

“Law Amid the Ruins: Doing Business After Disaster”

Sponsored by the McCormick Tribune Foundation

Organized by the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum

Cantigny Conference Series, May 11-13, 2005

Written by Lauren Bean, Editor, National Strategy Forum

I. Introduction

On May 11-13, 2005, experts from the government, business, legal, law enforcement, emergency responder, public health, public works and non-profit sectors met at the McCormick Tribune Foundation Cantigny Conference Center in Wheaton, IL to discuss continuity of operations (COOP) for the public and private sectors in the event of a catastrophic incident—an event that would have a widespread, potentially disastrous impact on U.S. critical infrastructure including medical, communication, transportation, financial, commercial, commerce, utility and trade services.

The McCormick Tribune Foundation sponsored the conference entitled “Law Amid the Ruins: Doing Business After Disaster,” which was organized by the American Bar Association Standing Committee on Law and National Security (ABA SCOLANS) and the National Strategy Forum.

Conference participants identified issues, raised questions and offered suggestions regarding U.S. emergency preparedness, response and recovery planning for a catastrophic incident. This executive summary provides a brief, comprehensive overview of the conference proceedings and the important themes and issues that emerged from the six discussion sessions. The conference was not-for-attribution.

Throughout the discussion, conference participants focused on five primary issues:

1. The likelihood of a catastrophic incident (a terrorist attack, a natural or man-made disaster, mass utility outage, etc.) occurring in the U.S. is incalculable. However, the impact of an array of possible scenarios needs to be anticipated and quantified through discussion, coordination and planning.

2. There needs to be a cohesive, national infrastructure protection and response plan that encompasses federal, state, and local government, the private sector and other stakeholders. Existing federal response plans, including the National Response Plan (NRP) and the National Infrastructure Response Plan (NIPP), offer a working foundation and a common vocabulary.
3. The information and coordination gaps that exist in current continuity planning, including the legal dimension, need to be addressed before another catastrophic incident occurs in the U.S.
4. There needs to be a strategy to engage and educate the public and private sectors about basic emergency preparedness leading to more complex emergency-related issues.
5. The task of continuity planning is complex and daunting. An effective plan needs to set realistic, achievable standards and goals.

II. Start with a Worst-Case Scenario, and then Work Backwards and Forwards

The conference opened with a hypothetical catastrophe scenario and discussion regarding the National Response Plan. The hypothetical “doomsday” nuclear scenario involved a 10 kiloton nuclear explosion in a shipping container placed on the pier in the Port of Long Beach, CA. Initial effects include a blast wave that would cause destruction within a one-mile radius. Long-term effects include radioactive fallout, as well as a ground burst scenario which would have widespread, destabilizing effects on the surrounding environment resulting in mass casualties, the disruption of services and possibly mass chaos (for example, an exodus of people from a contaminated area).

U.S. critical infrastructure is vulnerable to an array of threats. Participants agreed that the biggest challenge to preparing for a disaster may be deciding what to prepare for—a 10 kiloton nuclear explosion versus a multi-state blackout—a decision that dictates the roles and responsibilities of those involved in the planning, response and recovery processes. A nuclear attack scenario and the terrorism dimension introduce

new, more complicated layers to crisis and incident management, including the issue of national/international consequences and expectations.

A first step in undertaking this challenge may be to recognize that even the most improbable scenarios may occur in the future. Adopting a comprehensive, all-hazards approach may be helpful, but not flawless. Incident-specific consequences will vary depending on the threat and the magnitude of the disaster, the amount of destruction and the amount of post-scenario impact on an area.

Participants identified several fundamental, precautionary issues that stakeholders should consider in preparing for a wide range of threats: identifying where the initial responsibility lies and what the first responsibility is in the immediate aftermath of a disaster; anticipating an evacuation or shelter-in-place scenario; anticipating short- and long-term effects; assessing how cascading effects can be minimized or prevented; replenishing depleted resources; and restoring disrupted services.

III. Common Vocabulary, Common Goal

Participants agreed that an effective plan requires a common goal: collaboration. Collaboration requires a common understanding of the intended objectives of a continuity plan—effective preparedness, response and recovery.

At the federal, state, and local levels and between the private and public sectors, developing and implementing a continuity plan and achieving collaboration require a common vocabulary to frame the discussion. The misconstruing of continuity-related acronyms can hinder communication between those involved in the planning process.

