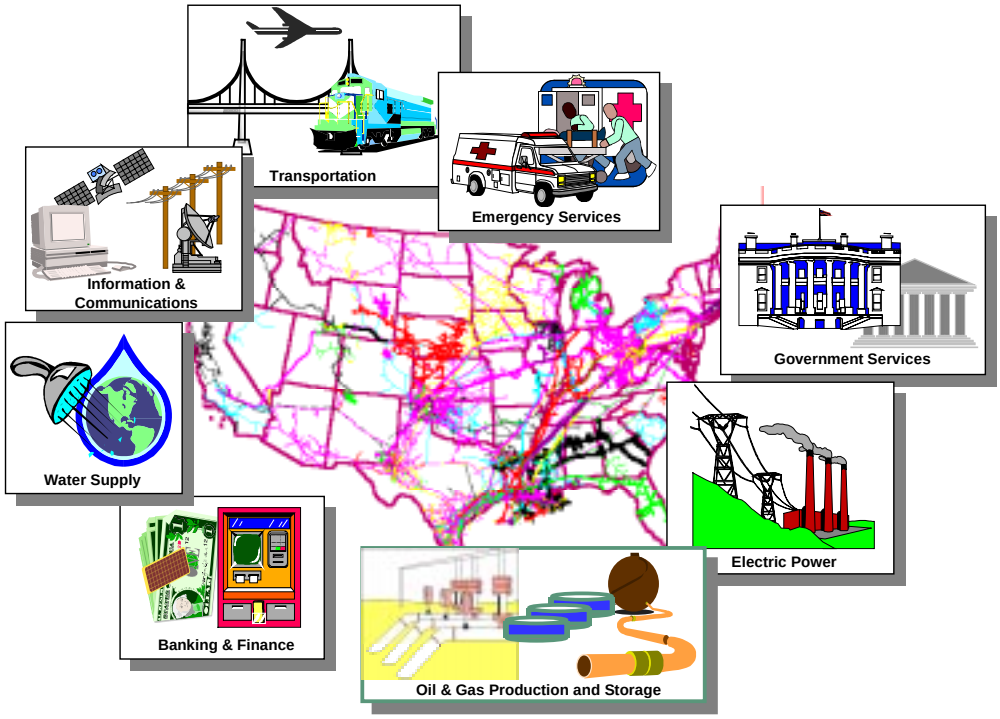
Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures



Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office

July 1998

Contents

Contents (Cont.)

Tabs

Tabs (Cont.)

Tables

Figures

Preface

Developing a robust and harmonized national research and development plan that comprehensively addresses critical infrastructure assurance needs is a complex challenge. This report is intended to be a first step in helping to meet that challenge. The information presented was developed by study teams composed of individuals from government, the private sector, academia and research institutes, and the Department of Energy national laboratory system. The contributions by these individuals were voluntary, reflecting a strong commitment to this roadmapping activity and a recognition of its importance to the nation.

The study teams addressed five infrastructure sectors: banking and finance, energy (electric power, natural gas, oil), information and communications, transportation, and vital human services (water supply systems, emergency services, government services). This report highlights the results of the work in each of those sectors.

It should be noted that the majority of the work by the study teams was completed prior to the release of Presidential Decision Directive 63 — Critical Infrastructure Protection — in May 1998 and the establishment by the Office of Science and Technology Policy of a Critical Infrastructure Protection Research and Development Interagency Working Group.

The study teams recognize that hard work remains to be done. The magnitude and complexity of the R&D question being considered make detailed planning and consensus difficult. It is the hope of the teams that the information presented is viewed in the positive spirit in which it is intended, and that it provides a basis for constructive debate and a foundation for the next steps in developing a viable infrastructure assurance R&D plan.

Study Team

Study Team Directors

John C. Davis, Commissioner — *National Security Agency*
David A. Jones, Commissioner — *Department of Energy*

Study Team Coordinator

Paula L. Scalingi — *Argonne National Laboratory*

Sector Study Team Members

Banking and Finance

Kawika Daguio — *American Bankers Association*
Peter H. Daly, Commissioner — *Department of the Treasury*
Judy Moore — *Sandia National Laboratories*
Anthony G. Oettinger — *Harvard University*

Coordinator: Thomas Baines — *Argonne National Laboratory*

Energy

Fernando L. Alvarado — *University of Wisconsin–Madison*
William M. Burnett — *Gas Research Institute*
Stephen Gehl — *Electric Power Research Institute*
Jean-Michel Guldmann — *Ohio State University*
David A. Jones, Commissioner — *Department of Energy*
Landis D. Kannberg — *Pacific Northwest National Laboratory*

Coordinators: William A. Buehring and Ronald E. Fisher — *Argonne National Laboratory*

Information and Communications

Guy Copeland — *Computer Science Corporation*
Douglas L. Mansur — *Lawrence Livermore National Laboratory*
Terry Mayfield — *Institute for Defense Analyses*
Irwin M. Pikus, Commissioner — *Department of Commerce*

Coordinator: Craig Swietlik — *Argonne National Laboratory*

Transportation

E. Fenton Carey — *Department of Transportation*
Steven R. Ditmeyer — *Federal Railroad Administration*
Bruce E. Peterson — *Oak Ridge National Laboratory*
Joseph L. Schofer — *Northwestern University*

Coordinator: Christopher L. Saricks — *Argonne National Laboratory*

Vital Human Services

Stephen W. Clark — *Environmental Protection Agency*
Joseph H. Keller — *Idaho National Engineering and Environmental Laboratory*
Robert L. Sherwood — *IIT Research Institute*
Richard A. Swanson — *Computer Science Corporation*
Kevin Tonat — *Department of Health and Human Services*

Coordinator: Jerry L. Gillette — *Argonne National Laboratory*

Study Integrators

James P. Peerenboom — *Argonne National Laboratory*
Thomas D. Wolsko — *Argonne National Laboratory*

Acknowledgments

The study team gratefully acknowledges the encouragement and insight provided by Kerri-Ann Jones (Associate Director), Bruce MacDonald, and Steven Rinaldi of the National Security and International Affairs Division of the Office of Science and Technology Policy. We also thank the many subject-matter experts and reviewers listed in the Section 5 for their substantive contributions to this report. Finally, we thank Argonne National Laboratory for coordinating the study effort and providing valuable administrative, editorial, and document preparation assistance.

Executive Summary

Introduction

This summary highlights the results of a four-month research and development (R&D) study conducted by the Transition Office of the President's Commission on Critical Infrastructure Protection. The study builds on work previously conducted by the Commission and provides a foundation for the next steps in developing a national infrastructure assurance R&D program. Preliminary R&D topics and associated roadmapping information are provided for eight critical national infrastructures: banking and finance, electric power, oil and gas production and storage, emergency services, government services, information and communications, transportation, and water supply.

The goal of this infrastructure assurance R&D is to support the development of technologies that will counter threats and reduce vulnerabilities in those areas having the potential for causing significant national security, economic, and/or social impacts. Physical and cyber threats — as well as new threats from the growing complexity of, and interdependencies among, infrastructures — are addressed. Specific technologies considered are those that protect infrastructure and thereby reduce vulnerability, detect intrusions and provide warnings, mitigate the effects of disruptions (incidents), assist in the management of incidents, and facilitate recovery.

Research requiring government investment is emphasized. This research must be accompanied by technology development within the private sector to ensure that useful products are developed. Although such private-sector development is outside the scope of this

Scope of Roadmapping Study

Study timeframe: FY2000 – FY2010.

Study focus: perceived technology shortfalls, or "gaps," between infrastructure assurance technology needs and available technologies

Categories of R&D included:

- ***Basic*** — increases the fundamental knowledge necessary for developing infrastructure assurance technologies
- ***Applied*** — investigates the feasibility and practicality of proposed technological solutions
- ***Advanced technology development*** — includes efforts to develop technologies and test their feasibility, effectiveness, and interoperability
- ***Proof of principle and validation*** — evaluates the effectiveness of technologies in an infrastructure environment; assesses the performance, cost-effectiveness, and practicality of the technology from the perspective of the infrastructure

study, technology transfer activities that facilitate the integration of "research" and "development" are qualitatively considered.

Study Results

The study team identified more than 70 R&D topics. Roadmapping information — R&D goals and challenges for three timeframes (near-term [before 2002], before 2005, before 2010), rationale, priority, and estimated resource requirements — was developed for each topic. The team, consisting of representatives from government, industry, academia and research institutes, and the Department of Energy national laboratories, also solicited input from, and coordinated with, numerous experts and stakeholders from their respective areas of representation in developing the topics and roadmapping information.

The estimates of resource requirements reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and

Summary of Roadmapping Results

- Over 70 R&D topics were identified to address infrastructure assurance needs across the eight infrastructures. The following themes describe the focus of these topics:
  - **Vulnerability Assessment** —assess the vulnerability of components, systems, and infrastructures.
  - **Information Assurance** — secure information while it is stored, being processed, and in transit.
  - **Monitoring and Detection** — monitor systems, detect threats and intrusions, and provide timely warning.
  - **Protection and Mitigation** — physically protect infrastructures and mitigate damage.
  - **Response and Recovery** — aid in rapid incident response and recovery.
  - **Modeling and Simulation** — develop models of components, systems, and infrastructures and examine the efficacy of alternative infrastructure assurance strategies and technologies.
  - **Systems Analysis** — analyze complex systems and identify and analyze infrastructure interdependencies.
  - **Decision Support** — support timely decision making with tools, methodologies, and information systems.
  - **Risk Management** — determine where best to allocate resources and how to manage risks.
- Estimated resource requirements for the R&D topics total approximately $7 billion.
- Investments beyond those associated with R&D in the critical infrastructures are needed to address interdependency and complexity.

are based on assumptions concerning the scope, the expected level of effort, and the pace of the research.

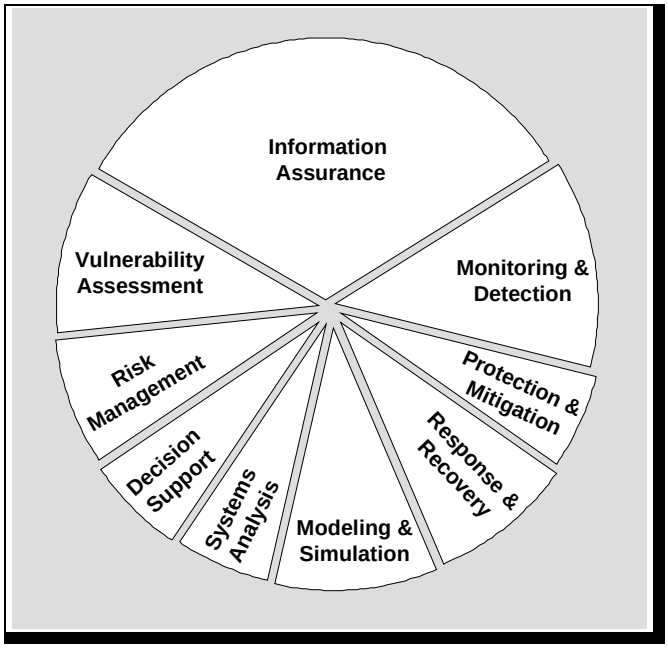
A number of common themes are evident within the R&D topics. Some of the themes directly correlate with the objectives of infrastructure assurance — to reduce critical vulnerabilities by protecting infrastructures, detecting intrusions, mitigating the effects of disruptions, assisting in the management of incidents, and facilitating recovery. Other themes focus on developing analytical or supporting technologies to help meet those objectives. Vulnerability assessment provides supporting baseline information for all of the other themes.

Estimated near-term (FY2000–FY2002) and mid-term (FY2003–FY2005) resource requirements total approximately $2 billion each, while long-term (FY2006–FY2010) resource requirements are estimated to be approximately $3 billion. A breakdown of near-term resource requirements by theme shows that information-assurance-related R&D requires approximately one-third of the total estimated resources. Monitoring and detection R&D represents about 15% of the portfolio, while vulnerability assessment and modeling and simulation each represent approximately 10%.

Included within each theme are elements that apply to, or crosscut, multiple infrastructures. With careful R&D planning and coordination, crosscutting elements could be combined into focused R&D areas to capitalize on synergies and reduce investment requirements.

R&D efforts need to focus on interdependencies and system complexity. The identification of interdependencies among national infrastructures and the characterization of how damage can propagate (cascade) across multiple infrastructures is a high priority.

Relevant ongoing and new R&D activities should be viewed as an integrated portfolio designed to meet strategic, technical, and programmatic infrastructure assurance objectives. Strategically, the portfolio should support the timely development of technologies to protect and assure critical infrastructures. Technically, the portfolio should include basic, applied, advanced technology development, and proof-of-principle and validation research. Programmatically, the portfolio should include R&D projects that, to the



extent possible, comprehensively address requirements of the various infrastructures.

Successful implementation of technologies from government-funded R&D requires close cooperation with industry and the private-sector owners and operators of our nation's infrastructures. Technology transfer and embedding should be integral parts of the R&D process. A technology transfer plan should be prepared along with an R&D plan to elevate the awareness of the issues and accelerate the introduction of infrastructure assurance technologies.

R&D must be consistent with, and responsive to, national infrastructure assurance policy. Such policy provides a framework for establishing R&D objectives, setting R&D priorities, and shaping a multiyear, multifaceted R&D portfolio that is commensurate in scope and scale with the physical and cyber challenges of the twenty-first century. Moreover, it provides a framework for establishing education and awareness programs, building partnerships with industry, and developing legislative initiatives intended to reduce vulnerabilities.

