Recognizing these shortcomings John Deere responded with an enterprise initiative. Today there is one plan for the company translated into thirteen languages. Units are audited for compliance, tabletop exercises are conducted, and managers are required to show their commitment to the plan through communications directed to the senior management. Most importantly, this process has provided an effective mechanism with designated contacts creating a "local responsibility" with "centralized oversight", The key is that those involved know what they have to do in crisis situations and who they should be communicating with.

Jeffrey Chisholm
Director Enterprise Security & Preparedness,
John Deere

Create a Framework of Priorities for Response and Recovery

Crisis response can become chaotic without a framework of principles that set goals and priorities for response. There must be a clear articulation of those goals and priorities so that everyone involved in the recovery effort is working together rather than at cross purposes.

Set a Framework that Governs Priorities for Response

Disaster mitigation processes must be governed by very clear goals. At DuPont, the number one priority is to assure the safety and welfare of employees and their families. Hurricane Irene came through on Saturday night. By Sunday night, our "I'm OK" system had accounted for the status of all 18,000 employees in the affected region. We also knew where our people were struggling with power outages.

After people, DuPont's priorities are: 2) protect the environment 3) restore orderly plant operations 4) Restore customer deliveries. These principles provide guidelines for our actions in every crisis and disaster response. We believe that if you don't have a cohesive set of principles, it's impossible to make informed choices. In our case, meeting our goals depends on our people. Without them, none of the other priorities can be implemented. One of the goals of the national preparedness system should be to clearly articulate those principles and priorities for the government.

Don Wirth
Vice President, Global Operations, Corporate Supply Chains
DuPont

Strengthening Public-Private Partnerships

Understand the Core Competencies of the Private and Public Sectors

There can be little question that infrastructure owners have the technical expertise, skilled workforce, and business incentive to manage risk and recover from disasters. The government should leverage these capabilities and processes rather than attempting to direct them. By the same token, there are issues that only the government can resolve.

Network Reliability: Key Driver in Disaster Recovery

AT&T maintains 99.9999 percent uptime reliability in its network. Just to give some idea of the complexity of that task: If you were to download the digital information processed through AT&T switches over a 24 hour period onto CD's, the stack would reach nearly 20 miles high. The processes, practices and investments that allow the company to achieve that near perfect operational resilience in its day-to-day operation are the same processes that it uses to recover from catastrophic disasters like the tornado in Joplin.

The Joplin tornado — the seventh deadliest storm in U.S. history (and 27th deadliest in world history) — generated winds in excess of 200 mph and took out a swath of telecommunications infrastructure in the region. Within 14 hours, the AT&T disaster network team had triaged the area and restoration teams were onsite and en route — with self-contained cells on wheels (COW) and cells on light trucks (COLT) which replaced the damaged cell sites. Within days, more than 85 percent of the AT&T cell sites in Joplin were operational. Emergency wire line service was re-established to hospitals and the police department as a first priority. But, within five days, more than 18,000 feet of fiber cable and 5000 feet of copper cable had been placed and spliced through the impact area.

Kent Bowen
AT&T Resident Liaison to DHS National Communications System
National Coordinating Center

Industry identified five priorities requiring government action to enable its ability to partner during and after a disaster:

- Establish coherent lines of communications between the public and private sectors
- Enable access to affected areas, including designated staging areas
- Provide security as necessary
- Assure access to fuel, transportation network, and energy
- Remove regulatory and credentialing barriers to movement of people and supplies

Enable Industry-Led Disaster Partnerships

Public-private partnership models are often organized around a seat for the private sector in a government operations center. The Business Emergency Operations Centers (BEOC) deployed in Louisiana and New Jersey, by contrast, create an industry-led, centralized command and control facility – one that activates and supports the State's emergency management mission before, during, and after a major disaster. And this may provide a more effective model for leveraging and deploying private sector assets and capabilities.

