

Free Executive Summary

Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery



Committee on Using Information Technology to Enhance Disaster Management, National Research Council

ISBN: 978-0-309-10396-1, 192 pages, 8.5 x 11, paperback (2007)

This free executive summary is provided by the National Academies as part of our mission to educate the world on issues of science, engineering, and health. If you are interested in reading the full book, please visit us online at <http://www.nap.edu/catalog/11824.html>. You may browse and search the full, authoritative version for free; you may also purchase a print or electronic version of the book. If you have questions or just want more information about the books published by the National Academies Press, please contact our customer service department toll-free at 888-624-8373.

Information technology (IT) has the potential to play a critical role in managing natural and human made disasters. Damage to communications infrastructure, along with other communications problems exacerbated the difficulties in carrying out response and recovery efforts following Hurricane Katrina. To assist government planning in this area, the Congress, in the E-government Act of 2002, directed the Federal Emergency Management Agency (FEMA) to request the NRC to conduct a study on the application of IT to disaster management. This report characterizes disaster management providing a framework for considering the range and nature of information and communication needs; presents a vision of the potential for IT to improve disaster management; provides an analysis of structural, organizational, and other non-technical barriers to the acquisition, adoption, and effective use of IT in disaster; and offers an outline of a research program aimed at strengthening IT-enabled capabilities for disaster management.

This executive summary plus thousands more available at www.nap.edu.

Copyright © National Academy of Sciences. All rights reserved. Unless otherwise indicated, all materials in this PDF file are copyrighted by the National Academy of Sciences. Distribution or copying is strictly prohibited without permission of the National Academies Press <http://www.nap.edu/permissions/> Permission is granted for this material to be posted on a secure password-protected Web site. The content may not be posted on a public Web site.

Summary and Recommendations

Section 214 of the E-Government Act of 2002 called on the Office of Management and Budget, in consultation with the Federal Emergency Management Agency (FEMA), to “ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.” This, the final report from the National Research Council’s Committee on Using Information Technology to Enhance Disaster Management, addresses the issues listed in Section 214 and provides recommendations for enhancing disaster management through the use of IT.¹ In this study, *disasters* are defined as natural, technological, and human-initiated events that disrupt the normal functioning of the economy and society on a large scale; *information technology* (IT) is broadly defined as including computing and communications technology; and *disaster management* is defined as encompassing mitigation, preparedness, response, and recovery efforts undertaken to reduce the impact of disasters.

The purpose of this report is to inform federal, state, and local policy makers and public safety and emergency management professionals about future opportunities for the application of IT to disaster manage-

¹The committee’s first report—National Research Council, *Summary of a Workshop on Using Information Technology to Enhance Disaster Management*, The National Academies Press, Washington, D.C.—was published in September 2005.

ment. Many of the report's recommendations are aimed at the diverse set of federal, state, and local agencies and other organizations (referred to here as disaster management organizations) with responsibility for disaster management activities. Several recommendations indicate what might be done at the federal level to foster IT innovation that would enhance disaster management efforts, but it was beyond the scope of this study to recommend exactly where responsibility for implementing these recommendations should be placed within the federal government. This report is not intended as a comprehensive look at the complex, highly multi-disciplinary topic of disaster management, nor does it explicitly address tradeoffs between investments in IT and other capabilities for disaster management or make recommendations about levels of funding for IT (or indeed other) disaster management activities.

USING INFORMATION TECHNOLOGY AS A POINT OF LEVERAGE TO ENHANCE DISASTER MANAGEMENT

The challenge of disaster management is reducing the harm disasters cause to society, the economy, and the lives of individuals and communities. That task requires disaster managers to reduce uncertainty, to calculate and compare costs and benefits, and to manage resources, often on a much larger scale and at a much faster pace than are supported by methods and means for solving ordinary problems. IT provides capabilities that can help people grasp the dynamic realities of a disaster more clearly and help them formulate better decisions more quickly. And IT can help keep better track of the myriad details involved in all phases of disaster management.

The committee concluded that IT has as-yet-unrealized potential to improve how communities, the nation, and the global community handle disasters. Briefings to the committee suggested that some progress is being made in using IT to enhance disaster management. Presentations made at its June 2005 workshop, additional briefings to the committee, and reports on responses to recent disasters indicated, however, that disaster management organizations have not fully exploited many of today's technology opportunities. This situation stands in contrast to the considerable success enjoyed by some sectors such as financial services and transportation in adopting new IT technologies routinely and aggressively.

