Summary of a Workshop on Using Information Technology to Enhance Disaster Management

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

ISBN: 0-309-65436-X, 40 pages, 8 1/2 x 11, (2005)

Summary of a Workshop on Using Information Technology to Enhance Disaster Management

Committee on Using Information Technology to Enhance Disaster Management

Computer Science and Telecommunications Board

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 Battelle Memorial Institute under subcontract number 189936 to a contract between the Federal Emergency Management Agency and 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 0-309-10037-2 (Book)
International Standard Book Number 0-309-65436-X (PDF)

Cover designed by Jennifer M. Bishop.

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.

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

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

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 the CSTB at cstb@nas.edu.

Preface

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" (Box P.1). The section cited as a goal "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." In early 2005, FEMA, via a subcontract through Battelle Memorial Institute, asked the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) to undertake a two-phase study on these issues.

This report culminates phase 1 of the project. CSTB established the Committee on Using Information Technology to Enhance Disaster Management, and a public workshop was held under the committee's auspices on June 22-23, 2005. A variety of representatives of federal, state, and local government agencies, private industry, and the research community participated. The workshop agenda is given in Appendix A. Appendix B includes biographical information for committee members and staff.

The committee's goal for the workshop was to establish a base of information for its study by hearing about present and future uses of IT from the perspective of federal, state, and local disaster management officials and users together with a sampling of relevant IT research and development activities. Panelists at the workshop were given roughly 15 minutes to provide their views on a set of questions (listed by panel or topic in Appendix A) posed in advance regarding the use of information technology to enhance disaster management. They presented a range of views on the present state of the art and practice and future opportunities to harness information technology to aid in the management of natural and human-made disasters. The slides (unedited and unreviewed by the NRC) prepared by many of the speakers for use in their presentations are available from CSTB's Web site at http://www.cstb.org.

This report summarizes some of the key points made by workshop participants. In phase 2 of its study, the committee will supplement the inputs received at the workshop with information gathered at several site visits and a series of additional briefings. Phase 2 will culminate in a final report, expected in spring 2006, that provides findings and recommendations on requirements for effective use of information technology for disaster management, research and development needs and opportunities, and related research management and technology transition considerations.

The committee thanks all of the workshop participants for their thoughtful presentations

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.

and discussion, as well as FEMA for sponsoring the workshop, and it extends special thanks to Chip Hines at FEMA for all his help in making this project possible.

While this report was being completed, Hurricane Katrina struck the Gulf Coast of the United States. 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 occurring in Katrina's wake underscore the importance 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 preparedness and response.

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:

Otto Doll, Bureau of Information and Telecommunications, State of South Dakota,
Deborah Estrin, University of California, Los Angeles, and
William "Al" Wallace, Rensselaer Polytechnic Institute.

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 Craig Partridge, BBN Technologies. Appointed by the National Research Council, he was 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 of Remarks Made by Workshop Participants

On June 22-23, 2005, CSTB's Committee on Using Information Technology to Enhance Disaster Management held a workshop in Washington, D.C., to obtain perspectives on the use of information technology (IT) [1] to enhance the management of natural and human-made disasters. Workshop participants invited as panelists included federal program managers and researchers, state and local officials and first responders, representatives from industry, and academic researchers from a variety of disciplines. In addition to providing perspectives on the current state of the art and practice, workshop presenters also described future opportunities to make better use of information technology to improve disaster management.[2]

This report provides the committee's summary of key points made by workshop participants. It does not aim to present comprehensively all the remarks made during the workshop. Reflecting the workshop's structure, this summary is organized to cover three major topic areas:

1. The critical and evolving role of information technology in disaster management,
2. Research directions for information technology in disaster management, and
3. Collaboration, coordination, and interoperability: pressing issues in a need-to-share world.

Each topic area was covered by two or more panels. Highlights of the comments made by speakers in each topic area are provided in the sections that follow.

One important issue that cut across all three topic areas is the capability for wireless communication, which plays a critical role in disaster management because in almost all situations, first responders will depend on wireless links. As discussed below under Topic 2, there are fundamental constraints to wireless communication, significant unsolved problems, and a number of areas of active research. As discussed below under Topics 1 and 3, enhancing interoperability among current and future wireless systems is also widely recognized as a pressing issue in disaster management and is the subject of a number of current initiatives.

[1] IT is used as a shorthand in this report to cover both computing and communications capabilities. It should be understood in the context of this report as synonymous with the term information and communications technology, which appears at several places in the workshop program.

[2] The workshop agenda, including questions posed in advance for the panelists, is given in Appendix A.

TOPIC 1: THE CRITICAL AND EVOLVING ROLE OF INFORMATION TECHNOLOGY IN DISASTER MANAGEMENT

Three panels discussed lessons learned about the effective use of IT in disaster management, technological and organizational barriers to the introduction and adoption of new IT systems, and types of IT that could be of particular use in disaster management.

Panelists made a number of points characterizing the challenges of providing more interoperable communications for disaster management across federal, state, and local agencies:

- Most communications interoperability issues are not technical. Better human organization, willingness to cooperate, and a willingness of government at higher levels to listen to those at local levels who really do the work and who are the actual responders are all critical factors in making better use of information technology for disaster management.
- Adoption of new equipment and systems that provide greater interoperability will take a long time. A speaker estimated at more than $60 billion the total amount invested by localities in their public safety communications infrastructure. Such an investment can be replaced only over decades.

Discussing the federal role in improving interoperability, panelists observed that:

- Disaster management—and the supporting IT infrastructure—is firmly rooted at the local level. Local organizations provide most of the infrastructure, personnel, and other resources. More than 90 percent of wireless public safety infrastructure is owned, operated, and maintained by localities. A speaker estimated that the total federal investment in interoperable communications represents something less than 3 percent of what the nation spends on public safety wireless communications. Local first responders make up the vast majority of day-to-day users. Even in an event on the scale of the September 11, 2001, attacks on New York City and the Pentagon, the federal presence, which was massive by normal standards, represented a fraction of 1 percent of all personnel involved. By virtue of their primary responsibility and reflecting long-standing organizational culture, localities and their police and fire services have, and generally seek to maintain, control of their communications systems.
- As a result, the federal role in improving interoperability is limited largely to providing guidance, coordination, and technical assistance. The federal government could, for example, provide a road map, a policy framework, and an architectural framework to create a system of systems. It could also support initiatives that motivate local agencies to move toward standards-based systems. A number of federal programs, including the Department of Homeland Security's SAFECOM, are aimed at providing such support.
- Federal interoperability activities are diverse and themselves require coordination. For example, the Homeland Security Act identifies no less than three separate agencies as responsible for aspects of interoperability. Indeed, more than 60 programs deal with interoperability across the federal government. The Department of Homeland Security's Office for Interoperability and Compatibility has created an umbrella program to coordinate these federal interoperability efforts. Interagency efforts are also underway to address the need for coordination. Still needed are a road map and a more coherent policy framework within which federal agencies can work together.

Commenting on activities at the state and local level, panelists noted that:

- Interoperability and coordination issues are also evident at the state level. A number of states have developed statewide communications interoperability plans, but many thus far involve only the state police.
- Localities have begun to recognize the need to better coordinate planning and communications. This work began in the 1990s and was accelerated by the events of September 11, 2001.

A panelist also noted that interoperability and coordination issues also arise in the context of public alert systems. The technology may exist today to create an all-hazards warning system, but fragmented responsibility and lack of coordination would likely lead to inconsistent messages and/or overly broad messages instead of the desired authoritative and targeted warnings.