Next Step Recommendations

- Formally validated infrastructure assurance requirements (needs), a baseline inventory of ongoing infrastructure-assurance-related R&D activities, and an inventory of applicable commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) technology should be developed. All of these elements are essential to ensure that:
  - The R&D roadmap comprehensively addresses needs;
  - Individual R&D topics are not addressed elsewhere; and
  - New research efforts focus on critical R&D gaps.
- Various forums, such as conferences, workshops, and joint planning meetings, should be established. These forums would bring together researchers, private-sector infrastructure owners and operators, and government agencies to discuss common problems and requirements, to establish research agenda, and to promote creative thinking to solve infrastructure problems.

Section 1
Introduction

Research and development are not presently adequate to support infrastructure protection. … [T]here is a need for additional technology with which to protect our essential systems.

Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," October 1997

1.1 Purpose

In July 1996, the President signed Executive Order 13010, which created a joint government and private-sector Commission — the President's Commission on Critical Infrastructure Protection. The Commission's goal was to develop a national strategy for protecting our critical infrastructures from a spectrum of threats and for assuring their continued operation. Eight critical infrastructures were identified: banking and finance; electric power; oil and gas production and storage; emergency services; government services; information and communications; transportation; and water supply.

After 15 months of evaluating these infrastructures, assessing their vulnerabilities, and deliberating assurance alternatives, the Commission submitted its report — *Critical Foundations: Protecting America's Infrastructures* — to the President. Among its findings, the Commission identified research and development (R&D) as a key element of a multifaceted infrastructure assurance strategy. This strategy incorporates R&D, information sharing, education and awareness, legal initiatives, and establishment of national structures to facilitate an effective partnership among the federal government, state and local governments, and infrastructure owners and operators. The Commission also recommended specific areas for research and initial levels of investment to provide the required technologies.

This report presents the results of a four-month R&D study conducted by the Commission's Transition Office. The purpose of this study was to define preliminary infrastructure assurance R&D areas, investment requirements, and associated roadmapping information. The study builds on work previously conducted by the Commission and provides a foundation for the next steps in developing a national infrastructure assurance R&D program. The goal of the R&D is to support the development of technologies that address the threats to, and vulnerabilities of, critical infrastructures that have the potential for causing significant impacts to our national security, economy, and/or social structure.

1.2 Scope of the R&D Study

The critical infrastructure sectors identified in Executive Order 13010 were addressed in this study. A timeframe of approximately 10 years, beginning in fiscal year (FY) 2000, was considered, although longer term needs were addressed in selected areas. The primary emphasis was on near-term R&D activities that would reduce critical vulnerabilities by protecting infrastructures, detecting intrusions, mitigating the effects of disruptions (incidents), assisting in the management of incidents, and facilitating recovery.

To the extent possible, this study focused on perceived technology shortfalls, or "gaps," between infrastructure assurance technology needs and available technologies. (Technology, broadly defined, includes processes, systems, models and simulations, hardware, and software.) However, given the breadth of R&D activities across the federal government and in the private sector, some of the recommended R&D may be addressed, at least in part, by other programs that may not focus specifically on infrastructure assurance. For example, portions of existing programs on force protection, information security and survivability, chemical and biological defense, and counterproliferation are likely to apply to infrastructure assurance as well. Additional efforts are needed to catalog such programs and establish a baseline of information to minimize duplication of effort, identify potential synergies among programs, and focus new research efforts on critical gaps not addressed elsewhere.

Table 1.1 defines the categories of research considered in this study. The emphasis was on research that requires government investment. However, as Figure 1.1 illustrates, this research must be accompanied by technology development within the private sector to meet infrastructure assurance objectives. Although such private-sector development was beyond the scope of this study, technology transfer activities that facilitate the integration of "research" and "development" were qualitatively considered.

Both physical and cyber threats were considered. The former include threats to tangible property, while the latter include electronic, radio-frequency, or

Table 1.1 Research Categories

Basic research — increases the fundamental knowledge necessary for developing infrastructure assurance technologies
Applied research — investigates the feasibility and practicality of proposed technological solutions, including studies and investigations of system-specific and non-system-specific technologies
Advanced technology development — includes efforts to develop technologies and test their feasibility, effectiveness, and interoperability
Proof of principle and validation — evaluates the effectiveness of technologies in an infrastructure environment (e.g., test beds); assesses the performance, cost-effectiveness, and practicality of the technology from the perspective of the infrastructure

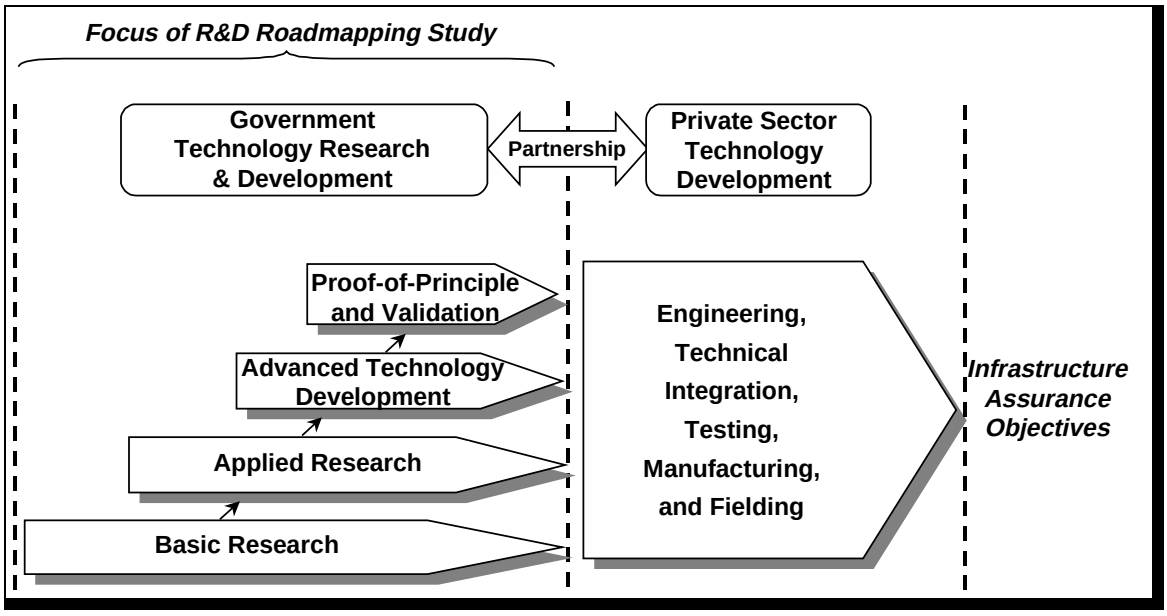


Figure 1.1 Government and Private-sector Partnership for Meeting Infrastructure Assurance Objectives

computer-based attacks on the information infrastructure or its components. Threats from aging infrastructure and natural disasters were outside the scope of this effort, although some of the recommended research could address problems in these areas.

Intrinsic threats from the growing complexity of, and interdependence among, infrastructures also were considered. Such threats increase the possibility that a rather minor, routine disturbance can cascade into a major problem that involves multiple infrastructures. These dependencies among infrastructures reflect multidimensional risk profiles and challenges that require comprehensive assurance planning based on innovative R&D.

1.3 Sector Study Teams

As depicted in Figure 1.2, five infrastructure sector study teams and an integration team were formed to develop roadmapping information for the eight critical infrastructures. This consolidation allowed the teams to study infrastructures with similar technology needs together. For example, the Energy Team addressed both the electric power and the oil and natural gas production and storage infrastructures, while the Vital Human Services Team addressed the water-supply system, emergency services, and government services infrastructures. The Integration Team coordinated the overall roadmapping activity, identified common research topics, examined interdependencies among the infrastructures, and integrated the sector roadmapping information.

To ensure a balanced R&D perspective, promote partnership, and facilitate outreach, each sector study team consisted of at least four members and a coordinator. The members represented government, industry, academia and research institutes, and the national laboratories (Figure 1.2). Team members solicited input from, and coordinated with, experts and stakeholders from their respective areas of representation.

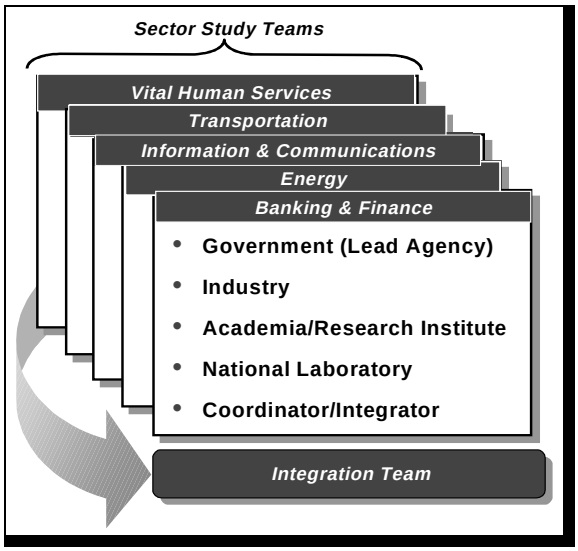


Figure 1.2 Structure of the Sector Study Teams

1.4 Study Approach

The substantial body of information previously developed by and for the Commission provided the foundation for this study. This information included the *Critical Foundations* report, a series of comprehensive sector reports, and several R&D reports that contained initial recommendations for protecting and assuring critical national infrastructures. The sector study teams also drew upon recent studies conducted by government organizations; advisory groups, committees, and task forces; industrial organizations; academic institutes; and national laboratories. This approach allowed the teams to identify related efforts, gain valuable insights and perspectives, and identify recurring topics.

In preparing its roadmap, each sector study team examined threats and vulnerabilities, identified key structural and regulatory issues, and formed assumptions about trends that could affect future infrastructure assurance. This effort required extensive interaction among team members, as well as with external subject-matter experts and stakeholders. In addition, each team held one or more meetings that included both team members and other experts from government, industry, academia and research institutes, and the national laboratories. These meetings provided a forum for discussing infrastructure assurance and technology transfer issues and for developing roadmapping information. Engaging external reviewers from the various areas of representation also ensured that the recommendations were comprehensive and meaningful.

Table 1.2 identifies the elements included in the sector roadmaps. Although all of the R&D recommendations were judged to be important, three priority categories were established (i.e., most important, very important, important). In prioritizing the R&D topics, the teams considered a number of interrelated factors, including the extent to which the research, if successful, would be expected to reduce vulnerabilities, lessen the effects of incidents, assist in managing incidents, or speed recovery activities after incidents. Other factors considered were the magnitude of the potential consequences that

would be prevented or mitigated and the importance of the research for ensuring national security and the economy.

Estimates of resource requirements were prepared for each R&D topic. The estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

In identifying R&D topics, the teams stressed partnership between government and the private sector. It was recognized explicitly that infrastructure risks affect both the public and private sectors. Also, the private sector holds much of the relevant technical and empirical data on infrastructure operations, interdependencies, and vulnerabilities. Further, the private sector generally develops technology only when it identifies a market for it. Therefore, successful implementation of technologies from government-funded research efforts requires close cooperation with industry and the private-sector owners and operators of our nation's infrastructures.

Table 1.2 Roadmapping Information

R&D topics — specific R&D that should be conducted and the expected product.
Goals and challenges — the performance goals for the R&D for three timeframes and the associated technical challenges.
Rationale — why the research is important (e.g., prevention, detection, mitigation, incident management, or recovery) and the risks of not having the technology available.
Priority — the relative priority of the R&D topic (most important, very important, or important).
Timeframe — the time needed to conduct the recommended R&D, including phases and sequencing.
Resource requirements — the estimated level of resources, as a function of time, needed to complete the research.

1.5 Report Organization

The remainder of this report is organized as follows. Section 2 summarizes R&D topics and preliminary roadmapping information for the five infrastructure sectors. Section 3 presents integrated roadmapping information, including estimated resource requirements. Section 4 presents recommendations for the next steps to take in future roadmapping and planning efforts. Finally, five attachments (tabs) provide detailed roadmapping information for the five infrastructure sectors. Tabs A–E provide R&D roadmapping information for the Banking and Finance, Energy, Information and Communications, Transportation, and Vital Human Services sectors, respectively.

Section 2
Sector R&D Topics and Roadmaps

Research and development topics and roadmapping information for the five infrastructure sectors are summarized below. To put this information into perspective, a brief description of each sector is provided along with an overview of the issues and trends that affect the infrastructure. A summary of the threats to, and vulnerabilities of, the infrastructure is also provided. (Detailed infrastructure sector reports are provided in Tabs A–E.)

2.1 Banking and Finance

2.1.1 Infrastructure Overview

The banking and finance infrastructure consists of institutions, agencies, and support systems (physical, procedural, and data) that facilitate lending, borrowing, issuing, trading in, or caring for money, credit, and other representations of value. This infrastructure includes banks and credit unions; insurance companies; lending and credit institutions of all kinds; securities and commodities dealers; state, federal, and international oversight and regulatory agencies; and the web of communications equipment and linkages that support transactions among those systems.

2.1.2 Issues and Trends

Several emerging trends threaten the safety and soundness of the banking and finance infrastructure. These trends include:

- Deregulation and increased competition, which can result in less marginal capability to absorb the costs of added security measures.

- Convergence of technologies in computing, communications, networking, and encryption, which increases the efficiency and flexibility of transaction support, but can add vulnerabilities.

- Internationalization of commerce, which gives new, nondomestic entities unprecedented access to U.S. systems and information.

- Changing definitions of value. For example, the *form* of money and the *way* that information about money are managed have become valuable assets.