This report describes both short- and long-term opportunities to enhance responsiveness and increase resilience by applying IT to disaster management. As in other sectors, successful use of IT involves multiple factors—making smarter use of existing technologies, creating opportunities to develop and adopt new technologies, and evolving organiza-

tional practices to best employ those technologies. Accordingly, this report also examines mechanisms to facilitate the development and effective use of IT.

Short-Term Opportunities to Use IT

Although the committee believes that investment in IT research and development (R&D) for disaster management should be guided in the long run by a comprehensive, stakeholder-driven roadmap (see below), it also sees opportunities for short-term investment in a number of specific areas that would yield significant benefits. The committee heard of many instances in which responders were able to make use of readily available technology—either provided by their organizations or acquired personally—that proved valuable during a disaster. The network effects associated with many of these technologies can create a critical mass of users that provides a potential point of interoperability and cooperation across agencies. For example, ad hoc use of 802.11x wireless capabilities in laptops carried by some first responders, peer-to-peer use of Land Mobile Radio System (LMRS) radios, and use of Family Radio Service/General Mobile Radio Service “walkie-talkies” all can help to provide communications even when the communications infrastructure is damaged. Such technology options may already be in the hands of users but may not be deployed in disasters because policies and procedures for their use are not in place.

Other examples of “low-hanging fruit” include the following:

- Use of sensors, wikis (editable Web sites), blogs, and data-mining tools to capture, analyze, and share lessons learned from operational experiences;
- Use of database, Web, and call center technologies to establish a service to provide information about available equipment, materiel, volunteers, and volunteer organizations;
- Use of planning, scheduling, task allocation, and resource management tools to help in formulating disaster management plans and tracking execution of the plans and to ensure timely recognition of problems and associated follow-up decision making; and
- Use of deployable cell phone technology to rapidly establish stand-alone communications capabilities for use in disasters where local infrastructure is damaged.

To exploit such short-term opportunities involves identifying them, establishing policies and procedures for their use, and providing training to users.

Recommendation 1: Disaster management organizations should take advantage of opportunities for adoption of existing technology or adjustment of policies and procedures that would allow significant short-term enhancement of disaster management.

Key IT-Enabled Capabilities and R&D to Achieve Them

Making good decisions and taking appropriate action during extreme events require having access to communications, data, and computational resources that can be used to effectively coordinate a large number of geographically dispersed participants and assets, to exchange a wide variety of types of information, and to evaluate many scenarios and responses—all of which are changing dynamically.

The committee identified six key areas of IT-enabled capability (described in Box S.1 and discussed in more detail in Chapter 2) in which shorter-term development and longer-term research offer the potential for significant benefits:

- More robust, interoperable, and priority-sensitive communications;
- Better situational awareness and a common operating picture;
- Improved decision support and resource tracking and allocation;
- Greater organizational agility for disaster management;
- Better engagement of the public; and
- Enhanced infrastructure survivability and continuity of societal functions.

Some of these capabilities address rather specialized problems that do not have a large commercial market, although commercial technologies will provide many of the building blocks needed to realize the capabilities. Disasters are low-frequency events outside the normal planning horizons of most organizations, whose structure, operations, and IT systems are designed to ensure day-to-day efficiency rather than the resilience and scalability that disasters demand. As a result, current research and development efforts may not necessarily focus on developing IT capabilities in a manner optimized for disaster management.

As detailed in Chapter 4, IT R&D needs and opportunities are evident across a spectrum from adoption (off-the-shelf technology is available today) to adaptation (the technology is on the horizon and ready for transfer to disaster management) to development (the technology is on the horizon and requires development for use in disaster management) to applied research (disaster-management-specific research is required) to basic research (fundamental research is needed to develop new capabilities).

In government mission areas such as defense and energy, a research infrastructure has been built over decades to ensure long-term, mission-driven scientific and engineering advances—an effort that has included a long history of investments in IT. The Department of Defense, for example, funds a mix of shorter- and longer-term R&D carried out through the Defense Advanced Research Projects Agency (DARPA) and the service laboratories as in-house, university-based, and contract research. These investments are aimed at building a variety of capabilities, such as the military's transition to a capability for network-centric warfare, that are also relevant to disaster management. To make the sort of IT-enabled progress in disaster management that is envisioned in this report, the disaster management community should also devote significant attention and investment to a long-term research program.