Several speakers pointed to standards in areas such as syntax (the organization and structure of data) and semantics (the meaning of the data) for representing, storing, and transferring information as critical to better use of IT in disaster management, noting that:

- Standards ease interoperability and can foster increased information exchange and help lower costs.
- Even good standards will have to be changed as circumstances evolve, which places a premium on processes and methods that tolerate extensibility and both incremental and rapid change.
- The lack of common semantics is a huge inhibitor for more effective use of IT.[3] The issue of data semantics boils down to the problem of reconciling terminology used by different organizations and systems so that data can be properly integrated. Different first-responder communities (e.g., fire protection, medical services, law enforcement) as well as different levels of government have different names for the same things or different definitions for the same terms. Semantics can also be different among neighboring jurisdictions, creating additional impediments to communications and information sharing.
- Implementing standards broadly is a slow process, given the time it takes to build consensus among the relevant communities and the resources and planning required to replace legacy systems.
- There are opportunities to build momentum for adoption of standards as localities seek to reduce costs by pooling resources with regional neighbors.
- One effective approach to bridge-building among systems and communities is to use a distributed architecture that is glued together by common semantics.

Several comments by panelists addressed the importance of coordinated information technology planning and acquisition to achieve greater interoperability and better-integrated disaster management capabilities:

- As jurisdictions upgrade their technology to fulfill their own acquisition plans, a stair-stepping effect occurs, with the result that localities' systems are frequently incompatible with their neighbors' systems. Overcoming the effects of these mismatches requires better-coordinated and synchronized acquisition cycles.
- Strategic planning on a multi-jurisdictional, cross-agency basis eases the burden on individual jurisdictions and agencies by giving them a common framework within which

[3] A reviewer of this report in draft form cautioned, however, that one should not expect semantic problems to be resolved by significantly changing the behaviors of individual communities and that one should instead expect IT systems to adapt to this reality.

to identify particular technologies that would be able to meet their individual requirements and would also be interoperable with the technologies of other communities and agencies.

- Localities are increasingly working together in regional organizations to leverage expertise, improve training and planning, and coordinate technology acquisition. Effective examples of such coordination cited by speakers include the Automated Regional Justice Information System for the San Diego region and activities under the auspices of the Metropolitan Washington Council of Governments.

Panelists offered several observations about the impacts of new IT on disaster management.

- Responders and emergency managers should focus on the goals to be achieved rather than on acquiring and using technology for its own sake.
- New IT capabilities can have a major impact by changing how information is used in a disaster. For example, systems that are architected appropriately could allow decision makers at the local level to directly access (pull) the information they seek rather than having to depend on (sometimes inappropriate) information being pushed to them.

Regarding successful introduction and adoption of new information technology, the panelists noted the following issues:

- To be useful in a disaster, IT must be in routine use. In a crisis situation, people tend to fall back on what they are comfortable with. Technology that is not included in planning, training, exercises, and standard operating procedures will not be used in an actual disaster. Similarly, it is also important to use during routine operations those systems and procedures that would be needed in a crisis.
- The rate at which IT changes continues to outpace the rate at which public safety organizations are adapting to it. In a number of instances visionary leadership has helped overcome the political, economic, and organizational challenges, but these are the exception, not the rule.
- The location of a jurisdiction's emergency management agency within its government structure varies widely and affects what aspects of emergency management are emphasized and how successfully a jurisdiction acquires and adopts IT.
- First responders and emergency managers must be able to rely on the technology they use to accomplish their work. As a result, they are very reluctant to depend on commercial infrastructure such as the public switched telephone network or cellular telephone systems, which historically have become very congested or collapsed quickly after major disasters.
- Being at the cutting edge in the use of IT is widely understood to have a number of drawbacks, including higher up-front acquisition costs, greater resources required to customize software and systems, and a tendency to customize systems beyond what is necessary.
- The cost of new technology is a major inhibitor of its adoption. The public safety community is primarily dependent on local revenue, which must also cover such local needs as education and roads.
- Life-cycle costs, including the ongoing expense of maintenance, training, and operations, should be factored in from the beginning and understood by all involved.
- The integration and deployment of technology should not be a one-shot event. Rather, it should be an iterative, ongoing process that involves all stakeholders, especially first

responders.

- Creating a feedback loop among those who use, acquire, implement, and develop technology is critical to both the development of useful capabilities and their successful adoption. Exercises, drills, live simulations (such as those employed by the military), and shadow operations (such as those conducted in conjunction with the 2003 Super Bowl in San Diego) help build the user community's confidence and trust in the technology and also provide essential feedback to technology developers and providers on actual user requirements and how existing technologies could be improved.

In addition, speakers noted several practical challenges to introducing new technologies:

- Making updates to IT systems can be difficult. For example, technical barriers (such as limited wireless bandwidth that constrains over-the-air updates) and logistical challenges (such as scheduling appointments to update systems) can complicate the process of updating maps and other large databases deployed in the field.
- Training responders to use new technologies presents significant challenges. Responders must be taken away from their daily duties, and motivating them to receive training can be hard, especially when responders do not see an immediate practical use for the training or technology.
- Incident reporting systems and other systems that collect field data provide useful information for developing future technology as well as assessing current technologies and operations. However, the data provided by responders is sometimes of little or no value. Responders who do not see a connection between data and practical results are unlikely to invest the effort to ensure that the data entered is complete, accurate, and timely.
- The introduction of new information technology that makes users' actions more readily observed or recalled raises concerns regarding exposure of those users to legal liability or to the professional risk of being second-guessed.

Panelists offered several comments regarding the growing use of data (in addition to voice) communications in disaster management:

- Systems that allow data to be accessed from the field are valuable in a number of settings. For example, access to effective directories of information could enhance the decision-making capabilities of first responders.
- Visual data such as pictures, video, and maps are increasingly complementing and being integrated with voice and text data.
- However, reliable voice communications are, and will continue to be, the unequivocal highest priority for the public safety community. For the firefighter entering a burning building or a police officer in a high-speed pursuit, for example, entering text or reading a screen would be distracting and dangerous.
- Wider adoption and use of data services will require cultural change. This process has already begun, as exemplified by police officers' common use of mobile data terminals in patrol cars.
- Wider use of data communications will create new interoperability challenges relating to protocol, syntax, and semantics that go well beyond those associated with voice communications.

Several panelists underscored the importance information technology for improved situational awareness and command and control, which were characterized as force multipliers

that would greatly improve what could be done with limited resources. They noted that:

- The importance of better situational awareness is illustrated by the observation that responders run the risk of becoming casualties themselves because they do not know enough about an incident scene when they arrive.
- A variety of situational awareness initiatives have been undertaken by various organizations. For example, the U.S. military has a long history of investment in information technology capabilities to provide situational awareness. The U.S. Forest Service's Situation Awareness Firefighting Equipment (SAFE) program—which includes wearable computer, wireless communications, global positioning satellite, night vision, and software components—is another example.

Several panelists also discussed opportunities to employ sensors and other surveillance capabilities for disaster management. Their observations included the following:

- Sensor systems provide new opportunities to detect hazards and gather other vital information in a disaster.
- The widespread availability and use of open, Internet Protocol-based technologies makes it easier and cheaper to link already deployed sensors such as video cameras.
- Surveillance capabilities raise privacy and civil liberties concerns that those deploying these technologies will need to carefully address.
- Better sensors and better detection, analysis, and filtering technologies do not, however, obviate the need for humans to be in the loop. Indeed, it is generally believed that only humans, not IT systems, should issue warnings or take similar actions in a disaster.