The effect of these trends on the U.S. banking and finance infrastructure can be moderated by the way in which government and industry respond to four challenges:

- Making policy trade-offs to balance competing goals among open markets, regulatory management, national security, and free trade;
- Adapting to the technical revolution in two infrastructures: (1) information and communications and (2) banking and finance;
- Accommodating the internationalization of commerce and information; and
- Defining new assets that require protection.

2.1.3 Threats and Vulnerabilities

Potential threats to, and vulnerabilities of, the banking and finance infrastructure originate from the lack of a clear understanding of how alternative responses in each of four areas might affect the industry.

Regulation and Control

If the architecture and dynamics of the banking and finance infrastructure are not well understood, the regulatory regimes intended to maintain the safety and surety of that infrastructure would be rapidly overcome by changes in technology, markets, and practices in the industry. The nexus between the concerns of the banking and finance infrastructure and those of the information and communications infrastructure is becoming so complex that policies developed in one area can have serious, unintended consequences to the other.

New Technologies

As the banking and finance community adopts new technologies to streamline transactions, the systems that support those transactions become more complex and difficult to secure. The efficiency, flexibility, and adaptability that make the new technologies attractive to the industry also create subtle (and potentially catastrophic) weaknesses in the system. Innovative use of the new technologies makes it possible for each point of presence in the infrastructure network to create a customized interface to the industry. Without proper protection and management, each point of presence can become a point of entry for someone intending to do harm to, or through, the infrastructure.

Internationalization of Markets

As the banking and finance infrastructure becomes more open to world commerce, many nondomestic points of presence enter the networks. Domestic standards and practice may not be the norm for such entities. These differences may result in

unforeseen vulnerabilities. In addition, the hardware and software that exemplify the new technologies may originate from nondomestic manufacturers and suppliers. The standards and practices by which these items are integrated into the infrastructure must take into account the potential vulnerabilities.

Financial Information

As individual entities and systems are integrated into the banking and finance infrastructure, the information collected, stored, and transmitted among various points of presence becomes more vulnerable to manipulation, disclosure, or destruction. Methods and techniques for securing both the system and the information it handles must keep pace with the points of presence and the sophistication of technologies available.

2.1.4 Summary of R&D Topics and Roadmaps

Table 2.1 summarizes the R&D topics and their corresponding roadmaps for the banking and finance infrastructure. The table provides brief descriptions of research topics grouped by priority (i.e., most important, very important, important); summaries of research activities for three timeframes (near-term [before 2002], before 2005, and before 2010); and *estimates* of the financial resources required to support the R&D activities for each timeframe. Table A contains more detailed descriptions of these research topics, supporting rationale, goals and challenges, threats and vulnerabilities addressed by the research, and research roadmap information.

Table 2.1 Summary of Banking and Finance R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
		Most Important R&D Topics	
1	Simulation Model Development	Development and maintenance of a simulation model of the banking and finance infrastructure and analysis of management alternatives and policies. (A, ATD, POP)	**Near-term:** Engage industry and design, develop, maintain, and elaborate a constructive strategic simulation model (CSSM). ($18 million) ~**2005:** Develop the requirements, legal basis, policies, and techniques for protecting the sensitive, proprietary, and classified data required for the CSSM. Leverage existing work, models, mechanisms, etc. ($10 million) **~2010:** Prepare field operational model and life-cycle management plan. ($1 million)
2	Information Security Analysis	Analysis and evaluation of current cryptographic and surety analysis technology applications. Transfer and development or adaptation of new technologies. (B, A, ATD, POP)	**Near-term:** Develop a legal and procedural basis for expediting access to government off-the-shelf cryptographic analysis and surety analysis technology. Analyze and evaluate the efficacy of implementations of cryptographic and surety technologies. Develop and validate security implementation standards for banking and finance information applications (scaleable, supporting variable security levels). ($32 million) **~2005:** Implement anonymity balance. Field scaleable key public management systems. ($6 million) **~2010:** Field entity authentication technologies. ($1 million)
		Very Important R&D Topics	
3	Intrusion Indication and Warning (I&W) Tools	Development of tools for detecting, discriminating, and managing intrusions and anomalies in information systems. (B, A, ATD, POP)	**Near-term:** Use insight from the development of the CSSM to determine where within the system I&W and sensitivity tools and techniques are applicable. Determine what data are required to implement those tools and techniques. ($29 million) ~**2005:** Develop an initial suite of tools. ($7 million) **~2010:** Field operational tools. ($1 million)
4	Systems Reliability Enhancement	Development and transfer of high-reliability trusted systems, network security agents, self-healing systems, and dynamic configurable firewalls. (B, A, ATD, POP)	**Near-term:** Develop, publish, and begin to implement initial standards and specifications. Develop prototypes of network security agents. ($54 million) ~**2005:** Complete implementation of standards and specifications, and prototypes of network security agents. ($15 million) **~2010:** Field prototypes of self-healing systems, configurable firewalls, and network defense agents. ($2 million)
		Important R&D Topics	
5	Information System Standardization	Development of an open architecture standard for the banking and finance infrastructure. (A)	**Near-term:** Publish initial standards for open architecture. ($6 million)
6	Electronic Commerce Security Enhancement	Development and implementation of networking equipment and standards for managing security of electronic commerce. (B, A, ATD, POP)	**Near-term:** Publish initial standards and specifications for equipment and support tools. ($9 million) ~**2005:** Field standards. ($9 million) **~2010:** Field operational tools. ($3 million)

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

2.2 Energy

2.2.1 Infrastructure Overview

The energy infrastructure includes electric power, oil, and natural gas. Each requires production, processing, and transportation to provide energy to customers, including residential, commercial, industrial, and government end users. Production consists of generation of electricity by power plants and well-head extraction of both oil and natural gas. Each requires large, complex transportation networks to deliver energy to end users. Each has transmission and distribution lines. Electric power requires substations and transformers; oil requires pumping stations and refineries; and natural gas requires compressor stations and gas processing centers. Storage is also a key component for oil and natural gas and is becoming a major component for electricity.

In addition to the physical components that comprise these three networks, each infrastructure uses Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems help to monitor and operate the physical components and can increase efficiency and safety within the infrastructure. Also, each of these infrastructures depends on other infrastructures, including information and communications and transportation systems, for operation.

These energy infrastructures are highly interdependent. Many electrical generating plants consume natural gas and oil. Electricity is required to operate petroleum refineries and pumping stations as well as most natural gas appliances. Even motor gasoline cannot be pumped without electricity.

2.2.2 Issues and Trends

The energy infrastructures (electric power, oil, natural gas) are essential to the quality of life in our society. When one or more of these energy infrastructures fail, then, in addition to personal and economic losses, this failure generates significant negative attitudes about the quality of life in our society. Our society and economy depend heavily on reliable and sustainable energy sources, such as electricity to operate our computers, gasoline to fuel our vehicles, and natural gas to heat our homes. Some of the emerging issues and trends in the energy infrastructure include the following:

- Deregulation and rapid restructuring are occurring in both the electric power and the natural gas industries, which is designed to enhance the competitive environment.

- The emphasis on competition is reducing operating margins, thereby increasing the likelihood of system disturbances from small events.

- Marketing companies, mergers and acquisitions, and competitive markets are changing the way in which commodities are purchased, and they test the energy infrastructure in new ways.

- Reduced investments in new technology create the potential for less reliable operation and additional disruptions in supply.

- The age of critical energy components, combined with decreasing operating budgets, represents a potential concern.

- Downsizing of the energy industry creates the potential for disgruntled "insiders" and a significant loss of expertise.

- The "not-in-my-backyard" attitude severely limits the number of new rights-of-way, which are needed for electric transmission lines and natural gas and oil pipelines.

- Increased dependence on information systems based on open architectures, centralized operations, increased communication over public networks, and remote maintenance creates additional vulnerabilities.

- Our dependence on foreign supplies and vendors raises concerns about the reliability of our energy supplies.

- Reliance on automated systems increases vulnerability to technological failure and cyber attacks.

2.2.3 Threats and Vulnerabilities

Threats to the U.S. energy system arise from a number of sources, including hostile governments, terrorist groups, other organized groups, disgruntled employees, malicious intruders, natural disasters, accidents, system complexities, and dependence on other infrastructures. The U.S. Department of Energy has documented more than 1,000 incidents directed against the U.S. energy system over the past 15 years; some supply disruptions have caused significant damage.

Well-organized groups (perhaps working with insiders) can cause massive physical and cyber damage to our energy supply systems. These groups could damage the system so severely that major cities, or multistate regions, could suffer severe, long-term energy shortages.

Furthermore, cyber vulnerabilities are rapidly increasing, as the industry becomes more automated and interconnected. While there are relatively few documented cases of insider attacks on computers, the reality is that a knowledgeable insider has an almost unlimited ability to cause problems, from bypassing access authorization to subverting systems.

The electric power and oil and natural gas infrastructures face many vulnerabilities, including the following:

- Those created in the operating system because of the rapid introduction of information systems based on open architectures, centralized operations, and increased communications over public telecommunications networks.

- SCADA systems because they often use common commercial hardware and software, connect to other company networks, and rely on dial-back modems that can be bypassed.

- Increased availability of vulnerability information, much of which is mandated by regulatory bodies to facilitate competition, and the availability of tools to exploit those vulnerabilities.

- Rapid assimilation of advanced technologies with inherent complexities.

- Consolidation of infrastructure corridors (e.g., communications, electric transmission lines, pipelines).

- Complexity of the system so that a failure is possible, either from accidental events or a deliberate attack, when the system has minimum capacity reserves and energy transfers are large.

2.2.4 Summary of R&D Topics and Roadmaps

Table 2.2 summarizes R&D topics and their corresponding roadmaps for the energy infrastructure. The table provides brief descriptions of research topics grouped by priority (i.e., most important, very important, important); summaries of research activities for three timeframes (near-term [before 2002], before 2005, before 2010); and *estimates* of the financial resources required to support the R&D activities for each timeframe. Tab B contains more detailed descriptions of these research topics, supporting rationale, goals and challenges, threats and vulnerabilities addressed by the research, and research roadmap information.

Table 2.2 Summary of Energy R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
		Most Important R&D Topics	
1	Real-time Control Mechanisms	Integration of real-time control systems to support timely decisions involving electric grid operations. System includes instrumentation and monitoring, models and simulations, control methods, and decision support tools.	(See topics 1.1–1.4 for roadmapping information.)
1.1	Instrumentation and Monitoring for Distributed Control	Applied research and technology development to produce hardware and software systems designed to collect and manage large data streams for implementing real-time control systems. (A, ATD)	**Near-term:** Implement common data model and identify measurement requirements. ($5 million) **~2005:** Develop advanced sensors, measurement timing standards, and data compression tools. Establish high bandwidth communication channels. ($32 million) **~2010:** Establish wide area monitoring, data storage and retrieval, and adaptive monitoring methods. ($57 million)
1.2	Analysis and Computation for Large-scale Systems	Basic research, technology development, and proof-of-principle pilots to develop advanced simulation techniques, user-friendly interfaces, and expert systems for handling large volumes of information. (B, A, ATD, POP)	**Near-term:** Implement on-line security assessment tools. ($15 million) **~2005:** Establish stability indices. Develop measurement-based analysis tools and parameters for integrating measurement- and model-based tools. ($37 million) **~2010:** Establish uncertainty theory and implement integrated analytical approach. ($48 million)
1.3	Advanced Control Methods	Primarily basic research to develop a new control theory for large-scale systems. Theory will apply to other large-scale systems (e.g., space structures). (B, POP)	**Near-term:** Assess current state of robust control theory and decentralized control theory. ($8 million) **~2005:** Advance theoretical basis for robust and decentralized control. ($32 million) **~2010:** Develop proof of principle and validation on integrated large-scale system control theory. ($48 million)
1.4	Decision Support Tools	Basic research to technology development of hardware and software systems to support real-time decision making. (B, A, ATD, POP)	**Near-term:** Develop new visualization techniques and operator interfaces for increased data volume. ($6 million) **~2005:** Implement first-generation reasoning tools. Develop tools to assist operators in handling many transactions. ($10 million) **~2010:** Develop autonomous agents and implement multiconstraint optimization tools. ($33 million)

Table 2.2 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics (Cont.)			
2	Analysis of Scale and Complexity	Development of a better understanding of the stability of large electric power systems; effects of uncertainties and changing conditions on the system; effects of complexity and scale on the behavior of people involved with the system; large network interactions, voltage collapse, and network security; techniques to reduce complexity; and countermeasures to avoid and control malicious acts aimed at the system. (B, A, ATD, POP)	**Near-term:** Study restructuring effects on complexity. Develop theoretical understanding of complex systems and applied understanding of the evolving complexity of the power grid. ($45 million) **~2005:** Develop an understanding of human interfaces and how humans handle scale and complexity. Understand effects of uncertainties on vulnerability and develop mitigation methods. ($30 million)
3	Vulnerability Assessment	Assessment of vulnerabilities to support decisions regarding research and capital investment for electric power system assurance. (B, A)	**Near-term:** Complete systematic and current estimates of vulnerabilities and threats. Estimate impacts of outages. Define modeling requirements. Characterize restructuring effects. ($9 million) **~2005:** Develop or enhance models. Analyze restructuring impacts. Evaluate infrastructure assurance options. ($9 million) **~2010:** Develop improved procedures and evaluate more options. ($14 million)
9	Critical Consequence Analysis	Development of models of the natural gas network to evaluate system vulnerability and response to incidents. (B, A)	**Near-term:** Complete and implement basic design of model. ($2 million) **~2005:** Develop incident/failure scenarios and consequence analysis, including curtailment impacts, by using the model. ($1 million)
10	Decision Support Systems	Development and implementation of risk management and decision support tools to allow natural gas and oil industry decision makers to prioritize resources, minimize risk, and respond to incidents. (B, A, ATD, POP)	**Near-term:** Assess data and tools. Assign decision analysis requirements with priorities. ($36 million) **~2005:** Develop expert system tools. Make models for highest priority items. Assess secondary priority items. ($36 million) **~2010:** Continue to develop high-priority items. Develop expert system tools and models for secondary priority items. ($48 million)
11	Physical Protection Assessment	Assessment of the physical assets of the natural gas and oil industry, vulnerable nodes, protection methods, and protection strategies. (B, A)	**Near-term:** Collect historic reports and data. Survey industry to determine highest vulnerabilities. Assess technology. Develop and implement strategies. ($5 million)
14	Cyber Protection Enhancement	Development of enhanced security measures for natural gas system SCADA control systems and electronic commerce. (B, A, ATD, POP)	**Near-term:** Identify encryption algorithms and standards. ($25 million) **~2005:** Complete technology review and selection. Manufacture chips. ($50 million) **~2010:** Implement **e**nhanced protection system for SCADA and electronic commerce. Obtain acceptance of approved standards by industry. ($126 million)