A number of agencies could play a role in developing and implementing such a program. The directly relevant mission of the Department of Homeland Security's (DHS's) Science and Technology Directorate is "to protect the homeland by providing Federal and local officials with state-of-the-art technology and other resources."² Other agencies have relevant capabilities in terms of IT and disaster-related research programs, modalities, constituencies, and existing connections with particular research communities, including the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), DARPA, the National Oceanic and Atmospheric Administration (NOAA), and the research laboratories of the armed services.

In a number of federal programs, multiple agencies work jointly to tackle broad problems. One possible model for such an interagency program is the Earthquake Hazard Reduction Program, in which NIST has a lead role and the U.S. Geological Survey (USGS), FEMA, and NSF are participants. Similarly, for disaster management, a lead agency (logically DHS) could provide a clear single point of responsibility, coordinate activities, report on progress, and so forth; the lead agency would not be responsible for all aspects of execution, which would fall to all of the participating agencies and their contractors and grantees.

R&D activities also need to be well coupled to the parts of DHS that are responsible for mitigation, preparedness, response, and recovery activities to ensure that requirements are grounded in operational needs and to ensure that solutions can be transferred into federal operations and the parts of DHS responsible for developing policy to ensure that technological and organizational questions are considered together.

²See http://www.dhs.gov/xabout/structure/editorial_0530.shtm.

BOX S.1 **Key IT-Enabled Capabilities**

- *More robust, interoperable, and priority-sensitive communications.* Disaster management requires robust, priority-sensitive communications systems capable of supporting interoperation with other systems. Providing these requires communication networks that are more resilient to disruption than today's commercial networks, that can last longer without utility power, that can expand capacity to meet emergency needs, that can autonomously reconfigure themselves, that can handle the range of communication needs and environmental conditions that arise in disasters, that have well-defined points of interoperability, and that are able to distinguish between and properly prioritize communications.

- *Better situational awareness and common operating picture.* Situational awareness is the ability for actors in a disaster—from national coordinators to emergency responders to the general public—to have information about an incident, to understand what that information means in the context of the situation and their goals, and to project patterns and trends. The common operating picture is a shared understanding of a situation by a group of people who need to act together to achieve common goals. The aim is to improve a person's ability to do his or her job more effectively.

- *Improved decision support and resource tracking and allocation.* Whereas situation awareness provides decision makers with information relevant to their tasks and goals, decision support focuses on assisting them in formulating prospective actions—helping them understand and assess characteristics and consequences of alternative courses of action and follow-up on decisions, closing the feedback loop from decision to result.

Recommendation 2: The federal government should leverage the capabilities of its agencies to carry out multidisciplinary research in pursuit of six key IT-enabled capabilities—more robust, interoperable, and priority-sensitive communications; better situational awareness and a common operating picture; improved decision support and resource tracking and allocation; greater organizational agility for disaster management; better engagement of the public; and enhanced infrastructure survivability and continuity of societal functions—and establish a coordinating mechanism for those research activities.

Roadmapping as a Tool to Engage Stakeholders and Inform R&D Investments

Until fairly recently, the technology choices facing most disaster management organizations were few, with much of the investment focused on building specialized communications systems in close partnership with

- *Greater organizational agility for disaster management.* The use of IT has enabled and driven changes to organizational structures and processes (e.g., more distributed decision making). Agility is at a premium in disasters because no one type of organization or group of organizations is always best suited for the variety of problems that arise. Related issues with significant IT implications include building rapport among people who do not share a history of cooperation and more quickly integrating the operations of multiple organizations.

- *Better engagement of the public* by (1) supplying information and (2) making use of information and resources that members of the public can supply. Although IT is used today to alert and inform the public before, during, and after a disaster, more use could be made of new communications modalities, and information could be better tailored and targeted to the needs of particular populations. More attention should be paid to the information and resources held by the public because members of the public collectively have a richer view of a disaster situation, may possess increasingly sophisticated technology to capture and communicate information, and are an important source of volunteers, supplies, and equipment. One important factor is how to engage the entire population, given the existence of groups with cultural and language differences and other special needs.

- *Enhanced infrastructure survivability and continuity of societal functions.* Large disasters upset physical infrastructure, such as the electric grid, transportation, and health care—as well as IT systems. IT infrastructures themselves need to be more resilient; IT can also improve the survivability and speed the recovery of other infrastructure by providing better information about the status of systems and advance warning of impending failures. Finally, IT can facilitate the continuity of disrupted societal functions by providing new tools for reconnecting families, friends, organizations, and communities.

a small set of vendors. Today, the set of technologies to choose from is much wider, and many more choices are possible in any particular area. But because disaster management is a system-level problem, there are no IT “silver bullets.” Dramatic improvements in one area of technology or process may have relatively little overall impact unless other interconnected pieces are modified to make use of such advances. Too much invested in radios and not enough in logistics might mean, for instance, that one can call for help but cannot get it.