Panelists also noted that existing and potential future technologies can improve the ability of responders to act in hostile environments and to extend where and when they can operate. For example, better sensors and IT systems that make use of them could aid night operations and urban search and rescue.

TOPIC 2: RESEARCH DIRECTIONS FOR IT IN DISASTER MANAGEMENT

Five panels discussed current research programs and potential directions for new research in information technology. Commenting on the nature of those efforts and describing lessons learned, several speakers made the following observations:

- IT research for disaster management is of an applied nature, reflecting challenges unique to the application and often requiring interdisciplinary efforts emphasizing coordination and collaboration among researchers and practitioners. As a result, the National Science Foundation's Digital Government program, which has supported work in disaster management, has employed atypical research management approaches.[4]
- Field research, which provides feedback and helps build community acceptance, is vital. Panelists cited the Disaster Management Interoperability Services program and the Biological Warning and Incidents Characterization project as examples of programs that have had success in carrying out field research that involved the public safety community.
- Successful development is iterative. It is important to provide responders with initial

[4] A reviewer of this report in draft form offered as another example of interdisciplinary work the Infrastructure Management and Hazard Response program in NSF's Engineering Directorate, which seeks to integrate engineering, social, behavioral, political, and economic research.

prototypes to bootstrap the iterative process.

- Testbeds and exercises are particularly critical in developing IT for disaster management because they provide opportunities for feedback from actual users about critical requirements of responders that may not otherwise be apparent. In some cases, large-scale testbeds are required for understanding issues that emerge only at a large scale. Simulations present opportunities not only for training but also for observation and assessment of IT capabilities such as decision support tools.
- Operational facilities that permit instrumentation, experimentation, and iteration are needed. Instrumentation is important for both real and synthetic environments.
- The Department of Defense, which is confronting many of the same interoperability challenges that face the public safety community, is in the process of researching, developing, and implementing a network-centric approach to communications and information management that would overcome existing stovepipes among systems and organizations.

Several panelists also made a number of more general observations about what kinds of information technologies and research are appropriate in what circumstances:

- Different information technologies are appropriate in the various phases of the disaster management life cycle, i.e., preparation, response, mitigation, and recovery.
- Researchers tend to look for overarching themes, but experience has shown that it is critical, in applying IT to disaster management, to start with real problems faced by real end users, to find solutions, and then to work back from there to overarching themes. Starting with overarching themes will lead to dead ends, and unimplemented and unimplementable technology.
- False positives are the bane of any system providing critical functionality and will result in technology not being used. Even if is seems that a few false positives ought to be tolerated, the reality is often that false positives will not be tolerated, especially when the consequences are great.

Several speakers focused on the topic of wireless and mobile communications.[5] They identified some general issues as well as areas of promising research and challenges related to this technology. Panelists noted several attributes of both commercial and governmental wireless technologies that are important in disaster management:

- In addition to being untethered, wireless communications are highly and dynamically reconfigurable without physical linking, which allows reprovisioning of communications infrastructure on the fly.
- Its dynamic nature makes wireless communication especially suitable for reaching areas not served well by fixed infrastructure, as well as places where the fixed infrastructure has been compromised or damaged.

As noted by panelists, several areas of wireless technology merit further research:

- Wireless communication is very challenging at the physical layer. Connectivity is often poor, and bit error rates are high. As a result, protocols that are robust and efficient in the

[5] Some of the comments of Nader Moayeri (manager, Wireless Communications Technologies Group, National Institute of Standards and Technology) who spoke in a later panel session, are also included in this section.

face of disconnections are important. The tradeoff between high data rates but limited reception, and low data rates but longer-distance reception, results in part from a shadowing effect, in which obstacles make reception more difficult at higher frequencies. Power consumption and limits on battery capacity can significantly constrain the use of mobile communications.

- Of particular interest for disaster response is the fact that it is hard to communicate through metal frame buildings or metal-containing debris—either low frequencies (with little capacity) or repeaters must be used. Options for deploying repeaters include pre-installing them in structures (like sprinklers) or having first responders leave them behind (like a trail of bread crumbs).
- Wireless networking is an active area of research. Ad hoc and mesh networking is being deployed and used today (especially by the Department of Defense), but there are many unsolved problems associated with complex wireless networks. For example, how can information be moved reliably through a complex network of unreliable nodes and links? How can such a network be set up and managed?
- Because network capacities are limited in comparison with those of wired networks, wireless networks are much more susceptible to overload if the wrong data is transmitted or is sent to the wrong people at the wrong time. Sending video to someone who does not want or need it not only distracts the human but uses up network bandwidth that cannot be used for something more useful. One approach is content routing, which attempts to move data to where it is needed for analysis or decision making without overloading wireless links. Another strategy is to anticipate the locations where many people will need to look at a particular piece of information, and then move that information to a local server for later asynchronous access.
- Network trustworthiness is important. If a network cannot be relied on, because of either technical or security problems, it will not be used. Improved network management capabilities are similarly important.
- Cognitive radios and other devices that hide complexity from users and move that complexity into the devices or the network have great promise, but they require more research.
- Wireless technologies can be used to provide location information independent of the Global Positioning System. Better techniques of that kind are needed for applications indoors, in dense urban environments, and so forth.

Several panelists spoke about general issues and promising research areas in information integration and data fusion. Several comments outlined the general problem area:

- A growing number and variety of sensors and other data sources are generating ever-larger volumes of data, including text, numeric, geospatial, and video data.
- Most information is manually processed today—meaning in practice that most data is ignored and is not analyzed even if it actually contains actionable information.
- Automation is essential to process, filter, and correct this flood of data, to present it as accurate and actionable information for human decision makers. Improved analysis, synthesis, and fusion of data will require progress on both the syntax and semantics.

Several comments described particular research topics of interest in information integration and data fusion:

- Considerable research has been done in data semantics. Progress has been made on a number of fronts in several different research communities, but many challenges remain.

For example, given the past lack of success in forging agreement on global schemas, it is widely believed today that a multiple schema approach is required that maps schemas to each other. A major technical challenge is how to reason about the relationship among what may be a large number of different schemas.

- A problem of particular interest for disaster management is the ability to fuse data from disparate sources. For example, how can geospatial data about the location of victims be integrated with online data about the location of medical facilities to provide information needed by emergency managers, first responders, and others.
- Adjudication management is an important area of potential value for data fusion. As information from multiple sources flows up to higher levels, a more complete picture can be created, enabling adjudication at the higher level to correct erroneous information that has arisen at lower levels. Adjudication also helps reduce the volume of information being pushed up, which can overwhelm decision makers.
- Another challenge is dynamic selection and combination of sources of data. Sources have varying quality and credibility, due to both human- and technology-related issues. Data may be redundant or contradictory. Data fusion has to advance to the point that multiple data streams of heterogeneous and often confusing data can be converted into actionable information.
- Detection of change is an area potentially ripe for research. It has been looked at primarily by database people concerned chiefly about detecting anomalies in database joins (a common database operation in which data from multiple sources is combined). With respect to disaster management, the interest is really detection of anomalies and determination of whether a change is significant or not.