The Benefits of Business-Led Partnerships

The success of the private sector response to Hurricane Katrina (the largest disaster in U.S. history) provided a model for the Louisiana Business Emergency Operations Center (BEOC). The Louisiana model brings together 42 private sector members representing key industries (oil and gas, commodities, communications, chambers of commerce, large corporations such as Wal-Mart, etc.) that are critical to a community's resiliency in times of a disaster. This model serves three major purposes:

1. *Facilitating two-way communications between the private sector and government to provide both sectors the information they need to prepare, respond, and recover.*
2. *Utilizing business and industry to assist with emergency response efforts when more cost effective and more efficient.*
3. *Leveraging business and industry to provide "real time" economic impact and to assist with bringing communities back online by having the major industries in the BEOC (retail, banking, fuel, etc.). These industries provide information from their stakeholders such as when gas stations and grocery stores are ready to come back on line.*

In addition, the Louisiana model includes a web portal or "virtual" BEOC where every business in Louisiana can register and experience the same benefits.

Kenneth H. Senser
Senior Vice President, Global Security, Aviation and Travel
Wal-Mart

Identify Risks that Cascade Across Systems and Sectors

The private sector views systemic risks as one of its greatest strategic risks — and it often does not own or control the assets that put its operations at risk. This creates a risk management gap that only the government can fill. A better understanding of the systemic and sector interdependencies and interconnections will help drive cooperation and coordination across the spectrum of preparedness, from prevention to mitigation to response and recovery.

Shared Consequences from System Risks

Imagine a disruption that could paralyze the inland waterway system — one of the major transportation routes of heartland commerce. This was one of the major disaster scenarios identified by ADM, involving assets or infrastructure that the company does not own or control, but which are critical to its business continuity.

As a direct result of that risk assessment exercise and the follow up work done to verify, clarify, and utilize the information, ADM determined that the full scope of the potential loss associated with a major event on the inland waterway system was not known — but that it was clearly in the "disaster" class which is a class of events with loss potential in the realm requiring prevention as a primary focus.

Preparedness for these types of risks requires public-private partnerships — and the federal government needs to look beyond the companies to the resilience of the entire system. For these problems, everyone has a role.

Richard Ryan
Assistant Deputy Director, Corporate Security
Archer Daniels Midland

Capitalize on Private Sector Capabilities

When it comes to disaster recovery, the private sector has already instituted response protocols that often are not fully leveraged by public sector disaster plans. In the insurance industry, the adage is that you cannot stop hurricanes, but you can minimize the damage. The industry has funded the Insurance Institute for Business and Home Safety to provide scientifically-based guidance on how to reduce damage from natural disasters. New research programs are being launched to identify best practices that protect against hail damage and/or protect rooftop equipment. These best practices, capabilities, and toolkits are web-based, publicly available and could be integrated into government disaster preparedness efforts.

Insurance as Part of National Disaster Preparedness

After a disaster, Travelers can move resources into the area within hours. Travelers' Mobile Claim Offices are fully self-contained and can serve as an important resource for our customers when telecommunications networks are disrupted.

Travelers' national Catastrophe Management office constantly monitors events and deploys personnel and equipment as needed, pre-staging whenever possible. Travelers' claim training and workforce management strategies make it possible to leverage our 13,000-person claim organization to quickly pair the right people with the right claim work. Partnerships with hotel, car rental, equipment, tree removal, roof tarping and gasoline vendors can also be critical to our response efforts when supply chains are disrupted.

In addition, the Travelers Institute, the company's public policy division, helps to raise awareness of issues of importance to the property casualty industry, including disaster preparedness. Through regional symposia, the company is facilitating discussion with regulators, government leaders, and other experts to mitigate disasters.

Joan Woodward
Executive Vice President
The Travelers Companies Inc.

Practice and Prepare for Partnership

Partnerships can't begin on the day of a major crisis; they take practice. The benefits from joint drills extend far beyond any single crisis scenario. They create the foundation of understanding about the differences in culture, organization, and perspective that is essential to effective collaboration before, during and after a crisis.

Partnership takes Practice

In 2009, the Maersk Alabama became the first U.S. flagged ship in 200 years to be attacked by pirates. What is less well known is that Maersk and the U.S. Navy had drilled that precise scenario just 2 weeks before the attack occurred. As a result, within 15 minutes of the attack, we had established a complete crisis communications tree between Maersk and the key stakeholders in the government. We both knew each other's procedures and people.