A clear vision of end-user goals, a detailed understanding of the individual pieces of the problem and their interrelationships, a detailed understanding of the required technologies, and defined paths for progress would help greatly to inform investment decisions. These are among the elements of a roadmap—an agreed-on, coordinated vision that can help organizations to plan development and investment strategies that can bring technologies together at the right time. Roadmaps are used in a number of sectors to accomplish this sort of alignment and cooperation.

A number of stakeholders, including first responders, public safety

and emergency management agencies, government officials, medical providers, volunteer organizations, infrastructure and transportation system owners, vendors, IT researchers, and disaster researchers, have important perspectives on how to build on existing organizations and technology where possible and how to drive the creation of new, cost-effective technologies and organizational structures where needed. However, an institutional home is needed to launch and sustain such activity.

Recommendation 3: The federal government should develop and regularly update an IT R&D roadmap for disaster management with the involvement of a full range of stakeholders.

IMPROVING ACQUISITION AND ADOPTION OF INFORMATION TECHNOLOGY

Adoption of IT for disaster management is challenging for a number of reasons, including the following (which are discussed in more detail in Chapter 3):

- Disaster management organizations often lack the resources to acquire valuable capabilities.
- The development and deployment of many promising technologies are risky and costly given the limited opportunities presented by commercial markets for these technologies.
- In most agencies with disaster management responsibilities, there is no person or unit specifically charged with tracking IT, identifying promising technologies, integrating them into operations, and interacting with IT vendors to make sure needs are addressed.
- Decisions regarding IT tend to be made independently by local organizations that must work together in disasters.
- Disaster management is concerned with environments that are intrinsically uncertain and unstable.
- Important sources of funds are typically only available once a disaster has been declared and also must be spent in a short time window.

Diversified Acquisition Strategy and Attention to Design Issues

Disaster management has traditionally relied heavily on specially built technology and on a traditional “waterfall” acquisition model in which a full set of specifications is developed and a vendor is selected to build a system in compliance with the specifications. In the commercial world and in sectors such as defense, there is growing acceptance of a richer, more diversified acquisition strategy that employs a mix of tradi-

tional (purpose-built) systems, adoption and adaptation of commercial off-the-shelf (COTS) technology and services, and use of open source software, open standards, and community-driven development approaches. Such a strategy for disaster management should draw on the strengths of the traditional vendor community yet also foster bottom-up development as a complement to traditional acquisition practices and more formal top-down development; tap the nation's technology base; and also encourage the "can-do" spirit of commercial developers, professionals, and volunteers involved in disaster management.

As mentioned above, COTS technology alone is unlikely to deliver all of the desired capabilities. But it is important in two ways—(1) adoption and adaptation of readily available technologies offer a path for building up disaster management capabilities in the short term, and (2) the interoperability often characteristic of COTS technologies makes them useful as building blocks for disaster management systems.

Recommendation 4: Federal, state, and local agencies should embrace a diversified acquisition strategy that includes increased use of commercial information technology and greater use of open source software and open standards development as a complement to more traditional acquisition approaches.

Reliance on turn-key systems has meant that disaster management organizations have paid less attention to the underlying design issues that ultimately affect the functionality of their IT systems. Often technologies have been acquired as stand-alone products with little consideration for how they integrate with other technologies already in use, even within the same agency. However, with networking becoming increasingly pervasive, careful attention should be given to how each particular IT system fits into the broader context of interconnected systems. Off-the-shelf technology such as desktop computers or network routers can provide basic building blocks, and some elements of design are also well established such as the Internet Protocol standard for packet networks, but a domain-specific architecture understood and owned by the organization is also needed. To accomplish this, organizations have to develop the necessary technical and technology management capabilities.

Recommendation 5: Disaster management organizations should work closely with technology providers to define, shape, and integrate new technologies as a coherent part of their overall IT system.

The committee believes that more can be done to embrace proven approaches for IT acquisition. Best practices for acquisition include an

emphasis on iterative development, increased opportunities to test and evaluate technology in practice together with realistic concepts of operations, and design and evaluation processes that allow for strong coupling among practitioners, researchers, and industry.