Several panelists spoke about decision support:

- The type of technology useful for decision making varies depending on whether it is being applied at the phase of preparation for, response to, or recovery from a disaster. To create and deploy the right technology solutions, it is critical to understand the differences between these situations, as well as the different time lines for decision making. Strategic risk management involves discussion, analysis, and long time lines. Effective operational risk management requires doing something now, based on whatever information is immediately available.
- Decision support currently is focused largely on optimization, or determining the optimal plan for achieving a goal. Experience has shown (based primarily on Defense Department efforts) that decision makers need "good enough" solutions produced in the time available rather than optimal solutions that arrive too late. It is important that the implications of decision makers' criteria for assessing outcomes be factored in and presented to them, to prevent the undesirable situation of having a solution that does a good job of meeting ill-advised criteria.
- Decision making is both planned and improvised. Sometimes, for example, the formal organizational structures prove too rigid and obstruct information sharing, prompting improvisation. One technical challenge is how to make it easier and more natural for people to improvise. Building such capabilities requires new models to predict and explain improvised roles, processes, and structures.
- It is critical to find the balance between what machines can do most effectively and what humans can do most effectively. That the balance may change over time as technology advances must be understood and managed as well.
- Advances in visualization of information are critical. Humans process visual data very efficiently but text data slowly. (For a computer system, the reverse is generally true.)

- Context (including a user's location, task load, and environment) is critical to decision support and situational awareness. What information people need or the form in which to present it cannot be determined in isolation if systems are to provide actionable information without overloading users.
- Even good information delivered at the right time may not be appropriate if it is delivered in the wrong way. An example that also illustrates the importance of sensitivity to context was provided by a panelist who noted that in a recent training exercise, Marines who were using personal digital assistants to work with map data rather than focusing on immediate dangers were the first ones to be "shot."

Several panelists focused on sensors, sensor networks, and autonomous devices:

- Unmanned aerial vehicles, especially when combined with improved network communications, have tremendous promise because they can carry weather and other types of cameras and sensors to places that human responders cannot reach safely or at all.
- The distance between a remote device and the human interpreting the device's information output to make decisions introduces major complications, with respect to both human processing and communications infrastructure.
- It can be very difficult to build and maintain situational awareness when information is delivered by remote devices, in what perceptual psychologists call a mediated presence. The brain tries to treat the information it is receiving as if it is being seen directly, which can introduce subtle mistakes. This so-called keyhole effect leads to a deconstructed environment for people trying to analyze the information they are receiving. Training can help alleviate, but will not eliminate, fundamental perceptual problems. These must be addressed by research that considers the entire data-information-knowledge cycle.
- An important aspect of autonomous, remote-presence devices is that they are active, not passive. If people stop focusing on the task at hand and instead concentrate on managing the technology (e.g., driving the robot, pointing the camera), the result can be tunnel vision.
- Sensor data may be especially useful for immediate response and mitigation efforts involving critical infrastructure, such as bridges. Deployment of sensors so that they are in place in advance of an event implies their integration into the design and maintenance cycles of the infrastructure—an effort that is beginning to happen but has to become ubiquitous. Further research is required to optimize deployment of sensors integral to critical infrastructure.
- The military is an important source of lessons in how to build computer simulations that can incorporate sensor data. Methods for cost-effective virtual prototyping and virtual exercises are critical to advancing the state of the art. Although the military has done much work in this area, which should be leveraged as much as possible, making this type of research cost-effective for civilian disaster management is a challenge that will require innovative approaches.

TOPIC 3: COLLABORATION, COORDINATION, AND INTEROPERABILITY: PRESSING ISSUES IN A NEED-TO-SHARE WORLD

Two panels considered current and future approaches to interoperability and information exchange. Several presentations focused on interoperability and wireless infrastructure activities being undertaken at the state level. A number of major trends were noted by panelists:

- New organizational models are being adopted that balance the roles of state-level bodies,

which coordinate communications activities, and local agencies, which retain responsibility for most acquisition and deployment decisions.

- Increasingly, states are building and operating statewide public safety communications networks. In some cases, subscriber equipment (radios) to access the network must be purchased by public safety agencies; in others the state supplies the equipment at no cost. In some states access to the network is free, whereas others charge access fees. According to panelists, these efforts to get localities to acquire and use more interoperable equipment have been relatively successful.

Panelists also offered a variety of perspectives on lessons learned about how to achieve interoperability:

- Regardless of the approach, major change will take many years. Systems that can be deployed in the short term to provide even limited capabilities to bridge existing communications systems are a useful interoperability tool.
- Achieving the goal of widespread deployment of interoperable systems requires a long-term strategy for migrating from today's systems to the desired capabilities. The migration strategy should be developed and refined in consultation with all the relevant stakeholders.
- Mandates, whether funded or unfunded, have not proved effective as means to achieve interoperability. Effective approaches require considerable consensus building and leave as much autonomy as possible at as low a level as possible.

Several comments were made about organizational and cultural challenges associated with increasing sharing of information for disaster management:

- Non-governmental organizations and other private entities (such as hospitals or operators of critical infrastructure) are increasingly seen as major players in disaster management. Many of these organizations have significant amounts of relevant data and information that is currently made available for disaster management only in a very ad hoc, unintegrated manner.
- Much work will be required to allow non-traditional sources to supply data for use in emergency operations. The reliability of sources is a critical issue. Data from a hospital, for instance, may have a higher level of reliability than that supplied by an individual eyewitness report.
- Indicators of the reliability of sources should be part of the data collected and distributed to emergency managers so that information can be assessed properly. The military long ago adopted this practice, but indicating the reliability of data is largely not done in current disaster management operations, at least not in any systematic fashion.

Finally, several speakers focused on opportunities and challenges for building future interoperable networks. Their comments included these:

- Adaptive technologies, such as cognitive radios, that sense their environment and modify their frequency, waveform, and even their power consumption to fit the situation will continue to evolve and play a growing role in public safety communications.
- Insufficient availability of radio frequency spectrum remains a constraint to realizing future public safety and disaster management networks. A number of approaches may provide practical improvements in spectrum allocation issues. "Lights and sirens" priority access allows public safety users to signal other users aside, much as an

ambulance does with road traffic. Time- and spatial-sharing can be further exploited. Spectrum rights obtained in secondary markets could be subject to preemption by communications for public safety.

- Envisioning, enabling, and building networks of the future will be facilitated by the availability of test beds and simulation environments that allow disparate technologies to be designed, built, and tested. Testbeds and capabilities for simulation will also facilitate the ability to analyze such technologies in relation to an information architecture and strategy.
- Information systems are increasingly network-centric rather than hierarchical. In network-centric operations, information is shared horizontally, among tactical-level peers, as well as vertically up and down the command chain. To move in this direction, the Department of Defense has had to overcome cultural obstacles and make a major investment in new technologies. Similar challenges can be expected for the public safety community.
- Information systems that provide access to state and federal databases are of growing importance for public safety and disaster management. Databases of interest range from motor vehicle records to weather forecasts to public health information.
- The availability of information in the form of Internet Protocol-based data will continue to be a driver for future networks. As the availability of data increases and its usefulness becomes better understood, networks will have to integrate and incorporate it.
- The Web services model is catching on as a way of exchanging and integrating data for disaster management.
- The Disaster Management Interoperability Services toolkit that is being supplied to the disaster management community by FEMA provides a way of exchanging information among systems and organizations. It is anticipated that this toolkit will help enable the building of a common operating picture during disasters.
- A culture of information technology tool sharing, which will help make use of future networks more effective, is beginning to take root in the disaster management community but needs further nurturing. Public-private partnerships are an important part of this effort, as are laboratories and test beds where vendors, researchers, and public safety and emergency management organizations can work to integrate their products and services.
- Increased trust among the various stakeholders is critical if their IT systems are to be more closely integrated.

