RAND
CORPORATION

TESTIMONY

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications
Make a charitable contribution

For More Information

Visit RAND at www.rand.org
Explore RAND Testimony
View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

TESTIMONY

Information Sharing and Emergency Responder Safety Management

BRIAN A. JACKSON

CT-258

March 2006

Testimony presented before the House Government Reform Committee on
March 30, 2006

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RAND
CORPORATION

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Brian A. Jackson[1]
The RAND Corporation

Information Sharing and Emergency Responder Safety Management

Before the Government Reform Committee
United States House of Representatives

March 30, 2006

Mr. Chairman and distinguished Members of the Committee: Thank you for inviting me to participate in today's hearing on this important subject. I should begin by saying that my remarks are principally based on the 2004 published study entitled *Protecting Emergency Responders, Volume 3: Safety Management in Disaster and Terrorism Response*.[2] The study was a joint effort of the RAND Corporation and the National Institute for Occupational Safety and Health. I am therefore drawing both on my own work and that of my co-authors, John Baker, Susan Ridgely, and James Bartis of RAND and Herbert Linn of NIOSH, although the specific content of my remarks today is my responsibility alone.

The focus of the study was on safety management – the processes and capabilities needed to keep responders safe at disaster response operations. Our study examined safety management in both major terrorist attacks and natural disasters. Specifically, we studied the responses to the September 11 attacks, Hurricane Andrew in 1992, and the Northridge Earthquake in 1994. Our work was done in close collaboration with the responder community, including individuals involved in managing the disaster responses we examined.

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] *Protecting Emergency Responders, Volume 3: Safety Management in Disaster and Terrorism Response*, B.A. Jackson, J.C. Baker, M.S. Ridgely, J.T. Bartis, and H.I. Linn, RAND Science and Technology and National Institute for Occupational Safety and Health, MG-170-NIOSH, June 2004, available at: http://www.rand.org/pubs/monographs/MG170/.

Other elements draw on other parts of RAND's research related to emergency and disaster response included in:

Protecting Emergency Responders, Volume 2: Community Views of Safety and Health Risks and Personal Protection Needs, T. LaTourrette, D.J. Peterson, J.T. Bartis, B.A. Jackson, and A. Houser, RAND Science and Technology Policy Institute, MR-1646-NIOSH, August 2003, available at: http://www.rand.org/pubs/monograph_reports/MR1646/, and

Protecting Emergency Responders: Lessons Learned from Terrorist Attacks, B.A. Jackson, D.J. Peterson, J.T. Bartis, T. LaTourrette, I. Brahmakulam, A. Houser, and J. Sollinger, RAND Science and Technology Policy Institute, CF-176-OSTP/NIOSH, March 2002, available at: http://www.rand.org/pubs/conf_proceedings/CF176/.

Safety management is a subset of overall disaster management, so there are strong parallels between what is needed to effectively protect responders and what is needed for an effective response. Many of the lessons from our work relate to information sharing among responding organizations.

Let me begin by stating the central messages from our study that are most relevant to the Committee's interests in this hearing. Our work identified a range of strategies to improve information sharing at disaster response operations. While interoperable technologies at the disaster scene and planning for information sharing are essential, success is driven in large part by the people involved in managing response operations – the "human bridges" among responding organizations – and, as our case studies showed, the necessary bridges are not always in place when disasters occur. Furthermore, the requirements for information sharing must be addressed during preparedness efforts. Building the needed relationships between individuals and organizations so that information can flow is difficult or impossible in the charged and high-pressure atmosphere of an ongoing disaster response. For sharing to occur effectively, the elements must be in place before a disaster occurs.

The Nature of Disasters Drive the Need for Information Sharing

The scale and demands of disasters require the participation of many different response organizations and specialties. Organizations involved in response operations span many professional disciplines – such as emergency management, fire service, law enforcement, emergency medical services, and responders from other government organizations at the local, state, and federal levels. They also frequently include organizations outside of government and from the private sector. For example, published estimates put the number of organizations involved in the 9/11 response at the Pentagon at over 100 and the number involved at the World Trade Center site at over 400.[3] Managing a disaster response effectively requires bringing together the activities of many disparate organizations into a unified effort, and doing so requires the ability to share information among them.

Information sharing is similarly critical for protecting the safety of responders. After a major hurricane, earthquake, or a large-scale terrorist attack, responders face a wide variety of hazards, which can vary from disaster to disaster. Assessing specific hazards and deploying protective measures may require technical specialists that are not present in all responding organizations.

[3] See *Protecting Emergency Responders, Volume 3: Safety Management in Disaster and Terrorism Response*, p. 32 and references therein.

For example, the airborne hazards present at the 9/11 response scenes from the pulverized building materials included a range of hazards that required specialized capabilities to analyze and assess. The uniqueness of post-disaster environments means that many responders may be facing unfamiliar hazards – or at least hazards that are rare in their day-to-day operations – and therefore lack sufficient knowledge to guide their deployment of protective equipment. Information will therefore need to be shared among involved organizations to ensure responders take appropriate protective measures during the response. With respect to responder safety, we refer to this as the need for integrated safety management – where the protective capabilities of all organizations present can be brought together to benefit all the responders involved.