This drill was initiated and organized by Maersk because we believe that these kinds of shared exercises are essential to creating the coordinated response capability — and a joint response is critical when the threats range from Somali pirates to port closures to massive oils spills. These drills — which can involve joint scenario development, joint crisis management, joint public communications — are invaluable for us understand the government priorities and processes and for them to understand ours. That understanding is critical to effective coordination, and it doesn't come from just talking.

Stephen M. Carmel
Senior Vice President, Maritime Services
Maersk Line, Ltd.

Areas for Action

The private sector participants at the Roundtables identified several priorities for action that can be met through strengthened public-private partnerships.

Clarify Roles and Responsibilities
The nation's preparedness must be a shared responsibility; it cannot be directed or regulated from the top down. The ability of the public and private sectors to partner effectively depends, in large part, on whether the two sectors can define and accept their respective roles and responsibilities. These must be determined by not only by what must be done, but which stakeholder has the best capability to do it. In many case, the systems expertise, competencies, tools reside in the private sector. Although government is a critical facilitator, the government does not — and cannot — play a leading role in private sector risk management and mitigation.

In the view of private sector participants, a model that works well is the Overseas Security Advisory Council (OSAC) which defines the customer (in this case the private sector which leads the economic engine) and posits the foundation principle that government supports and facilitates prevention, response and recovery.

Implement Performance-based Targets, not Checklist Standards
Performance targets describe a desired end state and allow companies flexibility in meeting those targets, consistent with their business models. Checklist standards, by contrast, push the private sector toward "lowest common denominator" procedures rather than best practices. Moreover, these kinds of standards cannot keep pace with changing risks or create sufficient flexibility for innovative responses.

Identify Clear and Transparent Communications Channels
The lack of clear point of contacts — on both sides — is seen as a major stumbling block. There is strong consensus that finding the right point of contact cannot be left to chance connections during a crisis. Although there is no single point of contact or silver bullet solution, there is a need to create an information sharing environment that assures that clear communications channels before during and after an event. The right connections are made before, during and after an event.

Harness the Power of Intelligent Networks and Social Media

The focus for national preparedness should be on creating situational awareness, enhanced decision-making and rapid response; Platforms like the U.S. Resilience System, that are based upon distributed intelligent social networks and crowd-sourcing, can enable far more agility and adaptability than a highly structured, hierarchical capability with significantly better outcomes at far less cost. Exploiting U.S. leadership in this area has the potential to create significant engagement in preparedness, disaster response, and regional resilience building.

Develop an Industry-Led Emergency Operations Center to Coordinate With Government at the National Level

FEMA should expand its support of the private sector and community resiliency by developing a national, industry-led emergency operations center with virtual capabilities. The emergency operations center should include representatives from organizations or associations that support community resiliency before, during and after a disaster. The primary purpose of the center should be to improve communications between government and the private sector at the national level, utilize supply chains and other private sector best practices that are more cost effective and efficient in times of disaster, and leverage business capabilities to assist with recovery.

Increase Opportunities for Joint Training and Collaboration

Currently, joint exercises are mandatory only for oil spills, but the government needs to practice and prepare for partnership across a range of potential disruptions, particularly where it needs to engage private sector assets and expertise. Joint exercises may fail because they are often focused only on the most catastrophic events. A better path to collaborative working relationships would be to work together more frequently on smaller problems that build confidence in collaboration and trust among the partners.

Questions for Future Consideration

How can the public and private sectors better collaborate to address emerging cyber risks?
Cyber risks pose emerging, fast-moving, highly complex and high impact challenges that are poorly understood. The risks are largely unknown. There is no common lexicon and no data set to anticipate the duration and impact. As important, the interdependencies between the physical and cyberworlds have not been well mapped. All physical response plans are based on the assumption that IT and communications are available.

How can the competitive advantages of resilience be balanced against the shared value of collaboration and information-sharing around best practices, processes and tools?
In an age of turbulence, the ability to weather any storm can become a competitive differentiator for companies, and best practices are often seen as proprietary. But, in a world of interdependencies — where small failures can amplify — there is also shared value from creating resilient companies, communities and countries. How can we build the business case for sharing information about best practices and tools for resilience that increase the capacity for resilience more broadly?