Table 2.2 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics (Cont.)			
16	Institutional Barriers	Investigation of the institutional issues that are potential impediments to the achievement of energy system infrastructure assurance objectives. (A)	**Near-term:** Develop partnerships. ($13 million) **~2005:** Develop tools and roles and establish priorities. ($15 million) **~2010:** Maintain support and networking needs, such as the FBI security center. ($45 million)
17	Infrastructure Interdependencies	Investigation of the interdependencies within the energy system (e.g., gas and electricity generation) and between the energy system and other infrastructures. (B, A, ATD)	**Near-term:** Relate technical complexities to business disruptions and economic losses. Complete in-depth analysis of technical impacts. Examine requirements for advanced computational modeling and simulation tools. ($6 million) **~2005:** Identify and analyze options to reduce interdependency impacts. Develop analysis tools. ($5 million) **~2010:** Obtain results of analyzing options to reduce interdependency-related vulnerabilities. ($11 million)
Very Important R&D Topics			
4	Information Assurance and Cyber Security	Development of cyber threat assessment and risk management tools for the electric power system. Understand complexity of large, dispersed information systems. Develop high-security SCADA network architectures. Develop efficient encryption techniques for the electric power system. Develop authentication/ authorization tools. Develop improved cyber intrusion detection techniques. Develop threat analysis of high-frequency weapons on information systems.	(See topics 4.1–4.7 for roadmapping information.)
4.1	Threat Assessment and Risk Management	Applied and technology R&D to develop tools to help designers safely move the electric power industry into a more interconnected, market-based system. (A, ATD)	**Near-term:** Conduct systematic, industry-wide threat assessment and vulnerability mapping. Develop base risk management tools. ($15 million) **~2005:** Develop standardized, industry-wide threat model. Integrate risk management tools into design tools. Ensure consistent models are used to define threat environments and assess risk. Integrate models into design and validation tools. ($10 million)
4.2	Large Systems Analysis	Basic and applied research to develop and extend models to ensure the stability of the electric system in the face of faults, cyber attacks, and other assaults. (B, A, ATD, POP)	**Near-term:** Develop basic models and simulations and basic design tools. ($13 million) **~2005:** Develop integrated models and near real-time prediction, model-based control. ($14 million) **~2010:** Validate the entire power grid. Incorporate models into design. Develop simulation and validation tools. ($18 million)

Table 2.2 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Very Important R&D Topics (Cont.)			
4.3	High-security SCADA Systems	Applied research to develop high-security SCADA systems for electric power. Results include design guidelines, design tools, models, test and evaluation tools. (A)	**Near-term** Develop a baseline understanding of existing systems and current industry practices. Develop design guidelines. ($24 million) **~2005:** Develop and validate proof of concept. Standardize efforts for deployment of new SCADA networks. ($24 million) **~2010:** Produce and adopt standard SCADA design guidelines. ($32 million)
4.4	Efficient, Adaptable Encryption	Basic and applied research to develop and implement encryption technologies that have minimal downside impacts on operations. (B, A)	**Near-term:** Develop a baseline understanding of requirements for major system areas. Evaluate encryption technologies. ($22 million) **~2005:** Deploy encryption technologies throughout the power industry. ($23 million) **~2010:** Deploy dynamic and high-bandwidth encryption. ($30 million)
4.5	Robust Authentication and Authorization	Basic and applied research is needed to develop and deploy strong authentication and authorization controls to both the SCADA and information networks in the electric power industry. (B, A, ATD)	**Near-term:** Map the requirements for authentication and authorization of existing systems. Define general-purpose, scaleable mechanisms. Begin working with standards. ($22 million) **~2005:** Work with the electric power industry and product manufactures to adopt standardized mechanisms. ($23 million) **~2010:** Implement standardized authentication and authorization models on all new systems added to the grid. ($30 million)
4.6	Intrusion Detection	Basic and applied research to detect probes, penetrations and attacks on information systems. Probes and attacks must be detected quickly to trigger a response. (B, A, ATD)	**Near-term:** Develop understanding of threats and current vulnerabilities. Deploy threat detection to both the communication and control infrastructure of the grid. ($22 million) **~2005:** Develop and deploy efficient, dynamic intrusion detection tools. ($23 million) **~2010:** Link intrusion detection into central threat center for grid-wide system monitoring. Deploy automated response capability. ($30 million)
4.7	Directed Energy Weapons Countermeasures	Basic and applied research to examine the vulnerability of the electric power grid to high-energy radio frequency weapons. Research needed to protect information systems and critical electric system components. (B, A)	**Near-term:** Develop understanding of the current state of high-energy weapons. Construct and test devices. Develop test bed. Prepare design guidelines for protection. ($18 million) **~2005:** Integrate information learned into overall design tools. ($18 million) **~2010:** Conduct further research into protecting against directed weapons. ($24 million)

Table 2.2 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Very Important R&D Topics (Cont.)			
5	Emergency Response and Recovery Information Technologies	Development of emergency response and recovery protocols and procedures for information technology systems within electric power grids. (B, A)	**Near-term:** Develop concept. Identify critical components and protection and mitigation strategies. Begin developing exercise process and computer simulation models. ($2 million) **~2005:** Conduct exercises on a periodic basis. Develop and apply lessons learned from exercises. Begin developing concept for oil and natural gas pipeline networks. ($3 million) **~2010:** Refine process as changes warrant. Begin conducting exercises for oil and gas pipeline networks. ($4 million)
6	Transmission and Distribution Technologies	Development of advanced technology to increase the security of electric power transmission and distribution. (ATD, POP)	**Near-term:** Examine specific infrastructure assurance contributions for several R&D topics. Improve siting and environmental impact process for new transmission lines. ($100 million) **~2005:** Develop hardware and software. Complete proof of principle for smart instrumentation and control systems. Make progress in advanced power electronics systems. ($100 million) **~2010:** Achieve significant progress in superconducting technologies. Implement advanced power electronics systems. ($166 million)
12	Multisensor and Warning Technologies	Development and implementation of a multisensor system that warns of attempted intrusions. (B, A, ATD, POP)	**Near-term:** Assess current technologies. Design needed technologies. Establish industry-government partnership. ($28 million) **~2005:** Roadmap national technologies. Develop software and hardware. ($31 million) **~2010:** Implement technology pilot program. Commercially develop technologies. Set up an oversight committee. ($101 million)
15	Evaluation of Policy Effects	Study of the cause-and-effect relationships among laws, directives, operating policies, standards, and vulnerability of the energy system. (B, A)	**Near-term:** Determine the effect of numerous proposed policies on vulnerability and security of energy systems. Explore grid operation implications. ($29 million) **~2005:** Establish college programs with technical and public policy aspects of infrastructure assurance. ($6 million)
Important R&D Topics			
7	On-line Security Assessment	Development of algorithms, models, and methods for on-line, near-real-time assessments of the safe operation of the electric power system. (B, A, ATD)	**Near-term:** Examine incremental algorithms for system perturbations. Obtain 1,000-fold increase in speed with subcycle state information. Develop database replication techniques. ($10 million) **~2005:** Reduce cost and running times. Develop accurate tools and models for the national grid. Develop tools for geographic decomposition in nonsymmetric complex cases. ($10 million) **~2010:** Develop and implement improved and new tools. Reduce cost and running times. ($16 million)

Table 2.2 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Important R&D Topics (Cont.)			
8	Dispersed Generation and Backup Infrastructures	Evaluation of the role of dispersed systems and backup systems in electric power generation; development of advanced technologies for these systems. (ATD, POP)	**Near-term:** Analyze infrastructure assurance benefits of dispersed generation. Prioritize options. ($20 million) **~2005:** Demonstrate and integrate distributed generation systems with storage. Demonstrate and control with custom power systems. Develop improved backup system. ($20 million) **~2010:** Continue reducing costs and improving reliability of technology options. Improve ability for systems to run unattended for long periods. ($33 million)
13	Emergency Response Capability Enhancement	Development of protocols and procedures for the gas and oil industry to respond to emergencies. (A)	**Near-term:** Develop industry-government partnership. Establish roles for government and industry. Identify technology gaps. ($22 million) **~2005:** Develop roles. Develop a national emergency plan. Begin technology implementations. ($30 million) **~2010:** Ensure that technologies and best practices are widely implemented in industry. ($100 million)

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

2.3 Information and Communications

2.3.1 Infrastructure Overview

The information and communications infrastructure has three components: an underlying "link" for moving data, a network and transport component, and computing systems. The underlying physical link moves data from point to point (e.g., satellites, copper wire, optic fibers, wireless transmissions). The network and transport component is hardware (e.g., circuit switches) and software (e.g., control systems) that deal with addressing, routing, and data transport services. The computing systems generate, manipulate, store, display, or control information.

The combination of these components provides the communication, computation, control, information, and human collaboration systems that are critical to the functioning of other infrastructures and society. This highly complex infrastructure depends on interconnected multiple carriers across the nation and integrated advanced system hardware and software components. This infrastructure also forms the backbone of the Internet and connects with computer networks and communication networks on an international level.

2.3.2 Issues and Trends

The explosive growth of the Internet and its incorporation into business through the World Wide Web — for advertising products and services, electronic mail communications, and electronic commerce — have imposed an expanding new communications medium over the infrastructure. In addition to traditional telephone services, this infrastructure is increasingly being required to support Internet communications and new services. The interconnection of computer networks at an international level facilitates communications across countries without the traditional protections and protocols imposed by geographic boundaries. Information can be disseminated around the world in seconds through the Internet.

The increasing use of sophisticated computer control systems for the information and communications (telecommunications) infrastructure has introduced new technologies through additional hardware and software components and communications protocols. Further, the interconnection of multiple carriers and equipment types adds a new dimension in complexity.

Developments in technology and new security products continue to increase. Much of this development and manufacturing work is being done at non-U.S. locations by wholly or partly foreign-owned companies. This trend has the potential to introduce unknown vulnerabilities into systems and networks. The rapid growth of wireless and satellite communications to supplement wire lines adds a new aspect to telecommunications, and with it, a host of specialized technologies with exploitable vulnerabilities.

The telecommunications industry recently experienced many consolidations and mergers. These trends affect the implementation of security through corporate downsizing, reduced competition, and the potential for less diversity in product security.

Furthermore, other infrastructures depend more on the information and communications infrastructure for their continued operation. These infrastructures use remote control equipment (e.g., SCADA systems) more frequently, which creates a strong and direct dependency.

As the Internet becomes a medium of commerce, various legal issues in regard to the security of electronic commerce and privacy have emerged. The development and enforcement of laws to protect the Internet and systems are increasingly important areas that have not been definitively addressed.

2.3.3 Threats and Vulnerabilities

Threats to the information and communications infrastructure can come from many sources, such as deliberate attacks (cyber or physical) by insiders or outsiders, natural disasters, simple accidents, and failure of poorly designed or configured equipment. The goal is to continuously improve the protection of our systems and networks from security threats and vulnerabilities.

Because computer networks over the Internet are interconnected, an attack can originate from anywhere in the world. The traditional protection afforded by country boundaries and checkpoints is no longer sufficient. Systems are vulnerable because many networks are interconnected, and they are only as secure as the weakest link. This interconnection also provides intruders with a level of anonymity and impedes the ability to trace the specific location of an attack. The computing power available to intruders is becoming increasingly sophisticated, and advanced attack tools are available on the World Wide Web. Further, the design of security products often lags behind the technological capability of intruders to penetrate systems.

New technologies and features are launched rapidly in the telecommunications industry, potentially introducing new vulnerabilities as a result of incompatible protocols and interfaces. Moreover, technology that lacks component-level and integrated environment testing is used with other existing technologies in the network. Increasingly sophisticated hardware and software components and system control technologies have the potential to introduce design flaws, especially when these components are integrated into large-scale legacy systems. Finally, the increased loads on existing communications infrastructures, which have resulted from the expanded use of the Internet, place additional burdens on these systems.

2.3.4 Summary of R&D Topics and Roadmaps

Table 2.3 summarizes R&D topics and their corresponding roadmaps for the information and communications infrastructure. The table provides brief descriptions of research topics grouped by priority (i.e., most important, very important, important); summaries of research activities for three timeframes (near-term [before 2002], before 2005, and before 2010); and *estimates* of the financial resources required to support the R&D activities for each timeframe. Tab C contains more detailed descriptions of these research topics, supporting rationale, goals and challenges, threats and vulnerabilities addressed by the research, and research roadmap information.