Conference participants shared their definitions for the following terms:

- Continuity of Government (COG): maintaining the legitimacy of government as the entity in charge
- Continuity of Business (COB): the maintaining and survival of business
- Continuity of Operations (COOP): the continuance of operations of government and the private sector

IV. Existing Plans: Pros and Gaps (The National Response Plan)

In March 2003, President Bush issued Homeland Security Presidential Directive V, which called for the establishment of a new regime for incident and emergency management. In 2004, the National Response Plan (NRP) and the system upon which it is based, the National Incident Management System (NIMS), were developed by the U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) to coordinate federal and local agencies for emergency preparedness and to provide a common framework for incident management and emergency response at the national level.

Participants discussed the nature of the NRP—whether it is a national response plan versus a statement of principles and, as a plan, whether or not it is sufficient. Others raised questions regarding the scope of the NRP—is it really a national plan? Or is it a federal plan? It was agreed that the NRP is a good base start, but that greater emphasis needs to be placed on the following issues for the plan to evolve:

- The roles and responsibilities of the state, local and regional levels; more state and local interface
- The roles and responsibilities of the federal agencies, states and localities
- The preparedness, prevention and protection phases of the planning process
- The legal dimension of continuity planning
- The definition of “intelligence”; the processes, procedures and protocols regarding the form of operational intelligence support needed to implement the NRP
- Private sector coordination, roles and responsibilities, and sector-specific demarcations (industries, small business, community-at-large); those in the private sector that control key elements of U.S. critical infrastructure
- Civil-military integration in the event of a disaster
- Cyber-security

Participants agreed that the NRP is a planning structure, and that one of the most important questions to consider when assessing the NRP is whether this structure can function in a chaotic, post-disaster environment. Participants agreed that the NRP, in time, will evolve into a fully functional plan. In reinforcing this point, participants noted that several annexes and emergency support functions have been added to the plan since its formation, and other plans, including the National Infrastructure Protection Plan (NIPP), can complement the NRP.

V. It’s the Process, Not the Plan

Participants agreed that the planning stage—engaging people and agencies—is the most important step in the prevention, protection, response and recovery process. Establishing common ground for dialogue, understanding and collaboration among agencies at all levels and between sectors is imperative.

Managing Expectations

Participants agreed that an important step in the planning process is to come to a consensus about what is expected of a national response plan. What are its limitations? Also, what is expected of the people and agencies involved at the federal, state, and local levels and the private sector? What do these stakeholders expect of each other? What does the public expect of local, state and federal agencies? Each sector has its own idea of what it is responsible for, its own set of plans, and its own set of expectations of the responsibilities and functions of other sectors.

Assigning Roles and Responsibilities for Continuity of Operations: Who Has Responsibility for What?

Whether the incident is a nuclear attack scenario, which creates a unique dimension to the planning process, or a natural disaster, the issue of agency-specific responsibilities for continuity of operations is a significant challenge—no one branch of government or sector has total authority.

- What is the federal government’s role in the event of a catastrophe for response, restoration and recovery?
- What is the role of state and local government agencies?
- What is the role of the private sector?
- What are their relationships to each other?
- Where does the initial responsibility lie?

A barrier to identifying the agency- and sector-specific roles and responsibilities is the tendency toward, as one participant noted, relying on the federal government to “save the day.” The issue of interdependency among agencies and sectors during and after a disaster is critical.

Participants agreed that in the initial aftermath of a disaster, the operational responsibility for (a) providing support and (b) serving as a conduit to the federal government to request assistance for emergency first responders is at the state and local levels. For example, in the event of the hypothetical nuclear attack scenario, local agencies might conduct situational and intelligence information assessments of the operational emergency area where the disaster occurred, which would then be transmitted to the state level in order to develop a collaborative understanding of what type of support might be needed.

The federal government has limited authority, as defined by the Constitution. In responding to a nuclear attack perpetrated by terrorists, the federal government has the

authority and responsibility to protect the states. Participants agreed that the federal level also has a responsibility to provide assistance to the state and local agencies—fire, police and first responders—in the aftermath of a catastrophic incident. Because of the nature of a nuclear terrorist attack as an “incident of national significance,” there will be a demand for information at the national level, although the task of providing that information lies with the local and state authorities. One participant noted that the role of the federal government in emergency preparedness, response and recovery is not limited to the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), which has direct responsibility for assisting the state and local governments, and the Department of Defense (DoD) and the military; responsibility extends to other government agencies including the Department of State (DoS), the Centers for Disease Control (CDC), the Department of Health and Human Services (HHS), and the Department of Commerce (DoC).