How can the private sector leverage best practices in risk management and resilience to identify opportunities to streamline rules and regulations?
As new practices and tools for risk intelligence and resilience emerge, there will certainly be new opportunities to create a supportive policy and regulatory infrastructure. The private sector can help implement Executive Order 13563, which promotes retrospective analysis of rules that may be outmoded, ineffective, insufficient or excessively burdensome and help accelerate the transition from a homeland security strategy to a national resilience and preparedness strategy.

What are the new skills sets needed to create a resilient workforce able to anticipate and manage volatility and uncertainty?
Working together, the public and private sectors can identify the new skills needed to implement resilience and discuss how these skill requirements can be integrated into existing educational and training programs — from professional curricula to technical and trade institutions.

Morning Session Agenda

Eisenhower Executive Office Building
Room 430A
725 17th Street, NW
Washington, D.C. 20006

9:00 WELCOME

Richard Reed Special Assistant to the President, Resilience Policy

Debra van Opstal Director, The Resilience Project

9:10 ROUNDTABLE INTRODUCTIONS AND PERSPECTIVES

Short 3 minute perspectives on the business case and best practices in risk and disaster management

10:15 BREAK

10:30 FACILITATED DISCUSSION

Facilitator: **Richard Reed** Special Assistant to the President, Resilience Policy

Questions:

- How can the federal government better integrate and leverage the risk and disaster management capabilities and competencies of the private sector for national preparedness?
  - What specific expertise or assets present in the private sector are most useful to the government
  - How can business ensure it is provided to local and federal officials in a timely and effective manner in an emergency?
- What is critical to business's continuity of operations and what should government do to support resumption of operations after a disaster?
- What is needed to make public-private collaboration for preparedness more efficient and effective?
- What can public policy makers learn from the private sector about managing risks in global networks?

12:00 ADJOURN

Morning Session Participants

Philip Auerswald
Senior Fellow
Kauffman Foundation

Debra Ballen
General Counsel and Senior Vice President of Public Policy
Insurance Institute for Business & Home Safety

Kent Bowen
Resident Liaison to DHS National Communications System, National Coordinating Center
AT&T

Stephen M. Carmel
Senior Vice President, Maritime Services
Maersk Line, Limited

Jeffrey Chisholm
Director Enterprise Security & Preparedness
Deere & Company

Spiros Dimolitsas
Senior Vice President for Research and Chief Technology Officer
Georgetown University

Edward Erickson
Vice President
IntraPoint

Craig Giffi
Vice Chairman
Deloitte LLP

James A. Hush
Vice President, Strategic Security and Aviation
The Coca Cola Company

Michael D. McDonald
President and CEO
Global Health Initiatives, Inc.

Robert Moore
Vice President of Global Security Services
Hewlett-Packard

John O'Connor
Senior Director, Supply Chain Operations Cisco Systems, Inc.

Erik R. Peterson
Director
Global Business Policy Council
A.T. Kearney

Richard Ryan
Assistant Deputy Director
Corporate Security
Archer Daniels Midland

Kenneth H. Senser
Senior Vice President
Global Security, Aviation and Travel
Wal-Mart Stores, Inc.

Donald D. Wirth
Vice President, Global Operations Corporate Supply Chains
DuPont

Joan Woodward
Executive Vice President
The Travelers Indemnity Company

GOVERNMENT

Patricia Hoffman
Assistant Secretary
Office of Electricity Delivery and Energy Reliability, Department of Energy

Richard Reed
Special Assistant to the President for National Security Affairs and Senior Director for Resilience Policy
National Security Staff

Douglas Smith
Assistant Secretary
Private Sector Office
Department of Homeland Security

Ahsha Tribble
Director, Critical Infrastructure Protection and Resilience Policy
National Security Staff

Lawrence Zelvin
Director for Incident Management Resilience Policy
National Security Staff

THE RESILIENCE PROJECT

Debra van Opstal
Director

Dana Martin
Deputy Director

C. William Booher, Jr.
Senior Advisor

Denise Swink
Senior Advisor

Afternoon Session Agenda

The Ronald Reagan Building
Conference Room 6.5E
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The Competitive Advantages of Resilience: A Dialogue with Business Executives