Table 2.3 Summary of Information and Communications R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics			
1	Vulnerability Detection and Analysis	Identification, collection, and dissemination of vulnerability information; development of threat and vulnerability lexicon; development of methodologies and technologies to avoid, reduce, or eliminate vulnerabilities. (B, A, ATD)	**Near-term:** Develop lexicon and procedures for collecting, analyzing, and disseminating vulnerability information. ($90 million) **~2005:** Develop database to identify vulnerability information about the infrastructure. Develop metrics and measures to gauge the effectiveness of tools to detect and analyze vulnerabilities, and automate tools to detect vulnerabilities. ($90 million) **~2010:** Develop coordinated and scaleable tools for vulnerability detection and data notification at the national level. Establish international cooperation for collecting and sharing information on vulnerabilities. ($150 million)
4	Characterization and Notification of Threats	Collection of data, analysis, and development of tools to address threats to the information and communications infrastructure. (B, A)	**Near-term:** Develop procedures for collecting, analyzing, and disseminating threat data. ($25 million) ~**2005:** Implement national database of threat and response information. Profile potential attackers. ($30 million) **~2010:** Develop and distribute coordinated, national-level tools for threat notification. Establish international cooperation for collecting and sharing threat data. ($40 million)
5	Intrusion and Incident Detection and Warning	Development of efficient and cost-effective tools and methodologies for rapid incident detection and warning. (B, A, ATD)	**Near-term:** Develop manual tools and procedures to detect incidents and issue warnings. Establish metrics for assessing intrusion detection systems. ($90 million) **~2005:** Develop automated tools to detect incidents and issue warnings, strategy-based intrusion detection systems, automated trace-back tools, and scaleable detection systems. ($90 million) **~2010:** Develop scaleable tools at a national level to detect indications and warnings of an attack. Establish international cooperation and sharing of data on attacks. Create scaleable assessment tools to evaluate Internet threats. ($150 million)
6	Response, Recovery, and Reconstitution	Development of methods to contain, stop, or eject intruders; mitigate damage; and restore service. (B, A, ATD)	**Near-term:** Develop manual tools to detect, contain, and eject intruders, and to perform triage for recovery on attacked systems. ($95 million) **~2005:** Develop automated tools to detect, contain, and eject intruders, and perform triage for recovery on attacked systems. ($105 million) **~2010:** Continue development of automated tools to improve robustness, efficiency, and timely response in recovery. ($100 million)

Table 2.3 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics (Cont.)			
7	Security Architectures	Development of new and improved security architectures. (B, A, ATD)	**Near-term:** Establish methodologies for automated distribution of security patches. Prepare security implementation policies. ($125 million) **~2005:** Develop advanced firewall technologies and active, dynamic network technologies. ($150 million) **~2010:** Develop scaleable, robust security architectures to integrate security components. ($250 million)
8	Assurance Technologies	Development of tools and methodologies to implement new and improved assurance technologies. (B, A, ATD)	**Near-term:** Establish standards and methods of incorporating assurance into system development and complete product evaluation policies. ($95 million) **~2005:** Develop tools for efficient product evaluation and system-level evaluations. ($105 million) **~2010:** Continuously develop and refine methodologies and techniques for incorporating assurance into system development. ($175 million)
10	Management of Information Protection	Development of tools and methodologies for effective management of information protection in information and communication systems. (B, A, ATD)	**Near-term:** Research and develop concepts and techniques for protecting data and performing configuration management in local and remote infrastructure components. Define performance metrics for evaluating information protection. ($30 million) **~2005:** Research information protection concepts that carry use conditions, or metadata, with the information. Establish economic metrics for evaluating information protection. ($30 million) **~2010:** Continuously develop and refine measurement concepts, tools, and technologies for managing the protection of data in diverse environments. ($50 million)
Very Important R&D Topics			
2	Valuation of Information	Development of tools and methodologies to assist information owners in determining the value of their information and choosing cost-effective protective measures. (B, A)	**Near-term:** Develop manual tools, techniques and procedures to assess the value of information. ($30 million) **~2005:** Develop automated tools to assist information owners in assessing the value of information and determining appropriate levels of protection. ($30 million) **~2010:** Develop and refine automated tools to assist information owners in assessing the value of information and protection, including information that can be aggregated from multiple sources. ($50 million)
9	Advanced Concepts and Theory	Development of tools and methodologies to design and implement cost-effective security measures. (B, A, ATD)	**Near-term:** Establish standards, techniques, and procedures for software development. ($30 million) **~2005:** Research and develop ways to use expert systems in network management and to adaptively secure systems. ($30 million) **~2010:** Develop self-describing secure systems. ($50 million)

Table 2.3 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
		Very Important R&D Topics (Cont.)	
11	Characterization of Minimum Infrastructure for Essential Services	Identification of the critical elements in the information and communication infrastructure required to provide essential national, governmental, and military services. (A, ATD)	**Near-term:** Define and characterize minimum essential government and military communications, operations and services, and the required infrastructure to support those services. ($15 million) **~2005:** Establish interagency contingency and coordination plans and address the introduction of redundant systems in critical applications. ($15 million) **~2010:** Develop plans and deploy additional technologies to ensure redundancy as new technologies emerge and the scope of government services evolves. ($25 million)
13	Modeling and Simulation Tools	Development of tools and methodologies for simulating complex information and communication systems and architectures and can analyze alternative security configurations. (B, A, ATD)	**Near-term:** Define requirements and initiate modeling and simulation on small network systems. ($135 million) **~2005:** Develop tools and models for modeling complex systems at the architectural level, and tools and techniques for modeling interdependencies and vulnerabilities in systems. ($150 million) **~2010:** Develop automated tools for detecting deviations from system specifications at the architectural level, and technologies and specifications for self-describing systems. ($250 million)
		Important R&D Topics	
3	Risk Analysis	Development of automated tools for analyzing risks to information and information systems. (B, A)	**Near-term:** Develop semiautomated risk analysis tools and formulate techniques and metrics to assess risk. ($75 million) **~2005:** Develop automated risk analysis tools to dynamically assess risk on systems and networks as components change. ($75 million) **~2010:** Develop advanced and automated risk analysis tools to incorporate the emergence of new technologies and system components. ($50 million)
12	Encryption Technology	Development of cost-effective suite of hardware and software technology for encryption. (B, A, ATD)	**Near-term:** Establish national standards for security key management. ($125 million) **~2005:** Develop robust, high-performance, cost-effective, cryptographic technologies. ($150 million) **~2010:** Continually advance and refine robust encryption technologies given the significant increases in computing power available. ($250 million)

[a] The order of the R&D topics within a priority category (most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

2.4 Transportation

2.4.1 Infrastructure Overview

The transportation infrastructure is composed of all surface, air, and waterborne components of the U.S. transportation system but excludes pipelines, which are part of the energy infrastructure. These components include the following:

- Public and private airborne and groundside aviation activity,
- Railway and highway movement and trans-shipment of goods and people (including intercity passenger and mass transit services), and
- Inland waterborne commerce and maritime navigation and their associated port and terminal facilities.

2.4.2 Issues and Trends

Despite the increased freedom to enter the carrier market, which was a product of deregulation that began 20 years ago, the number of rail, bus, and barge companies in the U.S. has declined since 1990. Many new air carriers have tried unsuccessfully to enter the market. It is becoming more common to see privately held infrastructure concentrated in fewer hands, leading to an unprecedented degree of centralized command and control of essential functions. Although the Intermodal Surface Transportation Efficiency Act of 1991 enabled improvements to our primary and secondary highway system, these roads remain in an unsatisfactory condition in light of the demands placed upon them. The gap between highway needs and performance is the greatest it has been in decades, primarily as a result of deferred spending and reduced maintenance budgets. A recent trend — the public's unwillingness to pay for transportation infrastructure through tax-supported mechanisms — has resulted in private commercial interests and joint public-private ventures that provide more transportation capabilities. This shift transfers much of the responsibility for transportation security to organizations less experienced in, and thus potentially less capable of, handling such responsibility (e.g., tollway authorities).

The desire to reduce costs and increase efficiency has led to increased reliance on information technologies as substitutes for capital investments. Experienced human surveillance has been replaced by automated surveillance. Because so much of the fixed transportation infrastructure is relatively isolated, reliability and dependence on automated systems become critical issues. The degree to which reliability is compromised by the open architectures of many data handling systems is currently unknown.

2.4.3 Threats and Vulnerabilities

Many threats and vulnerabilities are direct consequences of emerging open architectures, which allow extensive information sharing and asset management, centralized control, and infrastructure isolation. The lack of a fully secure and equally reliable alternative to the space-based navigation system is also problematic. Moreover, concern has been expressed about the nature of actual security threats (physical and cyber) and management's understanding and ability to prepare for and deal with threats before they become catastrophic. Recent events have shown that terrorists are willing and able to unleash chemical and biological agents in mass transit facilities; moreover, it cannot be ruled out that they are equally willing and able to attack air terminals, undertake large-scale cyber invasions, or wreak concerted destruction on multiple road and rail "choke points."

2.4.4 Summary of R&D Topics and Roadmaps

Table 2.4 summarizes R&D topics and their corresponding roadmaps for the transportation infrastructure. The table provides brief descriptions of research topics grouped by priority (i.e., most important, very important, important); summaries of research activities for three timeframes (near-term [before 2002], before 2005, and before 2010); and *estimates* of financial resources required to support the R&D activities for each timeframe. Tab D contains more detailed descriptions of these research topics, supporting rationale, goals and challenges, threats and vulnerabilities addressed by the research, and research roadmap information.

Table 2.4 Summary of Transportation R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics			
1	Vulnerability Analysis of Existing Systems	Investigation of vulnerabilities of existing transportation systems within and between operating modes, with special emphasis on communication and architectures and on distributed and centralized command and control systems. (B, A, ATD)	**Near-term:** Conduct pilot studies of actual operations. ($9 million) ~**2005:** Develop assessment tools. ($9 million) **~2010:** Complete assessments of transportation systems. ($6 million)
7	Real-time Hazard Threat and Detection Monitoring	Development of reduced cost (both unit and systemwide) detection devices for widespread use in transport systems. (B, A, ATD, POP)	**Near-term:** Ensure applied R&D is under contract. Develop detection devices. ($8 million) ~**2005:** Complete prototype testing. ($12 million) **~2010:** Commercialize public-private ventures. ($12 million)
13	Intrusion Detection	Adaptation and development of customized intrusion detection systems for both physical and cyber assets of the transportation system. (ATD, POP)	**Near-term:** Define requirements and award contracts to customize intrusion detection systems. ($4 million) ~**2005:** Complete design and testing of systems. Begin to implement multiple applications. ($6 million) **~2010:** Commercialize intrusion detection for physical and cyber assets. ($1 million)
15	Threat/ Intelligence Database and Network	Creation of a fully integrated facility to provide intelligence regarding plots for destroying physical infrastructure and/or invading electronic control and data systems. (ATD, POP)	**Near-term:** Define requirements and award contracts for an integrated facility for providing intelligence concerning threats. ($1 million) ~**2005:** Complete a fully functional facility. ($2 million)
16	Information Assurance	Identification and implementation of appropriate artificial-intelligence (AI)-based technologies for preventing acceptance of corrupted or erroneous material into information handling systems. (A, ATD)	**Near-term:** Define requirements and use existing tools to develop AI-based technologies. ($2 million) ~**2005:** Complete design and testing of new tools. ($3 million) **~2010:** Implement and commercialize AI-based technologies. ($1 million)
17	Software Assurance	Identification and implementation of appropriate AI-based technologies for on-line fault checking and self-diagnosis in critical day-to-day information handling systems. (A, ATD)	**Near-term:** Identify requirements for on-line fault checking in information systems. ($4 million) ~**2005:** Complete design and testing of new tools in critical information systems. ($6 million) **~2010:** Complete field implementation and commercialization. ($1 million)
18	Human Factors Analysis	Characterization and analysis of problems and limitations in event preparedness, prediction, and response specifically attributable to the human role in operating the transportation system. (A)	**Near-term:** Characterize problems and limitations inherent in preparedness, prediction, and response. Award contract. ($6 million) ~**2005:** Fully identify and implement changes for preparedness/prediction. ($4 million)
21	Public/Private Infrastructure Security Responsibility	Analysis of jurisdictions and legal structures to clarify command and decision chains for incident mitigation and situation management involving both public and private elements of the transportation infrastructure. (POP)	**Near-term:** Conduct scoping conferences. Issue requests for proposals. Select project teams. ($2 million) ~**2005:** Propose legislation (as needed).