It may be difficult to avoid overlap among the roles of the different levels, agencies and sectors; however, one common responsibility that these stakeholders share is a duty to the public to disseminate a clear, unified message in the aftermath of a disaster. This public information/public affairs sector, specifically the media, plays a critical role in communicating this message to the public. But, the responsibility for getting the correct information to those outlets lies at the local, state and federal levels.

VI. Broaching the Fear Issue: Educating the Public

The “fear factor”, or the fear of creating unwarranted public fear about the real possibility of nuclear terrorism and the fear of well-intentioned messages becoming farcical (for example, the duct tape and sheeting advisory) are legitimate concerns. However, there was consensus that a public education/communications strategy (one emergency support function, ESF15 - public communications, has been added to the NRP) and pre-loaded, sophisticated public awareness campaigns must be an integral part

of the planning process. The public is a key stakeholder and the public response can heavily impact the response efficiency of the local, state and federal agencies.

The American people need to better understand why they should proactively educate themselves and prepare for these scenarios, some of which might seem highly unlikely to a school staff member in Kansas whose broader concern is whether the students make it to school safely. Also, there is the issue of public denial that a nuclear attack will occur. What should they do and what can they do?

Participants agreed that the public must be engaged in thinking about and discussing possible catastrophe scenarios, the array of possible consequences (for example, mass casualties, radioactive protective measures, shelter-in-place and evacuation), and their expectations of the local, state and federal levels and vice versa before an incident occurs. Citizens will make their own decisions—if someone wants to flee, he or she will flee—however, minimizing mass panic through education is prudent.

One participant suggested that agencies be careful in drawing the line between planning and implementation for a catastrophic incident when dealing with issues that are inherently political, including public awareness campaigns. One approach to this concern might be to identify a well-known, apolitical organization such as the American Red Cross to sponsor public preparedness education.

Managing Resources

Participants emphasized that the resources needed to provide necessary emergency support functions in the aftermath of a catastrophic incident are critical to short- and long-term recovery. This includes the military, which is currently stretched thin and may not be readily available in the event of a disaster. The public and private sectors need to be thinking about this issue during the pre-planning phase.

Media

The media—radio, television, internet or print—has a critical role to play in educating the public before, during and after an event. One participant suggested that the media vacuum be filled by credible officials and that media personnel receive incident-specific training.

VII. Private Sector Roles and Responsibilities

The private sector represents one-third of the U.S. economy and 85 percent of U.S. critical infrastructure. Participants agreed that there is a lack of discussion about the private sector role and responsibilities in terms of business continuity, continuity of operations, and the role of market forces in modifying or influencing the behavior and expectations of the private sector.

Participants raised several questions:

- How prepared is the private sector for a catastrophic event? What are the important issues that need to be addressed in terms of the private sector role in the planning process?
- What type of planning and thinking is going on in the private sector about its role in the planning process?
- What are the private sector expectations of what the federal government will do?

In the event of a nuclear attack scenario, the disruption of the key private sector critical infrastructure would have devastating, widespread consequences. Faced with a nuclear attack in the Port of Long Beach, other ports might close, cutting off the supply chain infrastructure, which could facilitate and/or accelerate the impact of the attackers. How do we make the business case for security? How do we define a common operating picture for the private sector that would create incentives for collaboration, information-

sharing and strategizing? How does the government communicate the possible outcomes of various scenarios and processes?

Several participants suggested that energizing the discussion about the private sector and engaging the private sector to become more proactive in thinking systematically about the planning process for a catastrophic incident requires a strong motivation, “a carrot and stick” approach to induce compliance (standards and regulations). Another participant raised an important consideration—the issue of what motivates the private sector. The federal government is motivated to meet public expectations; the private sector is motivated by different things. Also, there is no enforcement mechanism to compel the private sector to enforce best practices for preparedness.

Participants debated the issue of whether the government should take a strong stance to increase private sector involvement in planning for a catastrophe. Participants agreed that voluntary standardization of industry would be slow. However, the issue of governmental promulgation of standards raised a red flag for one participant who noted that there are limitations regarding what the government can do in defining best practice for an industry. When the government attempts to dictate the behavior of an industry, the results can be disastrous. Still, there are ways the government can encourage the involvement of the private sector in COOP planning, including penalties and incentives.