The committee also identified four design principles (discussed in more detail in Chapter 3) that have particular importance for disaster management systems:

- Build emergency management systems for effective scaling from routine to disaster operation;
- Exploit redundancy and diversity to achieve resilience;
- Design systems with flexibility, composability, and interoperability as core guiding principles; and
- Distinguish between the user interface and the underlying technologies used to deliver a capability.

Training and Practice Through Routine Use of IT

Unless experience is gained through routine use or regular training, the full benefits of investment in IT systems are unlikely to be realized. Training, drills, and exercises all play an important role in the introduction of new technologies into organizational practice. Moreover, it is through routine use that the competence and confidence required to successfully use a technological capability, especially in the high-stress situation of disasters, are best developed. However, training large numbers of people to deal with infrequent events poses logistical challenges and is also costly.

Recommendation 6: In the design, acquisition, and operation of IT systems, disaster management organizations should emphasize the incorporation of disaster response capabilities into the systems that support routine operations.

Measurement and Assessment to Enhance Effectiveness

As the saying goes, one can only manage what one can measure. Because the resources available for disaster management are limited, decision making always involves tradeoffs. Weighing the benefits from particular IT investments against the returns on other sorts of investment is challenging. Although having measures of effectiveness is necessary to making such assessments, few applicable metrics are currently available.

Above all, acquisition of IT and associated organizational changes

should be driven by a focus on improving the effectiveness of those whose actions are integral to effective disaster management. The emphasis should be on measuring the resulting net effectiveness of disaster management activities, not the performance of the IT per se. For example, rather than focusing on the performance of particular systems (e.g., a firefighter radio system has 90 percent coverage), it is important to try to gauge net effectiveness (e.g., better communications coverage allows firefighters to better coordinate their response, improving capabilities for fighting forest fires by 20 percent). The development of such metrics is an area for further research.

Recommendation 7: Disaster management organizations should employ metrics to inform cost-benefit decisions for investment in IT for disaster management and should make enhanced end-user performance a primary objective of disaster management acquisition programs.

Independent mechanisms for assessment, such as the Transportation Safety Board, the U.S. Chemical Safety and Hazard Investigation Board, and the NASA Aviation Safety Reporting System, have proven useful in their respective domains. A critical requirement of these organizations is their independence from the agencies that have operational responsibilities. It may be advantageous to employ several organizations rather than a single national one, with each one focusing on a particular type of disaster or the range of disasters typical in a particular region. It is also important for assessments to be founded on multiple areas of expertise, including technical, social, and organizational dimensions. Obviously, the effectiveness of IT use is just one facet of an assessment of the overall effectiveness of disaster management activities for any particular incident, albeit an important one.

Recommendation 8: Disaster management organizations should make use of independent mechanisms for assessing the effectiveness of disaster management operations, including the use of IT, and for disseminating lessons learned and best practices.

Systematic Collection of Data

It is well understood as a result of endeavors in many areas (e.g., aircraft accident investigations) that making significant improvements depends on putting in place processes that allow learning from experience. IT can play a critical role in enhancing the science of disaster man-

agement by helping to support continuous improvement. Collecting adequate and trustworthy data is essential for the feedback necessary to drive improvements in disaster management.

Doing so requires better documentation of disasters and the responses to them, including the role of supporting technology. The widespread introduction of IT into disaster management provides opportunities for large-scale, automated, comprehensive collection of data about operations, decision making, and situational knowledge throughout a disaster. This information can be processed after the fact to improve understanding of the process of disaster management. IT can also help to make these lessons learned available in real time, putting them into the hands of decision makers when they are most needed.

Accomplishing this goal requires enhanced technical capabilities to capture data during the course of a disaster. In some cases, it may be necessary to find ways to anonymize data so that accurate statistics can be gathered without the difficulty of dealing with potential liability issues. Policy changes (analogous to the adoption of Good Samaritan laws³) may also be needed to ensure that individuals involved in a disaster response can be protected from liability (e.g., amendments to the Health Insurance Portability and Accountability Act [HIPAA] may be needed). Legislation may also be needed to ensure that intellectual property, privacy, liability, and other concerns of information providers are addressed if they are required to share such data for research purposes.

COUPLING RESEARCH AND PRACTICE

Effective development, use, and deployment of IT depend on a solid understanding of context and user needs. Moreover, the introduction of new IT often presents opportunities for new organizational approaches, and these opportunities should be considered in reorganization efforts. Similarly, successful technology development requires consideration of organizational context.