Table 2.4 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Very Important R&D Topics			
2	Simulation Tool Development	Creation of a suite of event prediction and management tools to be used in the evaluation of system disruptions for each mode of transport. (A)	**Near-term:** Identify and evaluate ways to create tools that can be used in event prediction and management. ($15 million) ~**2005:** Develop and validate basic tools. ($15 million) **~2010:** Validate and deploy completed model suite. ($5 million)
3	Determination of Risk Perception of Transport System Managers	Identification and formalization of quantitative measures of risk perception of transport system managers at all appropriate decision levels. (B, A)	**Near-term:** Conduct scoping. ($2 million) ~**2005:** Complete analyses. ($1 million) **~2010:** Update as required.
4	Communication and Inculcation of Sound Risk Management Principles	Development of information and training packages on security risks for operating authorities in all transportation modes; incorporation of vulnerability management into daily operations. (A, ATD, POP)	**Near-term:** Develop training program. ($2 million) ~**2005:** Complete analyses and have training actively occurring in all operating functions. ($2 million) **~2010:** Identify and implement fully secure emergency response communications.
6	Emergency Communications	Identification and implementation of fully secure emergency response communications to be employed in the event of transportation system disruptions (A)	**Near-term:** Identify and implement fully secure emergency response communications. ($6 million) ~**2005:** Commercialize high-reliability, secure emergency response communications. ($2 million)
8	Robotics Development and Adaptation	Development and adaptation of robotic, remotely controlled modules for performing damage assessment by first responders. (B, A)	**Near-term:** Develop and adapt robotic, remotely controlled modules. ($5 million) ~**2005:** Complete prototype testing. ($7 million) **~2010:** Commercialize public/private ventures.
9	Improvement of In-use Performance and Replacement Functionality of Transportation Structures	Development and adaptation of materials to maximize modularity, portability, and/or durability of function of permanent and temporary physical structures and assets in the transportation system. (A, POP)	**Near-term:** Develop and adapt materials to maximize modularity, portability, and/or durability. ($5 million) ~**2005:** Complete field testing in up to five applications. ($7 million) **~2010:** Commercialize structures.
10	Unified Vehicle/ Guideway Systems Hardening	Development and adaptation of materials technologies to improve the durability and resistance to damage from physical and cyber attacks on transportation systems including vehicles and guideways. (A)	**Near-term:** Complete scoping studies of materials technologies. ($2 million) ~**2005:** Develop prototypes to improve durability of transport systems. ($2 million) **~2010:** Perform field testing, and define and implement standards. ($2 million)
11	Asset Management	Development of reliable quantitative measures to make the most efficient use of physical and cyber resources in the transportation system. (A, ATD)	**Near-term:** Conduct scoping. ($1 million) ~**2005:** Validate and peer-review prototype tools. ($2 million) **~2010:** Commercialize tools. ($1 million)

Table 2.4 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Very Important R&D Topics (Cont.)			
12	System Representation Improvement	Development of improved methods to manage large quantities of interconnected and dependent transportation system data into clearly comprehensible formats (e.g., visual displays). (ATD, POP)	**Near-term:** Develop contracts with at least two teams. Improve methods to manage transport system data in a clear format. ($20 million) ~**2005:** Integrate database. Complete prototype tools. ($30 million) **~2010:** Implement multiple applications. ($20 million) (full U.S. coverage assumed)
20	Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building	Development of a body of knowledge and training materials to support the management of incidents and of functional recovery in real time when a significant emergency occurs. (B, A, POP)	**Near-term:** Define needs and procedures. Develop research contracts. ($3 million) **~2005:** Deploy trained teams to standby mode at strategic locations. ($5 million) **~2010:** Introduce active information exchange and revise procedures as needed. ($3 million)
Important R&D Topics			
5	Capacity Margin Analysis	Development of reliable quantitative estimates of losses associated with the absence of surplus carrying capacity in each component of the transportation system. (A)	**Near-term:** Sign contract for analytical team(s). (>$1 million) ~**2005:** Complete analytical effort. (>$1 million)
14	Cyber Vulnerability Data Warehouse	Provision of access to information on advanced cyber security practices to owners of data repositories and networks in the transportation sector. (ATD, POP)	**Near-term:** Define requirements and award contracts. ($1 million) ~**2005:** Complete and verify database. Warehouse access protocol. ($2 million)
19	Recovery Training	Development of training packages that maximize communication to and endorsement of the essential components of response and recovery by all transport system operating authorities. (A)	**Near-term:** Contract for training program development. ($1 million) ~**2005:** Implement training program. ($2 million) ~**2010:** Continue training program. ($1 million)

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

2.5 Vital Human Services

2.5.1 Infrastructure Overview

The vital human services infrastructure encompasses three infrastructures: water-supply systems, emergency services, and government services. The water-supply system infrastructure includes sources of water; reservoirs and holding facilities; aqueducts and other water transport systems; filtration, cleaning, and treatment systems; distribution pipelines and other delivery mechanisms; cooling systems; and water systems that deal with water runoff, wastewater, and fire-fighting needs. The emergency services infrastructure includes medical, police, fire, rescue systems, and personnel that plan for and respond to emergencies. The government services infrastructure includes the capability of federal, state, and local governments to provide essential services to the public during and after emergencies.

2.5.2 Issues and Trends

Vital human services are very intra- and interdependent infrastructures. For example, fire fighting is critically intradependent on a reliable water-supply system and heavily interdependent on the other critical infrastructures identified by the Commission. For example, emergency response functions could be hampered if part of the transportation infrastructure were out of order. In this era of reduced taxation and shrinking government services, it is difficult to maintain these infrastructures and manage the risk of future threats.

2.5.3 Threats and Vulnerabilities

Water-supply Systems

The vulnerability of community water-supply systems to contamination from biological agents, chemical agents, or toxins is of considerable concern. There are several specific instances of terrorist threats to contaminate water supplies with biological or chemical agents. However, most water-supply systems are fairly safe from such attacks because hazardous agents do not mix well or survive in water. These agents do, however, pose a threat if they are inserted at critical points in the system. In addition, water-supply systems are vulnerable to physical and cyber attacks. Pumping systems are quite vulnerable and, if destroyed, could shut down a water-supply system for months. Water-supply systems increasingly depend on computer systems, which are vulnerable to cyber attacks.

Emergency Services

First responders are the most vulnerable entity within the emergency services infrastructure. These personnel are trained to deal with a variety of materials, but they are not trained, nor do they have adequate equipment, to deal with weapons of mass

destruction, such as biological or chemical warfare agents. First responders and the emergency services infrastructure are vulnerable because detection equipment and training to handle such emergencies in a timely fashion are not available.

Government Services

The primary vulnerability of the government services infrastructure is its evolving complexity and increasing dependency on all infrastructures to provide services. The information and communications, electric power, banking and finance, and transportation infrastructures are all critical components in providing government services.

2.5.4 Summary of R&D Topics and Roadmaps

Vital human services R&D topics and their corresponding roadmaps are summarized in Table 2.5. The table provides brief descriptions of research topics grouped by priority (i.e., most important, very important, or important); summaries of research activities for three timeframes (near-term [before 2002], before 2005, and before 2010); and estimates of the financial resources required to support the R&D activities for each timeframe. Tab E contains more detailed descriptions of these research topics, supporting rationale, goals and challenges, threats and vulnerabilities addressed by the research, and research roadmap information.

Table 2.5 Summary of Vital Human Services R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics			
1	Identification and Characterization of Biological and Chemical Agents	Characterization of the behavior of chemical and biological agents in water, the effect of water treatment chemicals on these agents, and the actual risks posed by these agents in the water supply system. (B, A)	**Near-term:** Characterize known agents. ($14 million) ~**2005:** Identify unknown agents and characterize their physical and chemical parameters and behavior in different environments. Develop and implement database and information exchange mechanisms. ($15 million) **~2010:** Continue to identify and characterize unknown agents. ($25 million)
2	Biological and Chemical Agent Detectors	Development of detectors that provide real-time analysis of water samples to detect the presence of biological and chemical agents in quantities that pose risks to the population. (B, A)	**Near-term:** Adapt current slate of detectors for applications to the water-supply system. ($30 million) **~2005:** Improve sensitivity of current detectors, enhance capability for real-time measurements, and extend detector capabilities to other agents. ($45 million) **~2010:** Develop new generation of detectors to meet more stringent requirements associated with additional, newer agents. ($55 million)
3	Supervisory Control and Data Acquisition (SCADA) Systems	Application of information assurance techniques to water-supply SCADAs; development of appropriate, cost-effective protocols. (A)	**Near-term:** Develop vulnerability assessment criteria and techniques for SCADA systems. ($15 million) **~2005:** Develop techniques to rectify security problems and preliminary protocols for design and operation of secure systems. Conduct pilot tests of improved systems. ($15 million) **~2010:** Conduct additional pilot tests and develop a final set of design and operational protocols. ($25 million)
4	Vulnerability Assessment of Water-supply Systems	Identification and development of methods, tools, and information to assess and cost-effectively reduce the vulnerabilities of water-supply systems. (A)	**Near-term:** Develop criteria for evaluating vulnerability-reduction options. Characterize options. ($9 million) **~2005:** Develop and pilot test evaluation methods and tools. ($12 million) **~2010:** Apply lessons learned to methods and tools, enhance information base, improve methods and tools, and perform additional validations. ($16 million)
5	Center of Excellence for Risk Assessment of Water-supply Systems	Establishment of a center of excellence to support communities in conducting vulnerability and risk assessments of water-supply systems and in making decisions regarding water-supply assurance. (B, A)	**Near-term:** Establish requirements for development and operation of center. Start up center. ($8 million) **~2005:** Develop/test tools, models, and communication methods. ($9 million) **~2010:** Continue research activities from earlier phases. Reevaluate the role of the center and adjust accordingly. ($11 million)
6	Detectors and Detection Systems for Emergency Services	Development of inexpensive, sensitive, rugged, easy to operate, and portable contaminant detectors and detection systems for use by first responders to an emergency. (B, A)	**Near-term:** Identify requirements for known contaminants. Adapt robotic technologies for this use. Initiate basic research into the science of new detectors. ($30 million) **~2005:** Produce detectors with first generation requirements. Continue basic and applied research into new detectors and robotics. ($45 million) **~2010:** Develop/test a new slate of detectors and robotics for emergency services. ($55 million)

Table 2.5 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics (Cont.)			
8	Multihazard, Real-time Simulation and Modeling	Upgrading of simulation models of hazards and protective actions to incorporate real-time data for emergency managers and decision makers. (A)	**Near-term:** Define requirements for such a system and initiate development. ($17 million) **~2005:** Develop and pilot test a prototype system. Integrate lessons learned into next version of system. ($21 million) **~2010:** Conduct additional pilot tests. Develop, test, and distribute a final set of models constituting the system. ($23 million)
10	Decontamination Technologies	Identification, characterization, development, and adaptation of decontamination technologies to be used in chemical/biological incidents. (A)	**Near-term:** Identify and characterize appropriate existing technologies. Develop decision needs for evaluating and selecting decontamination options. ($55 million) **~2005:** Focus on developing new decontamination technologies. Finalize evaluation and selection criteria for deciding what technologies are most appropriate for any given application. ($75 million) **~2010:** Complete development and demonstration activities on the technologies examined in the previous timeframe. Initiate research on another set of technologies. ($105 million)
11	Systems Analysis of Public Health Emergency Response Systems	Comprehensive analysis of the public health response system to characterize threats and vulnerabilities, determine critical elements and linkages, and identify technology needs. (A)	**Near-term:** Conduct surveys on treatment capabilities and initiate development of analysis tools. ($13 million) **~2005:** Develop and pilot test analytical models. Develop a preliminary set of alternative treatment practices and conduct emergency preparedness exercises. ($15 million) **~2010:** Complete analysis tools. Develop/distribute information on alternative treatment practices and emergency preparedness practices. Conduct additional emergency preparedness exercises. ($17 million)
Very Important R&D Topics			
7	Integrated Emergency Management System	Development of an integrated emergency management support system to assist in effective response by emergency services personnel. (A)	**Near-term:** Specify system requirements and work on the development of a prototype system. ($13 million) **~2005:** Develop and test the prototype. Develop and test a full, integrated system. ($15 million) **~2010:** Complete research and deploy system. ($5 million)
12	Support Systems for Reconfiguring Government	Development of software support systems that aid governments in reconfiguring services during emergencies. (A)	**Near-term:** Define basic requirements for such a system and develop a limited prototype. ($10 million) **~2005:** Develop and pilot test more enhanced prototypes. ($12 million) **~2010:** Complete development of the system. Test, validate, and deploy full-scale system. ($16 million)

Table 2.5 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
		Important R&D Topics	
9	Behavioral/Psychological Studies of Reactions to Incidents	Determination of public and emergency responder reactions to chemical/biological incidents; preparation of training and communication techniques. (A)	**Near-term:** Establish a baseline of required and anticipated responses. ($6 million) **~2005:** Develop and conduct training courses. Develop and pilot test enhanced communication techniques. ($6 million) **~2010:** Distribute study results and recommendations to emergency services organizations. ($2 million)

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

Section 3
Integrated R&D Topics and Roadmaps

Common R&D themes are described, and crosscutting issues, as well as interdependency and complexity R&D needs and topics, are discussed. An integrated R&D roadmap and estimate of resource requirements are presented.

3.1 Common R&D Themes

A number of common themes underlie the R&D topics presented in Section 2. Some of these themes directly correlate with the objectives of infrastructure assurance — to reduce critical vulnerabilities by protecting infrastructures, detecting intrusions, mitigating the effects of disruptions, assisting in the management of incidents, and facilitating recovery. Other themes focus on developing analytical or supporting technologies that are needed to help meet these objectives.

Table 3.1 highlights the common infrastructure assurance R&D themes. The first four themes — information assurance, monitoring and detection, protection and mitigation, and response and recovery — correspond to the aforementioned objectives. The analytical themes include modeling and simulation, systems analysis, decision support, and risk management. The final theme, vulnerability assessment, provides supporting baseline information for all of the other themes.

The sector R&D topics in Tables 2.1–2.5 can involve research elements that correspond to one or more of the themes. For example, monitoring and

Table 3.1 Common R&D Themes

Information Assurance — secure information while it is stored, being processed, and in transit
Monitoring and Detection — monitor systems, detect threats and intrusions, and provide timely warning
Protection and Mitigation — protect infrastructures physically and mitigate damage
Response and Recovery — aid in rapid incident response and recovery
Modeling and Simulation — develop models of components, systems, and infrastructures and examine the efficacy of alternative infrastructure assurance strategies and technologies
Systems Analysis — analyze complex systems and identify and analyze infrastructure interdependencies
Decision Support — support timely decision making with tools, methodologies, and information systems
Risk Management — determine where best to allocate resources and how to manage risks
Vulnerability Assessment — assess the vulnerability of components, systems, and infrastructures

detection, modeling and simulation, and decision support are all elements of energy R&D Topic No. 1 (Real-time Control Mechanisms). Because this topic involves integrating real-time control systems to support timely decisions, decision support is designated as the primary theme. The other themes are secondary.