VIII. Interdependency: Dividing Responsibility

Who is responsible for coordinating all of the efforts? What is the coordinating mechanism of sectors? Is there a private-public sector linkage between industries and the government? Participants agreed that cross-industry dialogue, which is imperative for collaboration and support, is starting to occur, but that there is a further need to elevate and induce the discussion through a neutral forum. For example, the Industry Advisory Council (IAC) was established to bring industry and government executives together to exchange information, improve communications and build partnerships; the Information

Sharing and Analysis Centers (ISACS), created by Presidential Directive 63 was designed to share concerns about vulnerabilities, threats, intrusions, and anomalies within and between industry sectors and the National Infrastructure Protection Center (NIPC). The objective of ISACS is to develop sector organizations to gather, analyze and disseminate private and public sector information to its members and NIPC.

IX. Addressing the Legal Dimension

Participants agreed that there is a critical information gap regarding the legal dimension of continuity of operations. There is a need to identify the embedded legal issues. Federal agencies have a solid grasp of the NRP. The federal government has identified its legal authorities as well as its areas of vulnerability. However, questions were raised as to whether state and local agencies have thought about their legal authorities and areas of vulnerability in the event of a catastrophic incident. One participant added that there is a lack of understanding among state and local agencies regarding how their systems would be coordinated during a large-scale incident.

Participants agreed that there is more to be done in addressing the legal dimension of continuity planning. For example, have federal, state and local agencies, specifically local law enforcement, anticipated the issues they will confront in a possible isolation/quarantine scenario in the event of a contamination incident and how they will coordinate to resolve these issues? Federal statutes and regulations do not address handling of a national bioterrorism incident involving various degrees of contagion: How do you handle detention? What are the rules of engagement? What about the use of force? What are alternative approaches to the use of force?

One way to address the issue of quarantine and the broader subject of legal implications goes back to the issue of education and communication—education regarding the various levels of quarantine, relevant preparedness and response procedures, and the legal risks. For the private sector, this means educating industry about the possible impact of an event, such as a containment/detention situation, and the

ensuing embedded issues such as the disruption of the supply chain, disruption of overseas capabilities including trade, the impact of regulations, a responsibility to employees and shareholders, and other issues.

For both the private and public sectors, this means addressing the issue of information-sharing.

X. What’s Next: Conclusions and Next Steps

Participants agreed that the current COOP planning is a good start. However, the current level of response is “too federal.” The next steps that are needed to build on and expand upon continuity planning for the private and public sector include:

- *Frame the discussion:* What do we mean by COOP, COG and COB?
- *Manage expectations:* What is the goal?
- *Manage roles and responsibilities:* Who is responsible for what? (Planning, funding, providing incentives, setting standards, communications, etc.)
- *Generate a clear message:* What are we planning for?
- *Educate the public:* What are the information gaps?
- *The National Response Plan:* How do we facilitate and integrate greater state and local interface?
- *Examine existing plans:* Do they adequately address the issue of cascading effects?
- *Re-examine the existing concept of national security:* Is the definition adequate?
- *Ensure cooperation:* What can be done to strengthen the private-public sector partnership?
- *Improve information-sharing networks:* What are the barriers? How can they be resolved?
- *Engage the private sector:* What are business concerns and motivations for security?

“Law Amid the Ruins: Doing Business After Disaster”
McCormick Tribune Foundation Cantigny Conference Series
May 11–13, 2005

- *Confronting legal issues:* Is there an opportunity for a new body of Catastrophic Risk Law specializing in catastrophic risk issues?
- *Plan for legislative changes:* What new factors will arise?
- *Change our assumptions about the future:* How can we maintain a level of adaptability?

McCormick Tribune Foundation Cantigny Conference Series post-conference reports may be found at the foundation’s website, www.mccormicktribune.org/citizenship.

More information about the National Strategy Forum may be found at their website, www.nationalstrategy.com.