Appendixes

Appendix A

Workshop Agenda

WORKSHOP ON USING INFORMATION TECHNOLOGY TO ENHANCE DISASTER MANAGEMENT

June 22-23, 2005
Washington, D.C.

Wednesday, June 22

9:00–10:00 a.m.	Continental Breakfast
10:00–10:30	**Welcome to the Workshop** *Jon Eisenberg,* Study Director and Senior Program Officer, Computer Science and Telecommunications Board/National Research Council (NRC) *Charles Brownstein,* Director, Computer Science and Telecommunications Board/NRC *Ramesh Rao*, Chair, NRC Committee on Enhancement of Crisis Management—Improving the Use of Information Technology in Disaster Preparedness, Response, and Recovery and Professor, University of California, San Diego *Barry West*, Chief Information Officer/Director Information Technology Services Division, Federal Emergency Management Agency (FEMA)

NOTE: Copies of the slides used in the presentations and made available by the panelists to CSTB for public distribution can be viewed at CSTB's Web site at www.cstb.org. The slides have not been viewed or edited by the National Research Council, and opinions expressed and statements made in them are solely those of the individual panelists and have not been endorsed or verified as accurate by the National Academies.

Topic 1: The Critical and Evolving Role of Information and Communication Technologies (ICTs) in Disaster Management

Questions Posed in Advance to Panelists: How might we better manage future crises? What impact will major technology trends have on how disaster management is handled in the future? How can we leverage commercial technology cost-performance curves yet meet special requirements? What new technologies, approaches, and policies would help, and what research directions are promising?

10:30–12:00 noon **Context for and Visions of the Future, Grand Challenges for ICTs in Disaster Management**
15 minute presentation by each panelist, followed by 15 minute Q&A

John Harrald, Director, Institute for Crisis, Disaster, and Risk Management, George Washington University (*Moderator*)
David G. Boyd, Director, Office for Interoperability and Compatibility, Science and Technology Directorate, U.S. Department of Homeland Security
Helen Wood, Senior Advisor, NOAA Satellites and Information Service and Chair, National Science and Technology Council's Subcommittee on Disaster Reduction
Jack Potter, Director, Emergency Medical Services, Valley Health and Vice Chair, COMCARE Board of Directors
Peter Miller, Program Manager, Mission Support Office, HSARPA, Science and Technology Directorate, U.S. Department of Homeland Security

12:00–12:45 p.m. Lunch

Questions Posed in Advance to Panelists: What lessons have been learned from past crises and exercises? What gaps in IT capabilities are evident, and how might they be addressed? Where is the state of the art not sufficient to meet our needs?

12:45–2:00 **Perspectives on the Current State of the Art: ICTs in Disaster Management Practice**
15 minute presentation by each panelist, followed by 15 minute Q&A

Ellis Stanley, General Manager, Emergency Preparedness Department, City of Los Angeles, California (*Moderator*)
Mark Deputy, Senior IT Specialist and Urban Search and Rescue Team Assistant Task Force Leader, Montgomery County, Maryland
William Maheu, Executive Assistant Chief of Police, San Diego Police Department
Robert Roth, Fire Technology Specialist, U.S. Forest Service, USDA

2:00–2:15 Break

Questions Posed in Advance to Panelists: What are especially demanding aspects of disaster management? What initiatives are under way to address them? What specific requirements are there from specific groups or application areas? What general lessons can be learned?

2:15–3:30 **Emerging Applications and Other Drivers for ICTs in Disaster Management**
15 minute presentation by each panelist, followed by 15 minute Q&A

William Maheu, Executive Assistant Chief of Police, San Diego Police Department (*Moderator*)
William Metz, Director, Center for Integrated Emergency Preparedness, Argonne National Laboratory
Jaime Gomezjurado, Project Manager and VP, Business Development, Medical Emergency Response Network Research Project, Semandex Networks, Inc.
Lois Clark McCoy, President, National Institute for Urban Search and Rescue
Peter Brooks, Institute for Defense Analyses

3:30–3:45 Break

Topic 2: Research Directions for ICTs in Disaster Management

Questions Posed in Advance to Panelists: What research areas have application to disaster management? How might leading-edge research be applied to disaster management? How should the research agenda be established and evolved? How can research results best be transitioned into deployed capabilities? What are the commonalities between commercial, civilian, and military capabilities and research and development activities, and how can technology advances and knowledge be transferred from one to the other?

3:45–5:00 **Current ICT Research Programs Related to Disaster Management**
15 minute presentation by each panelist, followed by 15 minute Q&A

Peter Steenkiste, Professor, Carnegie Mellon University (*Moderator*)
Larry Brandt, Program Manager, Digital Government, National Science Foundation
Gary Ham, Senior Research Scientist, Battelle Memorial Institute
Earnest Paylor, Program Director, Pacific Disaster Center (PDC) and Senior Advisor for Interagency Programs, Office of the Special Assistant and NASA Liaison to the Assistant Secretary of Defense–Networks and Information Integration (NII)
Pamela Sydelko, Leader–Modeling, Simulation and Visualization Group, Decision and Information Sciences Division, Argonne National Laboratory

5:00–6:00 **ICT Everywhere: Ubiquitous and Pervasive Mobile (ad hoc) Communications and Networking**
15 minute presentation by each panelist, followed by 15 minute Q&A

Timothy Brown, Associate Professor, University of Colorado Boulder (*Moderator*)
Richard Howard, Research Professor, WINLAB, Rutgers University
Scott Midkiff, Professor, Virginia Tech

Mani Chandy, Simon Ramo Professor of Computer Science, California Institute of Technology

Thursday, June 23

Topic 2: Research Directions for ICTs in Disaster Management (continued)

8:00–8:30 a.m.	Continental Breakfast
8:30–9:45	**Identifying and Aggregating Useful Data—Information Integration and Fusion** *15 minute presentation by each panelist, followed by 15 minute Q&A* *Gio Wiederhold*, Professor (Emeritus), Stanford University (*Moderator*) *Yigal Arens,* Director, Intelligent Systems Division, Information Sciences Institute, University of Southern California *Craig Knoblock*, Research Associate Professor, University of Southern California *Peter Scott,* Associate Professor, University of Buffalo *Zachary Ives*, Assistant Professor, University of Pennsylvania
9:45–10:45	**Information Overload: Making Useful Data Actionable—Decision Support, Collaboration, Situational Awareness** *15 minute presentation by each panelist, followed by 15 minute Q&A* *Robert Neches*, Director, Distributed Scalable Systems Division, Information Sciences Institute, University of Southern California (*Moderator*) *David Mendonça*, Assistant Professor, New Jersey Institute of Technology *William Wallace*, Professor, Rensselaer Polytechnic Institute
10:45–11:00	Break
11:00 a.m.–12:15 p.m.	**Sensor Networks, Autonomous Devices, and GIS** *15 minute presentation by each panelist, followed by 15 minute Q&A* *Robin Murphy,* Professor, University of South Florida and Director, Industry/University Cooperative Research Center on Safety Security Rescue (*Moderator*) *Ayman Mosallam*, Professor, Civil and Environmental Engineering, University of California, Irvine *Susan McGrath*, Associate Research Professor of Engineering, Dartmouth College *David Kehrlein*, Senior Consultant, Environmental Science Research Institute (ESRI), formerly GIS Manager, California Governor's Office of Emergency Services
12:15–1:00	Lunch

Topic 3: Collaboration, Coordination, and Interoperability: Pressing Issues in a Need-to-Share World

Questions Posed in Advance to Panelists: What policy and technical initiatives are currently under way to improve wireless interoperability across federal, state, and local levels? What results are anticipated, and over what time frames? How is data (including voice) generated, used, and shared across organizational boundaries today? What can be learned in terms of technology and practice from efforts to forge more interoperable systems? How are standards helping/not helping? What kinds of interoperability are desired in the future? What technical, operational, economic, and policy challenges are likely to be unresolved, and merit further research? How do communication systems relate to other information management systems related to disaster management? What obstacles to technology transition must be overcome?