Each of the themes is discussed below. Table 3.2 provides a mapping among R&D topics and themes. Primary and secondary themes are shown.

3.1.1 Information Assurance

As national infrastructures increasingly depend on computers and networked information systems to improve efficiency and enhance economic competitiveness, they also become more vulnerable to potential cyber attacks. In addition, the basic technology is changing rapidly, open architectures are being pursued, and government policy is encouraging increased competition. These changes affect both the individual critical infrastructures and the national interdependent infrastructures, and as well as increase infrastructure vulnerability as a whole. Significant new investments in R&D are required to protect the communications infrastructure, and the information created, stored, processed, and transmitted on it.

3.1.2 Monitoring and Detection

Reliable automated monitoring and detection systems, timely and effective information collection technologies, and efficient data reduction and analysis tools are needed to identify and characterize localized or structured attacks against infrastructure. Technologies are also needed to allow highly toxic chemical and biological agents to be detected, identified, measured, and subsequently treated. A protection and attack sensing and warning capability is needed to provide early threat warning to government organizations and private-sector infrastructure owners and operators, thereby preventing widespread infrastructure disruptions that have potentially serious consequences on our national security, economy, and quality of life.

3.1.3 Protection and Mitigation

Real-time system control, infrastructure hardening, and containment technologies are needed to protect infrastructure systems against threats and mitigate the impacts of disruptions. Advanced survivability, reliability, and assurance enhancement measures need to be explored and developed. Technologies also are needed to contain and isolate the impacts of information system disruptions so that the complete system or dependent infrastructures are not affected.

3.1.4 Response and Recovery

A wide range of new technologies and tools are needed for planning for, responding to, and recovering from incidents, such as physical- and cyber-based attacks

Table 3.2 Mapping among R&D Topics and Primary and Secondary Themes[a]

R&D Topic No.	R&D Topic Title	Information Assurance	Monitoring and Detection	Protection and Mitigation	Response and Recovery	Modeling and Simulation	Systems Analysis	Decision Support	Risk Management	Vulnerability Assessment
Banking and Finance										
1	Simulation Model Development					P				
2	Information Security Analysis	P								
3	Intrusion Indication and Warning Tools		P				S			
4	Systems Reliability Enhancement			P					S	S
5	Information System Standardization						P	S		
6	Electronic Commerce Security Enhancement						P	S		S
Energy										
1	Real-time Control Mechanisms		S			S		P		
2	Analysis of Scale and Complexity			S			P			
3	Vulnerability Assessment									P
4	Information Assurance and Cyber Security	P	S						S	
5	Emergency Response and Recovery Information Technologies				P					
6	Transmission and Distribution Technologies			P						
7	On-line Security Assessment					P				
8	Dispersed Generation and Backup Infrastructures			P						
9	Critical Consequence Analysis				P	S				
10	Decision Support Systems							P	S	
11	Physical Protection Assessment									P
12	Multisensor and Warning Technologies		P							
13	Emergency Response Capability Enhancement				P					
14	Cyber Protection Enhancement	P								
15	Evaluation of Policy Effects						P			
16	Institutional Barriers						P			
17	Infrastructure Interdependencies						P			
Information and Communications										
1	Vulnerability Detection and Analysis		S							P
2	Valuation of Information								P	
3	Risk Analysis								P	
4	Characterization and Notification of Threats		P							
5	Intrusion and Incident Detection and Warning		P							
6	Response, Recovery, and Reconstitution				P					
7	Security Architectures	P								
8	Assurance Technologies	P								
9	Advanced Concepts and Theory	P								
10	Management of Information Protection	P								
11	Characterization of Minimum Infrastructure for Essential Services	P								
12	Encryption Technology	P								
13	Modeling and Simulation Tools					P				
Transportation										
1	Vulnerability Analysis of Existing Systems					S				P
2	Simulation Tool Development					P				S
3	Determination of Risk Perception of Transport System Managers								P	
4	Communication and Inculcation of Sound Risk Management Principles								P	

Table 3.2 (Cont.)

No.	R&D Topic Title	Information Assurance	Monitoring and Detection	Protection and Mitigation	Response and Recovery	Modeling and Simulation	Systems Analysis	Decision Support	Risk Management	Vulnerability Assessment
	Transportation (Cont.)									
5	Capacity Margin Analysis			P						
6	Emergency Communications			S	P					
7	Real-time Hazard Threat and Detection Monitoring		P							
8	Robotics Development and Adaptation				P					
9	Improvement of In-use Performance and Replacement Functionality of Transportation Structures				P					
10	Unified Vehicle/Guideway Systems Hardening			P						
11	Asset Management							P		
12	System Representation Improvement							P		
13	Intrusion Detection		P							
14	Cyber Vulnerability Data Warehouse		P							
15	Threat/Intelligence Database and Network		P	S						
16	Information Assurance	P								
17	Software Assurance	P	S							
18	Human Factors Analysis						P			
19	Recovery Training				P					
20	Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building				P					
21	Public/Private Infrastructure Security Responsibility						P			
	Vital Human Services									
1	Identification and Characterization of Biological and Chemical Agents		S	P						
2	Biological and Chemical Agent Detectors		P							
3	Supervisory Control and Data Acquisition Systems	P								
4	Vulnerability Assessment of Water-supply Systems									P
5	Center of Excellence for Risk Assessment of Water-supply Systems							P		
6	Detectors and Detection Systems for Emergency Services		P							
7	Integrated Emergency Management System							P		
8	Multihazard, Real-time Simulation and Modeling					S		P		
9	Behavioral/Psychological Studies of Reactions to Incidents						P	S		
10	Decontamination Technologies				P					
11	Systems Analysis of Public Health Emergency Response Systems						P			S
12	Support Systems for Reconfiguring Government							P		

[a] P = primary theme; S = secondary theme.

that affect local or national infrastructures. This includes crisis and consequence management systems, personal protective equipment, and emergency medical and decontamination technologies.

3.1.5 Modeling and Simulation

Modeling and simulation tools and environments (e.g., test beds) need to be developed for studying infrastructure-related problems and dynamic response mechanisms under varying conditions. Such tools allow experimentation that cannot be performed in realistic environments of any appreciable scale. For example, robust infrastructure and nodal analysis techniques and tools need to be developed for modeling large-scale distributed/networked systems and interdependent infrastructures. Such tools would support systems analysis and decision making.

3.1.6 Systems Analysis

Systems analysis needs to be performed to identify critical nodes and components within infrastructures, to examine infrastructure coupling and interdependencies, and to help understand the behavior of complex systems. Such analysis also is needed to help support decisions on how systems can be protected from physical and cyber threats and degraded gracefully, if necessary, to prevent cascading impacts within and across infrastructures. That is, comprehensive systems analysis techniques are needed for addressing physical and cyber security issues in an integrated fashion. Modeling and simulation tools and vulnerability assessment information support such analyses.

3.1.7 Decision Support

Decision support methodologies, tools, and information systems are needed to help identify and prioritize critical assets for protection, mitigation, incident management, and recovery; compute return on investment in competing security technologies; and develop overall infrastructure assurance investment strategies. Measurable criteria also need to be established that address national security, economic competitiveness, quality of life, and other important attributes. Such methodologies, tools, and information systems would help determine what infrastructure assets are critical, and thus aid in the priority use of resources in a degraded environment.

3.1.8 Risk Management

Methodologies and tools are needed to identify and manage risks to infrastructures and information, and to determine where best to allocate limited resources. Research areas include developing methodologies for measuring the relative risks and the degree of impact of infrastructure assurance investment strategies; for enhancing the ability of users to perform consequence assessment and risk analysis; for developing effective risk management approaches and strategies; for dealing with uncertainties in, or incomplete knowledge of, threats, vulnerabilities, and protection measures; and for managing risks

across the multiple components and organizations involved in the infrastructures. Methods also are needed to more effectively characterize risks and communicate risk information.

3.1.9 Vulnerability Assessment

The specific weaknesses (vulnerabilities) of infrastructure components and systems to credible threats need to be identified and analyzed. A comprehensive awareness also needs to be developed of the inherent susceptibilities of technologies on which infrastructures and key components are or will be reliant; technologies that potentially could be used maliciously to disrupt, damage, or destroy infrastructures or key components; and technologies that could have protective applications and potentially be used to safeguard infrastructures and components. This baseline information provides a frame of reference for risk management and investment decisions.

3.2 Crosscutting R&D

Included among the many topics within each theme are elements that apply to, or crosscut, multiple infrastructure sectors (Figure 3.1). These elements primarily involve basic and applied research aimed at increasing the fundamental knowledge necessary for developing infrastructure assurance technologies and investigating the feasibility and practicality of proposed technological solutions. With careful R&D planning and coordination, crosscutting elements could be combined into focused R&D areas to capitalize on synergies and reduce resource requirements. Combining these elements also would promote integration of the R&D efforts and reduce the number of "stovepipe" activities (i.e., narrow, sector-specific activities that are not effectively coordinated across program boundaries).

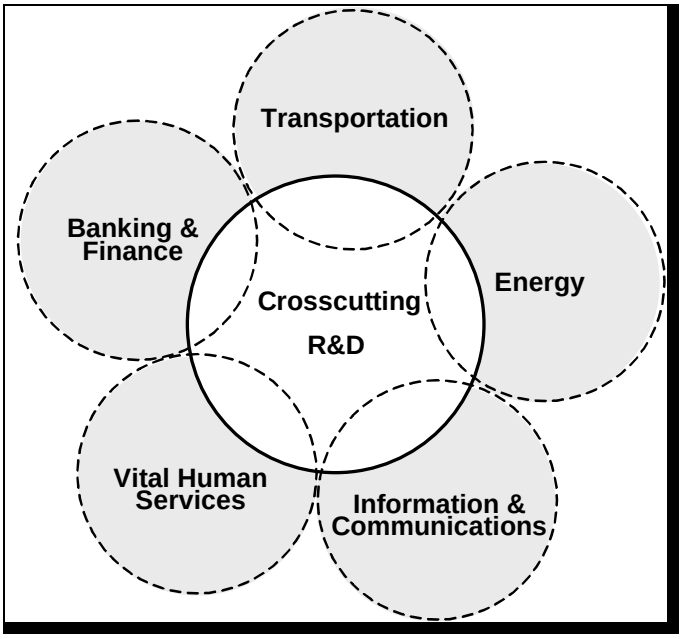


Figure 3.1 Crosscutting R&D

Cyber protection for electronic commerce and SCADA systems is one example of crosscutting R&D within the information assurance theme. Electronic commerce is a basic component of many infrastructure operations — it includes transfers of financial assets in banking and finance, power purchases in the electric power system, and

confidential information sharing in government services. Similarly, transferring operational instructions to system control devices via SCADA systems is emerging as a primary operating method for many infrastructures (e.g., electric power system control of transmission; control of oil, gas, and water pipelines; and control of switching systems in transportation). These trends, coupled with the increased use of open and standardized information and communication architectures, have increased the vulnerability of both electronic commerce and SCADA systems to cyber attacks. New cyber protection technologies are needed to improve the security of these information transfer systems and protect the critical infrastructures they support.

Many basic and applied research topics identified in Table 3.2 (under Information Assurance theme) support the development and application of cyber protection technologies. For example, the basic research topic, Advanced Concepts and Theory, would provide fundamental knowledge for developing advanced information and communications systems and networks. Similarly, Security Architectures would include the design of new and improved security architectures composed of components (i.e., firewalls, switches, encryption technology) and services that ensure confidentiality, integrity, and availability for information and communications systems. While Encryption Technology would develop efficient and cost-effective technologies, Management of Information Protection is both a basic and applied research topic expected to provide methods, tools and techniques, and standards that support information protection in information and communications systems. Finally, Assurance Technologies would include both basic and applied research to develop tools and techniques that test and verify that the hardware and software components, and their integration into systems, meet information and communications system requirements. These research topics contribute to the development of cyber protection technologies for electronic commerce and SCADA systems that would benefit all infrastructures.

Another example of crosscutting R&D involves comprehensive and detailed vulnerability assessments, which are fundamental for making effective decisions about protecting infrastructures. The R&D topics shown in Table 3.2 (under Vulnerability Assessment theme) describe rigorous vulnerability assessments that would require new methods, tools, and techniques not currently available. It is important that vulnerability assessments are performed consistently across all sectors so that consistent infrastructure assurance strategies can be developed to protect critical infrastructures. Such assessments are also important to support interdependency analyses.

The development of large-scale models also would require significant basic and applied research (under Modeling and Simulation theme in Table 3.2). Advanced computational algorithms, advanced simulation architectures, approaches for dealing with complexity, and massive data storage and fast retrieval are some of the basic research elements that support large-scale modeling. Advanced visualization techniques, user-friendly machine interfaces, and expert systems for information handling are some of the applied research topics that support large-scale modeling and simulation. These basic and applied research elements would support the large-scale modeling and simulation topics

included in the banking and finance, energy, and information and communications R&D roadmaps.

The detection and effective management of intrusions (cyber and physical) is another example of crosscutting R&D. The current infrastructure trend is to reduce labor costs and rely on automated systems. This trend places greater expectations on the capabilities of these automated systems to provide reliable and timely information.