Information Sharing Needs for Protecting Emergency Responders

Effective decisionmaking in disasters relies on having access to the right information at the right time. Though managing overall disaster response has a broader set of information requirements, safety management requires key pieces of information to guide risk management and decisionmaking.[4] Information requirements include:

- *Information about the hazard environment* – Incident commanders and safety managers need to know the hazards responders face, what they mean from a safety perspective, and what can be done about them. If hazard assessment requires specialized technical capabilities, the results of that assessment will need to be shared among responding organizations. When shared, the information needs to be presented in ways that response organizations can act upon it for decisionmaking.

- *Information on the responder workforce* – Incident commanders and safety managers that are making decisions at a disaster scene need to know who is involved in the response and what they are doing. This information is needed to make risk management decisions and, if safety issues arise, locate affected responders so their needs can be addressed. For example, in Hurricane Andrew the large area affected by the disaster and the involvement of many convergent volunteers in the response meant that incident managers had little information on the responders at the scene and their activities. In the absence of central accountability systems for responders, these data are only maintained within individual responder organizations and must be shared to enable coordination of activities at a response.

[4] Similar types of hazard information are also needed to enable decisionmaking about measures to protect members of the public who may be located in or near the disaster scene.

- *Information on evolving safety issues* – If responders who are involved at a disaster are being injured or exposed to hazardous environments, commanders need to know about it. Getting such information rapidly is critical to enable deployment of protective measures. In a number of the cases we examined, including operations at the World Trade Center after the September 11 attacks and Hurricane Andrew, response commanders indicated that data on the injuries suffered by responders at the scene were not collected or were not collected in a way where they could be effectively used to address the safety problems that were causing the injuries. If this information was collected at all, it was generally collected within individual organizations and therefore unavailable to the managers of the overall response. Building a common picture of the hazard environment so action can be taken to protect all responders at a disaster therefore requires sharing such information.

- *Information about safety equipment* – Addressing many safety issues requires the use of specific types of protective equipment. Managing safety effectively therefore requires information on what equipment is available and how to match that equipment to the hazard environment at the disaster. The classic example of this issue is the problems of interoperability of safety equipment – whether replacement cartridges for respirators or batteries for other equipment – that affected responders to the September 11 attacks at both the World Trade Center and the Pentagon.[5] In the wake of a disaster, large amounts of equipment and other resources are frequently sent to the area by many organizations acting independently. Effective information management and sharing about available equipment is critical to match the right resource to a safety need. Without it, responders may not be able to find what they need among the stocks of equipment at an incident scene.

However, successful safety management – and, by extension, disaster management – is not just a point of “more information sharing to everyone at all times.” Responders have different information needs. The overall incident commander or safety manager of a disaster response operation needs strategic level information to make macro-scale safety decisions for the response as a whole. At the tactical level, individual responders need specific information to guide their own protective and operational decisions. Given the demands of a disaster scene, both responders need to be able to find the information they need quickly from the streams of data available to them. Simply having all information flowing to everyone might actually reduce

[5] See *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*, B.A. Jackson, D.J. Peterson, J.T. Bartis, T. LaTourrette, I. Brahmakulam, A. Houser, and J. Sollinger, RAND Science and Technology Policy Institute, CF-176-OSTP/NIOSH, March 2002, available at: http://www.rand.org/pubs/conf_proceedings/CF176/.

the chances that information *needs* will be met if the result of increased sharing is that critical data must be sifted out of a larger background of less immediately relevant information.[6]

Addressing Information Sharing Needs for Safety Management Requires a Combination of Approaches

Information sharing is not just about interoperability and whether specific technologies can talk to one another. Solutions to other shortfalls must focus on how organizations come together and interact in environments where all have their own specific missions while also contributing to a larger, coordinated response effort. Any approach for information sharing must also be able to be implemented rapidly in the wake of a large-scale disaster that could happen with little or no notice, nearly anywhere in the country.

Our study made several specific recommendations to improve information sharing for safety management:[7]

- Specific plans that list the types of information that need to be collected, what organizations should do so, and how the data should be shared.
- Guidelines and standards that indicate what to do with information once it is shared. The fundamental goal is to improve actions that are taken, not just to increase information flowing among organizations.
- Technology tools for information management and collection including databases, accountability systems, logistics systems, and approaches to track injuries or illness among responders.

However, for such policies and tools to actually improve information sharing during disasters, additional actions must be taken *before* disasters occur. Development of plans for information collection and sharing is not enough. These tools must be incorporated into training and preparedness exercises to ensure that, when called upon, they will produce the desired results. Responders we interviewed during our study indicated that safety management is frequently

[6] We have made similar arguments regarding the more specific information sharing issue of communications interoperability – the goal is communication of needed information to the right people, when they need it, and in a way that can be acted upon. If the result of increasing interoperability is "everyone talking to everyone," therefore making actual communication more difficult, the effect on operational effectiveness could be negative rather than positive (see, "Communications Interoperability and Emergency Response," in *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty*, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (The Gilmore Commission), December 15, 2003.)