This issue of co-development of technology and organizational practice seems especially important at present. In the wake of Hurricane Katrina, a number of organizational structures, policies, and procedures are being examined. Also, a number of relevant technologies have reached a sufficient level of maturity to allow innovative organizational approaches to disaster management.

The interdependence of technology and practice suggests that developing a cadre of people with expertise in both disaster management and

³Good Samaritan laws shield people from liability in emergency circumstances provided that they have acted in a reasonable manner.

IT is likely to yield significant payoffs. Such a cadre of people is likely to be more astute at translating user requirements to technical needs. One basic need, of course, is to train a group of first responders and others responsible for disaster management in IT skills that go beyond those of a general user and to train a group of IT workers (e.g., database and system administrators and application builders) to have domain expertise in disaster management. Deeper expertise spanning both domains could be fostered through a number of mechanisms, including the following:

- A combination of fellowships, shorter-term visits to research centers, and other training and educational activities that help technology experts and other practitioners to stay abreast of the latest developments in both practice and technology;
- Field tests and field work conducted by IT researchers working with disaster management practitioners; and
- Combined disaster management-IT expert teams that jointly analyze the performance of processes and systems after a disaster.

Recommendation 9: Disaster management organizations should support the development of a cadre of people with expertise in both disaster management and IT.

Especially in light of the significant non-technical factors affecting adoption of IT for disaster management, it is critical to establish mechanisms that ensure that researchers are exposed to real problems and that practitioners are exposed to new technology opportunities. Because most practitioners are distributed across local agencies, forging such ties is likely to be harder in disaster management than in sectors like defense, but it is no less important.

Collaborative research centers could bring together experts from diverse domains in a neutral environment conducive to collaboration. Such centers could (1) develop a shared understanding of the challenges in all phases of disaster management from both a technological and an organizational perspective, (2) evaluate the application of technology advances to disaster management practice, (3) develop a culture and processes for transitioning knowledge and technology to the operational communities on a sustained basis, (4) build human capital at the intersection of IT and disaster management, (5) serve as repositories for data and for lessons learned from past disasters and disaster management efforts, and (6) provide forward-looking analysis to inform the development of technology capabilities, associated organizational processes, and roadmap development. A number of academic centers exist that offer a capacity for at least some of these efforts.

Practitioners in multiple disciplines could contribute to such centers, including scientists, engineers, and hazard and disaster researchers, and centers should include partnerships with federal, state, and local disaster management agencies. Indeed, it is critical that experienced and capable officials and operational elements of disaster management organizations be deeply involved in the work of these centers. One approach for engaging these groups would be to provide incremental funds to agencies specifically for working with researchers and developing next-generation technologies. Having multiple centers (rather than a single entity) also helps to ensure healthy intellectual competition, cross-fertilization of ideas, specialization in specific types of disasters and specific technology capabilities, and attention to the comprehensive needs of particular geographical areas.

Research centers could also act as a resource for agencies seeking to implement a diversified acquisition strategy and incorporate the latest best practices and a mechanism for disaster managers and responders to share experiences and communicate requirements to guide further technology developments.

Recommendation 10: The federal government should sustain (and develop as needed) a network of research centers where IT researchers, hazard and disaster researchers, and disaster management practitioners can collaborate to study and evaluate the use of IT for disaster management from both a technological and an organizational perspective, to transition knowledge and technology to those who practice disaster management, to build human capital at the intersection of IT and disaster management, and to develop future IT capabilities.

IMPROVING DISASTER MANAGEMENT

THE ROLE OF **IT** IN MITIGATION, PREPAREDNESS,
RESPONSE, AND RECOVERY

Ramesh R. Rao, Jon Eisenberg, and Ted Schmitt, *Editors*

Committee on Using Information Technology to
Enhance Disaster Management

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by the Battelle Memorial Institute under subcontract number 189936 to a contract between the Federal Emergency Management Agency and the Battelle Memorial Institute. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations and agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-10396-1

International Standard Book Number-10: 0-309-10396-7

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, <http://www.nap.edu>.