1:00–3:00 **Current Initiatives, Technical and Organizational Obstacles and Opportunities in ICT Interoperability**
15 minute presentation by each panelist, followed by 15 minute Q&A

Art Botterell, Associate Director, Emergency Information Systems Consultant, incident.com (*Moderator*)
Ellis Kitchen, Chief Information Officer, Maryland Office of Information Technology and Member, Interoperability and Integration Committee, National Association of State Chief Information Officers (NASCIO)
Steve Cooper, Senior Vice President and Chief Information Officer, Red Cross
Lloyd (Gene) Krase, Administrator, Kansas Division of Emergency Management
Otto Doll, Commissioner*,* Bureau of Information and Telecommunications, South Dakota
Dave Smith, Implementation Director, Indiana Integrated Public Safety Commission
Robert Fletcher, President, Readiness Consulting Services LLC and Member, National Fire Protection Association NFPA 1600 Technical Committee

3:00–3:15 Break

Questions Posed in Advance to Panelists: What should communications and other IT capabilities look like in the future? How do wireless communications systems relate to the emerging broader architecture for public safety, national security, and Disaster response? What are the implications of major information and communications technology trends for how we respond to crises? How can these opportunities better be exploited? What kinds of research, experimentation, and pilot programs would help?

3:15–4:30 **Envisioning, Enabling, and Building Networks of the Future**
15 minute presentation by each panelist, followed by 15 minute Q&A

Nancy Jesuale, President, NetCity Engineering (*Moderator*)
Nader Moayeri, Manager, Wireless Communications Technologies Group, National Institute of Standards and Technology
James Morentz, VP, Homeland Security Technology and Director, Public Safety Integration Center, Science Applications International

Corporation
Chip Hines, Program Manager, Disaster Management eGov Initiative, Office of the CIO, Emergency Preparedness and Response/FEMA, Department of Homeland Security

4:30–4:45 **Concluding Remarks**
Ramesh Rao, Chair, NRC Committee on Enhancement of Crisis Management—Improving the Use of Information Technology in Disaster Preparedness, Response, and Recovery

Appendix B

Biographies of Committee Members and Staff

COMMITTEE MEMBERS

Ramesh R. Rao, *Chair*, is currently a professor in the Department of Electrical and Computer Engineering, and director of the San Diego Division of the California Institute of Telecommunications and Information Technology, at the University of California, San Diego. His research interests include architectures, protocols, and performance analysis of wireless, wire line, and photonic networks for integrated multimedia services. Prior to his appointment as the Director of the San Diego Division of the California Institute of Telecommunications and Information Technology (Cal-(IT)²), he served as director of the UCSD Center for Wireless Communications (CWC) and was the vice chair of Instructional Affairs in the Department of Electrical and Computer Engineering. Rao did his undergraduate work at the Regional Engineering College of the University of Madras in Tiruchirapalli, obtaining a B.E. (honors) degree in electronics and communications in 1980. He did his graduate work at the University of Maryland, College Park, Maryland, receiving his M.S. in 1982 and his Ph.D. in 1984.

Yigal Arens is director of the Intelligent Systems Division of the University of Southern California's Information Science Institute in California. He is also co-director of DGRC, the USC/Columbia University Digital Government Research Center, and a research professor at USC's Daniel J. Epstein Department of Industrial and Systems Engineering. His primary research interests have been digital government, information integration, planning in the domain of information servers, knowledge representation, and human-machine communication. In 1983, he joined the faculty of the Computer Science Department at the University of Southern California. He joined USC's Information Sciences Institute (USC/ISI) in 1987, where he first worked on the Integrated Interfaces project, a multimedia presentation design system combining text, tables, maps, and other graphics. For almost 10 years he headed the Single Interface to Multiple Sources (SIMS) research group specializing in integration of heterogeneous databases and other information sources. Arens has been director of the Intelligent Systems Division, one of the largest artificial intelligence research laboratories in the United States, since 1999. Also, since 1999, he has been co-director of the DGRC. In 1999, together with two colleagues from ISI, Arens founded Fetch Technologies, a company that specializes in extracting data from Web sites. In 2002, he joined the Daniel J. Epstein Department of Industrial and Systems Engineering as research professor. In 2003, Arens founded USC's Center for Research on Unexpected Events

(CRUE), which he headed for its first year. Dr. Arens also was a part of the National Research Council's Committee on Information Technology and the States: Public Policy and Public Interests. Arens received his Ph.D. from the University of California at Berkeley.

Art Botterell is an internationally recognized expert in emergency communications who has served on the front lines of some of the biggest national disasters in recent U.S. history. Former FEMA director James Lee Witt hailed him as a "national asset." He has served as a consultant to the Department of Homeland Security and a number of other state, federal, and international organizations. He led the development of the Common Alerting Protocol (CAP)—the first international standard format for all-hazard public warning across multiple media. An experienced analyst, broadcast and multimedia producer, writer, and manager, Mr. Botterell studies the ways communities use information technology to manage the effects of sudden change.

Timothy X Brown is an associate professor at the University of Colorado, Boulder. He received his B.S. in physics from Pennsylvania State University and his Ph.D. in electrical engineering from California Institute of Technology in 1990, when he also joined the Jet Propulsion Laboratory. In 1992 he joined Bell Communications Research. Since 1995 he has held a joint appointment with the Electrical Engineering and Interdisciplinary Telecommunications Departments at the University of Colorado, Boulder. His research interests include adaptive network control, machine learning, and wireless communications systems. His laboratory has developed extensive experience in the design, implementation, and testing of wireless networking protocols. He has published over 50 papers in networking and wireless systems. He is a recipient of the NSF CAREER Award and was selected as the GWEC Wireless Educator of the year.

John R. Harrald is the director of the George Washington University (GWU) Institute for Crisis, Disaster, and Risk Management and a professor of engineering management in the GWU School of Engineering and Applied Science. He is a founding member, director, and immediate past president of the International Emergency Management Society (TIEMS). Dr. Harrald has been actively engaged in the fields of emergency, consequence, and crisis management and maritime safety and port security. He was the former director of the Disaster Recovery Institute (DRI) and served as the associate director of the National Ports and Waterways Institute for 10 years. Dr. Harrald was the principal investigator for maritime risk and crisis management studies in Prince William Sound, Alaska, the Port of New Orleans, and Washington State and for earthquake vulnerability studies funded by the National Science Foundation and the American Red Cross. He has studied the response to the Exxon Valdez oil spill, the Loma Prieta earthquake, Hurricane Hugo, Hurricane Andrew, the Northridge earthquake, the 1999 Turkey earthquakes, and the September 11 terrorist attacks on the World Trade Center and the Pentagon. He has also written and published in the fields of crisis management, emergency management, management science, risk and vulnerability analysis, and maritime safety. He was a reviewer for the committee that produced the report *Information Technology Research, Innovation, and E-Government*. Harrald received his B.S. in engineering from the U.S. Coast Guard Academy, an M.A.L.S. from Wesleyan University, an M.S. from the Massachusetts Institute of Technology, where he was an Alfred P. Sloan Fellow, and an M.B.A. and a Ph.D. from Rensselaer Polytechnic Institute.