3:00 **WELCOME and ROUNDTABLE INTRODUCTIONS**

Douglas Smith Assistant Secretary, DHS Private Sector Office

Debra van Opstal Director, The Resilience Project

3:15 **DISCUSSION QUESTIONS**

Facilitator: **Michael Frias** Deputy Assistant Secretary, DHS Private Sector Office

- How does your company develop and socialize the business case for enterprise resilience?
- How do you prioritize what risks to manage or mitigate, and what is the process to continuously review existing or evolving risks?
- How do you know if you're successful and how is success shared within your company?
- What do you see as the biggest risks outside your direct control — and where do you see the biggest opportunities for public-private partnerships to manage and mitigate risk?
- Are there capabilities resident in the private-sector that are critical to your business resilience that you would be willing to partner/co-invest with government to develop or deploy?

5:00 **NEXT STEPS and ADJOURN**

Afternoon Session Participants

PRIVATE SECTOR

Jeffrey Chisholm
Director Enterprise Security & Preparedness
Deere & Company

Edward Erickson
Vice President
IntraPoint

Craig Giffi
Vice Chairman
Deloitte LLP

John O'Connor
Senior Director, Supply Chain Operations Cisco Systems, Inc.

Richard Ryan
Assistant Deputy Director
Corporate Security
Archer Daniels Midland

DEPARTMENT OF HOMELAND SECURITY

Kathleen Appenrodt
Policy Advisor
Private Sector Office

Christa Brzozowski
Director, Global Supply Chain Security National Security Staff (NSS)
Detailed to the NSS from DHS Office of Policy

Michael Frias
Deputy Assistant Secretary
Private Sector Office

Alex Garza
Assistant Secretary for Health Affairs and Chief Medical Officer
Office of Health Affairs

Maria Luisa O'Connell
Senior Advisor
Customs and Border Protection

Marcus Pollock
Chief
Standards and Technology Branch
Federal Emergency Management Agency

Douglas Smith
Assistant Secretary
Private Sector Office

Roberta Stempfley
Acting Assistant Secretary
Office of Cyber Security & Communications, National Protection & Programs Directorate

THE RESILIENCE PROJECT

Debra van Opstal
Director

Dana Martin
Deputy Director

C. William Booher, Jr.
Senior Advisor

Denise Swink
Senior Advisor

About the U.S. Resilience Project

Building on Business Best Practice to Meet National Challenges

The primary goal of the U.S. Resilience Project (USRP) is to advance cutting-edge resilience policies, practices, and public-private partnerships by:

- Capturing cross-sector business best practices, processes and tools for resilience and preparedness;
- Creating a framework for public-private partnerships that builds on key competencies and best practices
- Educating public and private sector executives in cutting-edge tools and management strategies.

Key Concepts

Warning: Turbulence Ahead. The one thing we know with certainty is that the future will be volatile and uncertain.
Capturing the Business Case for Resilience. Since it is impossible to accurately predict every possible risk trigger, business leaders are creating new strategies that rely on agility and adaptability
Building Best Practices into National Strategies. Existing best practices in enterprise resilience already go a long way toward serving national mission needs, but are not always integrated into government strategies.
Valuing the 75 Percent Solution. Although government and industry objectives are not identical, private sector best practices can contribute significantly to national resilience – and free up government resources to address gaps.
Creating Two-way Partnerships. Partnerships must be built around defining key roles and responsibilities, based on capabilities, competencies and mission objectives.

Staffing

Debra van Opstal, director of the U.S. Resilience Project, was formerly a senior vice president at the Council on Competitiveness, authoring *Transform: The Resilient Economy*.

Dana Martin, deputy director of the U.S. Resilience Project, was formerly chief of staff and secretary to the board at the Center for the Study of the Presidency and Congress.

Denise Swink, a senior advisor of the U.S. Resilience Project, has more than 35 years of experience in management and supervisory positions, with key expertise in public-private partnerships, manufacturing, and infrastructure interdependencies.

Bill Booher, a senior advisor of the U.S. Resilience Project, was formerly executive vice president and treasurer of the Council on Competitiveness.

U.S. Resilience Project
Washington, D.C.
www.usresilienceproject.org