Copyright 2007 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON USING INFORMATION TECHNOLOGY TO ENHANCE DISASTER MANAGEMENT

RAMESH R. RAO, University of California, San Diego, *Chair*
YIGAL ARENS, University of Southern California
ART BOTTERELL, Contra Costa County, California, Office of the Sheriff
TIMOTHY X. BROWN, University of Colorado, Boulder
JOHN R. HARRALD, George Washington University
RICHARD HOWARD, Rutgers University
NANCY JESUALE, NetCity Engineering, Inc.
DAVID KEHRLEIN, Environmental Science Research Institute
WILLIAM MAHEU, San Diego, California, Police Department
ROBIN R. MURPHY, University of South Florida
ROBERT NECHES, University of Southern California
MASANOBU SHINOZUKA, University of California, Irvine
ELLIS STANLEY, City of Los Angeles
PETER STEENKISTE, Carnegie Mellon University
GIO WIEDERHOLD, Stanford University

Staff

JON EISENBERG, Study Director
TED SCHMITT, Program Officer
DAVID PADGHAM, Associate Program Officer
GLORIA WESTBROOK, Senior Program Assistant (through December
2006)
JENNIFER M. BISHOP, Program Associate

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

JOSEPH F. TRAUB, Columbia University, *Chair*
ERIC BENHAMOU, Benhamou Global Ventures, LLC
FREDERICK R. CHANG, University of Texas, Austin
WILLIAM DALLY, Stanford University
MARK E. DEAN, IBM Almaden Research Center
DAVID J. DEWITT, University of Wisconsin, Madison
DEBORAH ESTRIN, University of California, Los Angeles
JOAN FEIGENBAUM, Yale University
KEVIN KAHN, Intel Corporation
JAMES KAJIYA, Microsoft Corporation
MICHAEL KATZ, University of California, Berkeley
RANDY H. KATZ, University of California, Berkeley
SARA KIESLER, Carnegie Mellon University
TERESA H. MENG, Stanford University
PRABHAKAR RAGHAVAN, Yahoo! Research
FRED B. SCHNEIDER, Cornell University
ALFRED Z. SPECTOR, Independent Consultant, Pelham, New York
WILLIAM STEAD, Vanderbilt University
ANDREW J. VITERBI, Viterbi Group, LLC
PETER WEINBERGER, Google, Inc.
JEANNETTE M. WING, Carnegie Mellon University

JON EISENBERG, Director
KRISTEN BATCH, Associate Program Officer
RADHIKA CHARI, Administrative Coordinator
RENEE HAWKINS, Financial Associate
MARGARET MARSH HUYNH, Senior Program Assistant
HERBERT S. LIN, Senior Scientist
LYNETTE I. MILLETT, Senior Program Officer
DAVID PADGHAM, Associate Program Officer
JANICE SABUDA, Senior Program Assistant
TED SCHMITT, Program Officer
BRANDYE WILLIAMS, Program Assistant
JOAN WINSTON, Program Officer

For more information on CSTB, see its Web site at <http://www.cstb.org>, write to CSTB, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, call (202) 334-2605, or e-mail at cstb@nas.edu.

Preface

To improve how information technology is used in disaster management, Section 214 of the E-Government Act of 2002 called on the administrator of the Office of Electronic Government in the Office of Management and Budget, in consultation with the Federal Emergency Management Agency (FEMA), to “ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters” (see Box P.1). In early 2005, in response to a request from FEMA to the National Research Council (NRC), via a contract with Battelle Memorial Institute, the Committee on Using Information Technology to Enhance Disaster Management was established under the auspices of the Computer Science and Telecommunications Board to study these issues. The committee’s first report, *Summary of a Workshop on Using Information Technology to Enhance Disaster Management*,¹ summarized the discussions at a public workshop held on June 22-23, 2005. Representatives of federal, state, and local government agencies; private industry; and the research community participated in the workshop.

Over the next year the committee met four times and made several site visits to gather input from federal agencies; state and local public

¹National Research Council, *Summary of a Workshop on Using Information Technology to Enhance Disaster Management*, The National Academies Press, Washington, D.C., September 2005.

BOX P.1
Section 214 of the E-Government Act of 2002,
Public Law 107-347

SEC. 214. ENHANCING CRISIS MANAGEMENT THROUGH ADVANCED INFORMATION TECHNOLOGY

(a) PURPOSE.—The purpose of this section is to improve how information technology is used in coordinating and facilitating information on disaster preparedness, response, and recovery, while ensuring the availability of such information across multiple access channels.

(b) IN GENERAL.—

(1) STUDY ON ENHANCEMENT OF CRISIS RESPONSE.—Not later than 90 days after the date of enactment of this Act, the Administrator, in consultation with the Federal Emergency Management Agency, shall ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.