Richard Howard is a researcher at Wireless Information Network Laboratory (WINLAB) at Rutgers University. He is also a principal at Research Innovations, LLC, and he is the founder and Sr. V.P. of Technology at PnP Networks, a start-up company focused on applying artificial intelligence techniques to the problem of making computers and computer networks truly simple for people to use. Howard was formally the wireless research vice president at Lucent Bell Laboratories, where he did research on wireless technology from materials, components,

packaging, antennas, modeling, analysis, communication theory, and integrated circuit design to systems-level projects like fixed wireless loop and advanced cellular base stations. His work has emphasized multiple antennas, signal processing, and system performance from basic communication theory to field deployment. Howard's key achievements include new theory (and practical demonstrations) for dramatically increasing wireless system capacities based on multiple antennas. Other achievements have included algorithms and tool suites for optimization of cellular networks and application of advanced signal processing to linear power amplifiers for dramatic cost/size reduction and efficiency improvements. Howard received his Ph.D. in physics at Stanford University in 1977.

Nancy Jesuale has worked in local and state government since 1976 as a telecommunications strategic planner, and as director of public safety networks, telecommunications networking and network operations. Ms. Jesuale is the president of NetCity Engineering, Inc., a consulting practice dedicated to strategic planning and solution sets for government in public safety and fiber optic telecommunications systems. Current clients of NCE include the City of Los Angeles, the District of Columbia, the State of Oregon, the City of Charlotte, NC, and the Center for Wireless Network Security. As program manager for Public Safety for WiNSeC at Stevens Institute of Technology, Ms. Jesuale is responsible for establishing relationships, research programs, and public policy support. Ms. Jesuale has been an innovator in telecommunications strategies for local government since 1984. She is an appointee to the National Task Force on Interoperability and the Oregon State Interoperability Executive Committee. She is a past chair of the Public Technology Inc. Task Force on Information Technology and Telecommunications. She has been the director of strategic planning for telecommunications for the City of Los Angeles and has served on the Oregon Statewide Interoperability Executive Council.

David Kehrlein, now with Environmental Science Research Institute (ESRI), was the geographical information systems (GIS) manager for the California Governor's Office of Emergency Services (OES) for over 9 years. Before that he worked in the Forest and Rangeland Resource Assessment Program (FRRAP) of the California Department of Forestry and Fire Protection. Kehrlein was active on the Governor's GIS task force in 1992. He is a past director of the California Geographic Information Association (CGIA), and he is the chairman of the data standards committee. He was also chair of the Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE) GIS Specialist Group. He has organized response and recovery GIS support for 16 presidentially declared disasters from incident-level response to decision support at the state and federal levels. His group at OES also deployed a response/training GIS trailer that is equipped with large format plotting and scanning capabilities, a statewide GIS data repository, as well as satellite cell phone and a high-speed satellite Internet downlinking capability. Kehrlein received his B.A., graduating with honors in geography, from California State University, Sacramento.

William Maheu is chief of operations of the San Diego, California Police Department. A member of the police department for 23 years, Maheu is currently in charge of Child Abuse, Domestic Violence, Sex Crimes, Vice Operations, Mid City Division, Southeastern Division, Southern Division, Records, Property and various other programs. During his tenure with the department, he has had many assignments, including commanding officer of field operations/special resources, executive lieutenant of the Special Weapons and Tactics Team, special projects/long-range planning lieutenant, and narcotics sergeant. He has also been involved in several major projects, including the 2003 Super Bowl, the Republican National Convention, the Presidential Debate, development of the Psychiatric Emergency Response Team, and the development of the Homeless Outreach Team. Maheu graduated from the University of San Diego in 1983 with a B.A. in psychology.

Robin R. Murphy is a professor in the Computer Science and Engineering Department at the University of South Florida with a joint appointment in Cognitive and Neural Sciences in the Department of Psychology. She is an associate editor for *IEEE Intelligent Systems* and a member of the 1998-1999 Defense Science Study Group and is currently a member of the U.S. Air Force Scientific Advisory Board and the DARPA ISAT. She recently served on DoD Air Platforms FY2004 Technology Area Review. In addition, she is also a member of the board of directors for Continental Divide Robotics, which provides GPS and intelligent agent software for tracking parolees. From 1992 to 1998, she was an assistant professor in the Department of Mathematical and Computer Sciences at the Colorado School of Mines. Murphy joined USF in 1998, and in January 2002 she became director of the Center for Robot-Assisted Search and Rescue (CRASAR). In March 2003, she helped start the industry/university cooperative research center on Safety Security Rescue (SSR-RC) with the University of Minnesota and is the overall director. She leads the CRASAR rescue robot response team, the only such team in the world, and is a technical search specialist with Florida Task Force 3. Since 1995, she has focused on Urban Search and Rescue (USAR) as the test domain for her research, leading to her participation in the first known use of robots for urban search and rescue at the WTC disaster. Her USAR robotics work has earned a NIUSR Eagle award, and she serves on the executive board of the National Institute for Urban Search and Rescue. She has also won a USF Outstanding Faculty Research Achievement Award (2003), and the Honor Society of Phi Kappa Phi, USF Chapter Artist and Scholar of the Year Award (2004). Prior to graduate work, Murphy worked in the process control industry as a software project engineer. Murphy has also served as a member of the Army Unmanned Ground Vehicle Technology Committee at the National Academies. Murphy received a B.M.E. in mechanical engineering, and an M.S. and a Ph.D. in computer science (minor: computer integrated manufacturing systems) in 1980, 1989, and 1992, respectively, from Georgia Tech, where she was a Rockwell International Doctoral Fellow.

Robert Neches is director of Information Sciences Institute's Distributed Scalable Systems Division and a research faculty member of the University of Southern California Computer Science Department. He received his Ph.D. from Carnegie Mellon University in 1981 for work in machine learning, spent a year at the University of Pittsburgh's Learning Research and Development Center, and has been at USC ISI since 1982 (with the exception of service at the Defense Advanced Research Projects Agency from 1994-1997). His personal interests span control and coordination in distributed systems; collaboration and visualization aids for information management; and "system of systems" frameworks for information integration. The Distributed Scalable Systems Division looks at the full range of issues bearing on organizations gathering information, assessing it, making decisions, de-conflicting, and effecting resulting actions. Research within the division addresses distributed software systems engineering, information management, intelligent human-computer interaction, computer-supported cooperative work, resource management, and decision support. Applications within the division include all levels of command-and-control, crisis management, intelligence analysis, logistics, design and manufacturing, and space applications.