PARTICIPANTS

Ernest B. Abbott

Principal
FEMA Law Associates, PLLC

P.J. Aduskevicz

Vice Chair of Program Development
IEEE Communications Society
President, PJ Aduskevicz Enterprise LLC

Dan Bart

Co-Chair, American National Standards
Institute's Homeland Security Standards
Panel (ANSI-HSSP)
Senior Vice President, Standards and
Special Projects
Telecommunications Industry Association
(TIA)

Matthew R. Bettenhausen

Director of the Office of Homeland Security
State of California Governor's Office
Office of Homeland Security

James N. Bond

Chief, Eastern Law Division
Directorate of Legal Research for
International, Comparative and Foreign Law
Law Library of Congress

M.E. (Spike) Bowman

Director, Intelligence Issues Group
Federal Bureau of Investigation (FBI)

Edward G. Buikema

Acting Response Division Director
US Department of Homeland Security
Federal Emergency Management
Agency (FEMA)

Angeline G. Chen

Adjunct Professor
George Mason University Law School
Associate General Counsel
Lockheed Martin

Thomas J. Connelly

Associate General Counsel
Information Analysis and Infrastructure
Protection (IAIP)
US Department of Homeland Security

Angela Desmond

Deputy Associate Director
Division of Banking Supervision and
Regulation
Board of Governors of the Federal Reserve
System

Sheila G. Dryden

Consultant, National Communications
System
Information Analysis and Infrastructure
Protection (IAIP)
US Department of Homeland Security

James W. Duncan

Executive Officer, National Preparedness
Division
US Department of Homeland Security
Federal Emergency Management Agency
(FEMA)-Region V

Alan L. Ferber

Attorney-Advisor for Emergency Planning
US Department of Justice

Richard E. Friedman

President and Chair
National Strategy Forum

**“Law Amid the Ruins: Doing Business After Disaster”
McCormick Tribune Foundation Cantigny Conference Series
May 11–13, 2005**

Demetria Giannisis

Managing Director
Great Lakes Partnership (GLP) for
Infrastructure Security and Economic
Sustainability
President/CEO, Chicago Manufacturing
Center

Brenton Greene

Vice President, Strategic Initiatives
Lucent Technologies

Rosemary Hart

Special Counsel, Office of Legal Counsel
US Department of Justice

Patrick J. Laird

Vice President, Corporate Security
Exelon Corporation

Francesca M. Maher

Chief Executive Officer
American Red Cross of Greater Chicago

Paul M. Maniscalco

Deputy Chief/Paramedic (retired)
New York City Emergency Medical
Services
Assistant Professor
Homeland Security Policy Institute
The George Washington University

Gene W. Matthews

Director, Institute of Public Health Law
Centers for Disease Control (CDC)
Foundation

John A. McCarthy

Executive Director
Critical Infrastructure Protection Program
George Mason University School of Law

James E. McDaniel

Of Counsel
Lashley & Baer

Peter A. Modafferi

Chief of Detectives
Rockland County (NY) District Attorney's
Office

Roger C. Molander, PhD

Senior Research Scientist
The RAND Corporation

Michael John O'Dell, CBCP

Deputy Division Manager
Continuity of Operations Division
Titan Corporation

Jon M. Peha

Professor and Associate Director
Center for Wireless and Broadband
Networking
Department of Engineering and Public
Policy
Carnegie Mellon University

George A.B. Peirce

General Counsel
Defense Intelligence Agency (DIA)

Vincent I. Polley

President
KnowConnect, Inc.

John R. Powers, PhD

Chairman
The FirTH Alliance, LLC

Jill D. Rhodes

Senior Legal Advisor
SRA International

Ralph E. Sharpe

Of Counsel
Venable, LLP

Suzanne Spaulding

Managing Director
The Harbour Group, LLC

“Law Amid the Ruins: Doing Business After Disaster”
McCormick Tribune Foundation Cantigny Conference Series
May 11–13, 2005

Laurence Storch

Of Counsel
Dilworth Paxson LLP

John P. Sullivan

Lieutenant
Los Angeles (CA) Sheriff's Department
Los Angeles Terrorism Early Warning
Group

Brian Tishuk

Executive Director
ChicagoFIRST

Kathleen Tolan

Senior Advisor, Canada-US Relations
Infrastructure Assurance Program
Public Safety and Emergency Preparedness
Canada

David A. Trissell

Associate General Counsel, Emergency
Preparedness and Response
US Department of Homeland Security
General Counsel, Federal Emergency
Management Agency (FEMA)

Michael A. Wermuth

Director, Homeland Security Program
The RAND Corporation