(2) CONTENTS.—The study under this subsection shall address—

(A) a research and implementation strategy for effective use of information technology in crisis response and consequence management, including the more effective use of technologies, management of information technology research initiatives, and incorporation of research advances into the information and communications systems of—

(i) the Federal Emergency Management Agency; and

(ii) other Federal, State, and local agencies responsible for crisis preparedness, response, and consequence management; and

(B) opportunities for research and development on enhanced technologies into areas of potential improvement as determined during the course of the study.

(3) REPORT.—Not later than 2 years after the date on which a contract is entered into under paragraph (1), the Administrator shall submit a report on the study, including findings and recommendations to—

(A) the Committee on Governmental Affairs of the Senate; and

(B) the Committee on Government Reform of the House of Representatives.

(4) INTERAGENCY COOPERATION.—Other Federal departments and agencies with responsibility for disaster relief and emergency assistance shall fully cooperate with the Administrator in carrying out this section.

(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for research under this subsection, such sums as are necessary for fiscal year 2003.

(c) PILOT PROJECTS.—Based on the results of the research conducted under subsection (b), the Administrator, in consultation with the Federal Emergency Management Agency, shall initiate pilot projects or report to Congress on other activities that further the goal of maximizing the utility of information technology in disaster management. The Administrator shall cooperate with other relevant agencies, and, if appropriate, State, local, and tribal governments, in initiating such pilot projects.

safety officials and emergency management practitioners; experts in disaster management; information technology researchers; and hardware and software vendors. In preparing this, its final report, the committee also drew on perspectives and information gleaned from professional conferences, the technical literature, and government reports.

Chapter 1 briefly characterizes disaster management, placing the use of information and communication technology in the broader human and organizational context and providing a framework for considering the range and nature of information and communication needs. Chapter 2 presents the committee's vision of the potential for information and communication technology to improve disaster management. Chapter 3 focuses on structural, organizational, and other non-technical barriers to the acquisition, adoption, and effective use of IT in disaster management. Chapter 4 provides an initial outline of the elements of a research program aimed at strengthening IT-enabled capabilities for disaster management.

During the development of this report, Hurricane Katrina struck the U.S. Gulf Coast. In the days following the hurricane's landfall, damage to the communications infrastructure, together with a host of other communications and information concerns, was cited by decision makers and reported on in the press as among the major challenges facing those involved in response and recovery efforts. The tragic events that occurred in Katrina's wake have, of course, served to underscore the importance of disaster management; they have also highlighted the role of information technology in disaster management, the interplay between technical and organizational considerations, and the contributions that research and development in these areas could make to future disaster management activities. However, although a number of the inputs focused on Katrina, the committee's charge, its deliberations, and this report encompass disasters in all (natural and human-made) forms and in all phases, from mitigation and preparedness to response and recovery.

Ramesh R. Rao, *Chair*
Committee on Using Information Technology
to Enhance Disaster Management

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

David Borth, Motorola,
Thomas J. Cowper, New York State Police,
Sharon Dawes, University at Albany, State University of New York,
Otto Doll, State of South Dakota Bureau of Information and
Telecommunications,
Mica Endsley, SA Technologies,
Al Flax, Consultant, Potomac, Maryland,
W. Craig Fugate, State of Florida Office of Emergency Management,
Sara Kiesler, Carnegie Mellon University,
Prabhakar Ragahvan, Yahoo!,
Eric Rasmussen, U.S. Navy Medical Corps,
Myra Socher, TriMed, Inc.,
Kathleen Tierney, University of Colorado, Boulder, and
Charles Werner, Charlottesville, Virginia, Fire Department.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Samuel H. Fuller, Analog Devices, Inc., and Richard N. Wright, National Institute of Standards and Technology (retired). Appointed by the National Research Council, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

SUMMARY AND RECOMMENDATIONS	1
1 INTRODUCTION AND CONTEXT	15
2 THE POTENTIAL TO ENHANCE DISASTER MANAGEMENT: KEY IT-BASED CAPABILITIES	34
3 IMPROVING ACQUISITION AND ADOPTION OF IT FOR DISASTER MANAGEMENT	68
4 ELEMENTS OF A RESEARCH AGENDA	108
APPENDIXES	
A Illustrative Fictional Narratives of IT Use in Disaster Management	135
B Review of Interoperability Initiatives	151
C Workshop Agenda	157
D Speakers and Participants at Meetings and Site Visits	165
E Biographies of Committee Members and Staff	167