Masanobu Shinozuka is a distinguished professor and chair of the Department of Civil and Environmental Engineering at University of California, Irvine, and Norman Sollenberger Professor Emeritus of Civil Engineering at Princeton University. He is a member of the National Academy of Engineering (NAE). His research activities involve random vibration, reliability of structural systems, structural dynamics, structural control, continuum mechanics, and infrastructure systems, including lifeline networks. In particular, his pioneering and original research on digital simulation of stochastic waves is noteworthy. He has more than 500 publications in refereed journals and proceedings of national and international conferences in mechanics, structural engineering, and natural/man-made disaster mitigation. His contributions to

these areas have been recognized with a number of prestigious awards, such as Newmark, Freudenthal, and Von Karman Medals from the American Society of Civil Engineers, of which he is an honorary member. Shinozuka's recent research deals with the detection of damage and its locations within a network of utility and highway transportation systems subject to natural and man-made disturbances. In this regard, his most recent effort, under the sponsorship of the National Science Foundation, focuses on the development of energy-efficient and self-powered sensor networks and wireless data transmission systems that can be applied to real-time diagnosis of these systems after serious security breaches. He has a long history of working relationships with engineers and managers at Caltrans (California Department of Transportation), LADWP (Los Angeles Department of Water and Power), and MLGW (Memphis Light, Gas and Water), and more recently with SCE (Southern California Edison) to estimate the seismic performance of their systems. He also served as president and executive vice president of the International Association of Structural Safety and Reliability (IASSAR). Shinozuka received his Ph.D. from Columbia University from the Department of Civil Engineering and Engineering Mechanics in 1960 and an M.S. in civil engineering (1955) and a B.S. (1953) from Kyoto University.

Ellis Stanley is the general manager for the Emergency Preparedness Department of the City of Los Angeles. Currently he serves as an advisor to the Multidisciplinary Center for Earthquake Engineering Research (MCEER) and is a member of the center's Industry Advisory Board, and he chairs the Metro Emergency Manager's Forum of the International Association of Emergency Managers. He is vice-president for the public sector of the Business and Industry Council on Emergency Preparedness and Planning (BICEPP) and is on the Emergency Services Committee of the American Red Cross Los Angeles chapter. The city council has also appointed him to the Emergency Preparedness Commission for the county and city of Los Angeles, and he is a member of the city's Emergency Operations Board. Ellis was recently appointed to the board of directors of the National Institute of Urban Search and Rescue (NIUSR). He was the director of the Atlanta-Fulton County Emergency Management Agency and has been the director of an emergency management program for the city of Durham, Durham County, North Carolina and Brunswick County, North Carolina. In addition, he also served as a county fire marshal, fire and rescue commissioner, county safety officer; as president of the International Association of Emergency Managers (IAEM), the American Society of Professional Emergency Planners (ASPEP), the National Defense Transportation Association (NDTA), and the Metropolitan Atlanta chapter of the National Forum for Black Public Administrators (NFBPA); and as vice chair of the Association of Contingency Planners (ACP). He also chaired the Certified Emergency Managers Certification Commission. Stanley is a 1973 graduate of the University of North Carolina at Chapel Hill with a degree in political science.

Peter Steenkiste is a professor of computer science and of electrical and computer engineering at Carnegie Mellon University. His research interests are in the areas of networking and distributed computing. After joining CMU, he worked on a number of high-performance computing and networking projects, including Nectar, the first workstation clusters built around a high-performance, switch-based local area network. He has also done research in the areas of network quality of service, large-scale self-configuring network services, and network measurements. Steenkiste's current research is in the areas of pervasive computing and wireless networking. For example, he is working on technologies that will support the widespread deployment of context-aware services for mobile users. In the wireless area, he is developing protocols and algorithms for a "self-managing" wireless network and he is also looking at better techniques and methods for evaluating and testing wireless networks. Steenkiste received the degree of electrical engineer from the University of Gent in Belgium in 1982, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University in 1983 and 1987, respectively.

Gio Wiederhold is an emeritus professor of computer science at Stanford University, with courtesy appointments in medicine and in electrical engineering. His current research includes privacy protection in collaborative settings, large-scale software composition, access to simulations to augment decision-making capabilities for information systems, and developing algebra over ontologies. Prior to his academic career he spent 16 years in the software industry. His career followed computer technologies, starting with numerical analysis applied to rocket fuel, FORTRAN and PL/1 compilers, real-time data acquisition, and a time-oriented database system; eventually he became a corporate software architect. He has been elected a fellow of the ACMI, the IEEE, and the ACM. He spent 1991-1994 as the program manager for knowledge-based systems at DARPA in Washington, D.C. He has been an editor and editor-in-chief of several IEEE and ACM publications. Wiederhold served as a reviewer for several CSTB reports, including *Information Technology Research, Innovation, and E-Government*; *Youth, Pornography, and the Internet; Technical, Business, and Legal Dimensions of Protecting Children from Pornography on the Internet: Proceedings of a Workshop; Non-technical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet: Summary of a Workshop*; *Review of the FBI's Trilogy Information Technology Modernization Program*; and a letter report to the FBI. Wiederhold received a degree in aeronautical engineering in Holland in 1957 and a Ph.D. in medical information science from the University of California at San Francisco in 1976.

STAFF

Jon Eisenberg is a senior program officer with the Computer Science and Telecommunications Board of the National Academies. At CSTB, he has been study director for a diverse body of work, including a series of studies exploring Internet and broadband policy and networking and communications technologies. Current studies include an examination of emerging wireless technologies and spectrum policy and a study of how to use information technologies to enhance disaster management. In 1995-1997 he was an AAAS Science, Engineering, and Diplomacy Fellow at the U.S. Agency for International Development, where he worked on environmental management, technology transfer, and information and telecommunications policy issues. He received his Ph.D. in physics from the University of Washington in 1996 and a B.S. in physics with honors from the University of Massachusetts at Amherst in 1988.

Ted Schmitt is a consultant for the Computer Science and Telecommunications Board of the National Academies. He is currently involved in the CSTB projects providing a comprehensive exploration of cybersecurity and the use of IT to enhance disaster management. Before working at CSTB, Ted was involved in the development of the digital publishing industry and has taken an active role in various standards groups related to digital rights management. Prior to that, he served as technical director at a number of small technology companies in Germany, Sweden, and the United States. He started his career in 1984 as a software engineer for IBM, earning two patents. Ted is currently working on his M.A. in international science and technology policy at George Washington University. His graduate work is supported by a fellowship from the Diplomat and Consular Officers – Retired. He received a B.S. in electrical engineering in 1984 and a B.A. in German in 1997 from Purdue University and studied at the Universität Hamburg, Germany.

Jennifer M. Bishop is a program associate for the Computer Science and Telecommunications Board of the National Academies. She is currently involved in several studies, including Telecommunications Research and Development, Information Technology for Enhancing Disaster Management, and an inquiry into the information needs of citizens during a disaster. She

also maintains CSTB's contact database, handles updates to the CSTB Web site, coordinates the layout and design of *Update*, the CSTB newsletter, and designs book covers and promotional materials. Prior to her move to Washington, Bishop worked for the City of Ithaca, New York, coordinating the Police Department's transition to a new SQL-based time accrual and scheduling application. Her other work experience includes maintaining the police records database for the City of Ithaca, designing customized hospitality industry performance reports for a research firm, and freelance publication design. She is a visual artist working in oil and mixed media. She holds a B.F.A from Cornell University.

Gloria Westbrook joined the Academies with 7 years of administrative experience. She previously served as the executive assistant to the directors of the Office of Youth Programs and the Youth Opportunity Grant Program at the D.C. Department of Employment Services (DOES). While serving in the Director's Office Gloria received the Meritorious Service Award and the Workforce Development Administrator's Award of Appreciation for Dedicated Service. She also became a member of the National Association of Executive Secretaries and Administrative Assistants. Gloria is currently a senior program assistant for the CSTB project titled "Sufficient Evidence? Building Certifiably Dependable Systems." She attended Duke Ellington School of the Performing Arts for ballet and went on to further her dance education at the University of the Arts in Philadelphia, Pennsylvania.