[7] To place the information sharing recommendations of the study in the context of the other safety management recommendations, we have included the Executive Summary of the report as an Attachment to my written testimony.

given insufficient attention in preparedness exercises, which often focus on the operational elements of response, limiting opportunities to test and practice safety-related information sharing among responding agencies.[8]

Other pre-incident measures – even ones not specifically focused on information sharing – can also reduce the volume and types of information that must be shared during a disaster response. Technology standards are a good example. When pieces of protective equipment and supplies from different manufacturers are incompatible with one another – as was seen for a number of types of equipment in the 9/11 response operations – ensuring that responders have the equipment they need becomes more difficult. Additional information must be shared to track what kinds of equipment are in use, where replacement supplies are available, and how to match them to meet individual responders' needs. Since many different organizations may be involved in managing logistics at a large disaster, this increases the type and amount of information that must be shared among them. Standardized equipment – however that standardization is achieved – eliminates these information sharing requirements.

When an incident occurs, information sharing among organizations more broadly requires that individual groups can "plug into" a common structure and the right people from each organization interact effectively. The National Incident Management System (NIMS) was built on the Incident Command System that came out of the responder community. As such, it provides a common framework for organizations that need to work together during disaster operations. In our work, on responder safety management, we found that NIMS provides an appropriate structure for integrating the safety management efforts of the many organizations involved in a response. But what is not yet in place are the detailed plans – such as those mentioned above – for how, within NIMS, safety information will be shared, especially among responders from local, state, federal, and non-governmental organizations.

Furthermore, while incident management systems define positions and common approaches for organizations, effective information sharing depends on the people that occupy those positions. In our study, emergency responders we interviewed emphasized that the characteristics of the incident commanders and organizational leaders of response operations drive the effectiveness of management and information sharing. They need to know what organizations to reach out to for specific information and must trust those organizations sufficiently that they will act on the information that comes back. The relationships needed to enable information flows are built up

[8] See *Protecting Emergency Responders, Volume 3: Safety Management in Disaster and Terrorism Response*, pp. 85-6.

through operational experience and activities that involve many response organizations, such as metropolitan or regional exercises or preparedness programs.

As a result, the final core recommendation of our study was the need for individuals that could fulfill similar roles for safety management in disaster operations. We labeled these individuals "disaster safety managers" in the report, and a key part of their role would be to act as bridges between organizations for information sharing. The recommendation that individuals be designated to play that role grew out of our conclusion that there was no substitute for effective "human bridges" among organizations to share information and coordinate action. The capabilities suggested for the disaster safety manager included significant management and coordination experience, general knowledge of hazards across the range of possible disasters and response operations, knowledge on safety resources and their availability, knowledge about safety processes and decisionmaking, and preexisting relationships with the organizations likely to become involved in a response if a disaster occurred in that manager's area of responsibility.

Though specific details regarding the recommendation on disaster safety managers are not necessarily germane to a broader discussion of information sharing, there are a few points that are relevant. First, the fact that major disasters are thankfully rare means that few individuals build up all the experience needed to play these roles effectively, even over a career in emergency response. One cannot expect that every response organization will have individuals that can simply step in and do this if a disaster occurs. As a result, we believe there is a need to train individuals to fill these roles. In addition to ensuring that individuals with the right skills are available when a disaster occurs, the training process itself provides a pre-incident information sharing mechanism for relevant lessons-learned to improve future operations. Second, the nature of information sharing needs in disaster operation mean that the individuals playing this role must balance and coordinate in many directions. They must be local enough to have built the connections and relationships with the response organizations in their areas but broad enough to connect with the federal and other national level organizations that will join or support operations. To us, this suggested a model of a small number of individuals – drawn from federal, state, or local response organizations, or some combination thereof – where part of their job function was to build and maintain the connections between organizations to facilitate safety management information sharing in a disaster response.

Conclusions

The effective sharing of information among organizations during a disaster response operation is critical to its success. While interoperable communications and other technologies are one element of effective information sharing, the most critical elements are the “human bridges” that link response organizations. These bridges cannot be built overnight. Development of the necessary human resources and relationships requires significant training and interactions.

It is self-evident that coordinating and drawing on the strengths of all organizations involved will increase the effectiveness of the operational response to a disaster. Similarly, responders are better protected when there is a coordinated safety management effort, rather than relying only the efforts of separate organizations to protect their own members. This is impossible without effective sharing of the necessary information among responding organizations. Improved responder safety therefore represents an added potential payoff to addressing information sharing concerns.

I would like to thank you again for the opportunity to address the committee today, and look forward to answering any questions you might have.