As Table 3.2 shows, all sector R&D roadmaps identified topics that focus on monitoring and detecting intrusions. For example, the energy roadmap identified topics that address both cyber intrusions (e.g., Information Assurance and Cyber Security) and physical intrusions (e.g., Multisensor and Warning Technologies). Cyber intrusion topics were identified in the banking and finance (e.g., Intrusion Indication and Warning Tools) as well as in the information and communications (e.g., Incident Detection and Warning) roadmaps. R&D topics for water-supply systems focused on detecting chemical or biological agents (e.g., Identification and Characterization of Biological and Chemical Agents). Finally, transportation R&D topics were concerned with both cyber and physical intrusion detection (e.g., Intrusion Detection).

Although each infrastructure has specific needs for detecting and managing intrusions, significant synergy is present in the type of research being proposed. Cyber intrusion detection and management systems require basic and applied research to develop (1) authentication/authorization tools, (2) authentication management systems, (3) intrusion detection algorithms and technologies, (4) trace-back systems, and (5) intrusion warning systems. Physical intrusion and management primarily depend on the accuracy of detectors as well as on cyber components. Key factors in developing effective detectors are unit cost, reliability, durability, and maintainability, all of which have crosscutting dimensions.

Similar examples of crosscutting R&D can be found in each theme. As detailed programs are developed for the R&D topics, particular attention should be given to identifying such crosscutting R&D elements.

3.3 Interdependency and Complexity R&D

In addition to the crosscutting R&D areas that could reduce investment requirements, some R&D needs transcend the more narrowly focused R&D defined in the individual infrastructures. Such research requires investments beyond those associated with the individual sector topics. Perhaps the most compelling need involves interdependency and complexity.

This topic, which is not addressed adequately in the individual topics, focuses on the interdependence between physical and cyber infrastructure components both within and among the eight critical infrastructures. The complexity and interconnected nature of our infrastructures are due largely to an increased reliance on telecommunications and

computer processing for their management. The power and sophistication of cyber technologies and their widespread integration in the infrastructures increase the likelihood of unforeseen vulnerabilities and unintended consequences. As a result, not all aspects of one infrastructure's dependence on another are documented or understood. Further, hidden interdependencies are a strong possibility because of complex, and heretofore, not understood linkages.

The most obvious dependencies between the elements of one or more infrastructures are those that are linked physically. For example, consider a substation in an electrical distribution system that provides electric power to a telecommunications center. Failure or loss of power in the substation would directly affect the telecommunications center (subject to backup power supplies). The telecommunications center, in turn, may control the SCADA systems for gas pipelines and water-supply systems. The gas pipelines may fuel critical gas-fired generators in the electric system, and so forth. Such dependencies, sometimes called system interactions, must be fully identified and evaluated.

Other dependencies are not physically linked but are coupled because of location and exposed environment. For example, a common utility corridor that contains overhead electric power transmission lines, buried gas pipelines, and telecommunications cables, dramatizes such dependencies. Collocating infrastructures makes them more susceptible to such physical hazards as explosion, fire, flood, and seismic events, as well as sabotage.

Subtle interactions are another type of dependency that can exist in complex systems and occur without a direct link. The failure of a substation, for example, could cause topological reconfiguration of the electric network, which, in turn, could overload a similar substation within the system if the demand at that time exceeds the substation capacity. Here, the direct link does not normally exist, and the failure could occur only if certain conditions were imposed (e.g., peak load).

Direct system interactions, indirect coupling as a result of collocation, and subtle interactions usually occur shortly after an incident. However, another type of interaction can occur over an extended time, that is, time for the effect to propagate through elements of the infrastructures. Understanding this time delay is important in designing appropriate detection and mitigation technologies. Infrastructures, such as the water-supply system and gas and oil storage, which are limited resources subject to depletion, are candidates for these interactions. Also, the effect of threats (e.g., cyber threats to the banking and finance infrastructure) requires time to propagate, and, therefore, early detection and recovery are important factors in controlling their effects.

Natural hazards, such as seismic events or extreme weather, clearly illustrate how threats can affect multiple infrastructures simultaneously. Such threats also reveal interdependencies that can complicate or delay mitigation or recovery of a particular infrastructure from an incident. A major earthquake, for example, can disrupt many

infrastructures. At the same time, transportation structures, such as bridges and elevated highways, could collapse, making it difficult to provide vital emergency services.

Consequences of multiple disruptions to our infrastructure range from loss of human life and property to prolonged loss of shelter, food, and water, and disruption of financial services. Recovery of particular infrastructures from an incident can be delayed significantly or thwarted by the simultaneous unavailability of another infrastructure. Controlling or reducing the effect of interdependencies is a function of the type of incident, the area of occurrence, and the technology. Further studies should aim to improve our understanding of vulnerabilities that result from disruption to multiple infrastructures.

A well-organized, coordinated sabotage event could cause a wide area disruption of one or more infrastructures. A series of incidents, each planned and timed to reinforce the effects of the others, could interact (cascade) across critical infrastructures to degrade the services upon which all depend. The finely tuned, just-in-time interdependence of infrastructure systems gives potential attackers the capability to leverage localized damage into widespread system failure. A smaller scope sabotage could also propagate across several infrastructures because of embedded dependencies that exist within the architectures of our infrastructures. The complexity of automated systems induces additional risk. Table 3.3 summarizes several broad R&D topics and roadmaps needed to address interdependency and complexity issues.

3.4 Integrated Roadmap

Figure 3.2 provides integrated R&D roadmapping information for the three timeframes. Individual R&D topics are aggregated by theme. Interdependency and complexity R&D is also shown. The heavy bars indicate peak R&D activity. However, as indicated by the dashed lines, ongoing R&D is required at a reduced level throughout the study period.

Vulnerability assessment is an immediate need that will provide a baseline for focusing all of the other R&D activities. Such assessments must continue over time to capture the dynamics of the evolving threats and changes in the infrastructures (e.g., as a result of restructuring, market response mechanisms, or implemented infrastructure assurance technologies).

The four analytical themes — systems analysis, modeling and simulation, decision support, and risk management — focus on near- to mid-term R&D. However, some R&D efforts, particularly those involving modeling and simulation, are expected to extend through the long-term. Risk management R&D peaks after initial vulnerability assessments are completed. Applications of the developed tools and methodologies will likely motivate the need for continuing enhancement and development.

Table 3.3 Summary of Interdependency and Complexity R&D Topics and Roadmaps[a]

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Most Important R&D Topics			
1	Identification and Characterization of Dependencies	Identification of dependencies (direct and indirect) among national infrastructures, including space systems (e.g., Global Positioning System), and characterization of how damage can propagate across multiple infrastructures. (A)	**Near-term:** Identify and characterize infrastructure components, first-order dependencies, and degree of coupling among infrastructures. ($9 million) **~2005:** Identify and characterize higher order dependencies. Investigate coupling issues and resultant infrastructure vulnerabilities. ($9 million) **~2010:** Identify opportunities for decoupling infrastructures to reduce vulnerabilities and the potential for propagation of damage across infrastructures. ($10 million)
2	Analysis of Scale, Complexity, and Trends	Characterization of industry trends (e.g., restructuring) in terms of interdependence and effects of scale and complexity (e.g., due to cyber dependence) on system behavior. (A)	**Near-term:** Improve understanding of scale and complexity in terms of national interdependent infrastructures. Characterize industry trends that affect scale and complexity. ($6 million) **~2005:** Develop "science" of large-scale, complex, interdependent infrastructures. ($15 million) **~2010:** Develop strategies for mitigating effects of scale and complexity. ($15 million)
Very Important R&D Topics			
3	Systems Analysis and Simulation Tools	Development of systems analysis methods and simulation tools (e.g., nodal analysis tools) for assessing potential interdependence-related vulnerabilities due to physical and cyber threats. (B, A, ATD, POP)	**Near-term:** Develop architectures and robust nodal analysis techniques and simulation tools to analyze infrastructure sector vulnerabilities. ($15 million). **~2005:** Develop integrated tools to simulate interdependent infrastructure operation, dynamic feedback mechanisms, and overall system response to threats. ($25 million)
4	Consequence Analysis and Risk Management Methodologies and Tools	Development of methods and tools for assessing potential consequences (e.g., national security, economic, social) of interdependence-related disruptions and for managing risks. (A, ATD)	**Near-term:** Examine historical data (e.g., large natural disasters and widespread power outages) to develop a baseline of consequence information. Develop basic risk management and consequence analysis methods and tools. ($15 million). **~2005:** Develop integrated risk management and consequence analysis tools for all infrastructure sectors and consequence dimensions. ($21 million).
Important R&D Topics			
5	Protection and Mitigation	Development of protective measures (including infrastructure hardening) making the interdependent infrastructures able to resist a wider range of potential threats; system redundancy to improve reliability and reduce the chances of cascading impacts; and infrastructure survivability across a larger set of challenges. (B, A, ATD, POP)	**Near-term:** Identify existing protection and mitigation measures and technologies, including backup systems, workarounds, substitutes, and contingency plans, and characterize roles from an interdependence perspective. Initiate development of protection and mitigation technologies. ($27 million) **~2005:** Develop and pilot test protection and mitigation technologies. ($40 million) **~2010:** Demonstrate and validate effectiveness of protection and mitigation technologies. ($50 million)

Table 3.3 (Cont.)

R&D Topic			
No.	**Title**	**Description (Type[b])**	**Research Roadmap (Resource Estimate[c])**
Important R&D Topics (Cont.)			
6	Response and Recovery	Development of planning tools for identifying and evaluating response and recovery strategies. (B, A, ATD, POP)	**Near-term:** Develop tools for identifying and evaluating response and recovery mechanisms for multiple infrastructure disruptions. ($13 million) **~2005:** Develop and pilot test response and recovery tools and mechanisms. ($25 million) **~2010:** Demonstrate and validate effectiveness of response and recovery tools and mechanisms. ($25 million)

[a] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

[b] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[c] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

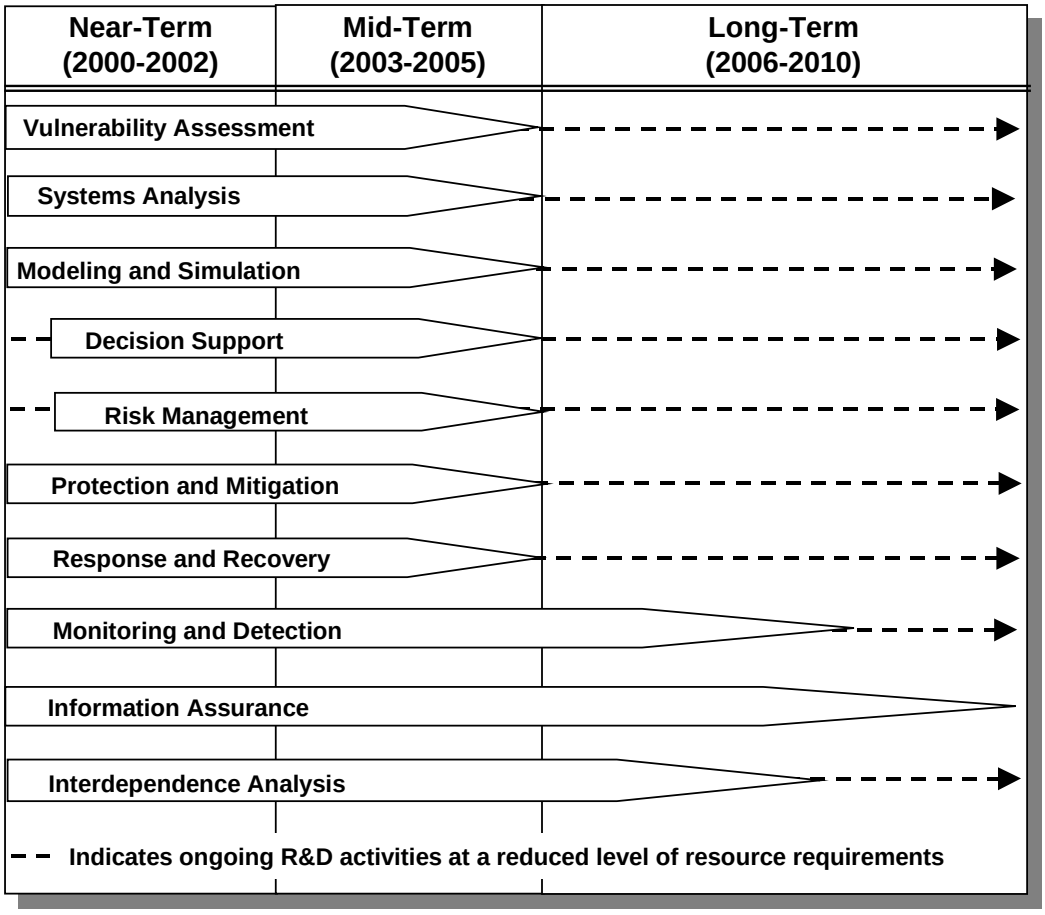


Figure 3.2 Integrated R&D Roadmap

Information assurance and monitoring and detection are both multifaceted, long-term R&D activities. As discussed previously, information assurance is critical for accomplishing the other R&D activities. That is, the rapid proliferation and integration of telecommunications and computer systems in virtually all aspects of infrastructure operation have made information assurance a critical activity. Research in the protection and mitigation and response and recovery themes varies significantly among the infrastructures, with a focus on near- and mid-term activities. As the dashed lines in Figure 3.2 indicate, long-term R&D activities are also likely to be required.

3.5 Resource Requirements

Tables 2.1–2.5 provide estimated resource requirements for the recommended R&D topics. The estimates are aggregated by sector into three timeframes: near-term (FY2000–2002), mid-term (FY2003–2005), and long-term (FY2006–2010). In preparing these estimates, each sector team made assumptions about the expected scope, the level of effort, and the pace of the research. They also made assumptions about government and private-sector responsibilities and the availability of ongoing R&D that could be leveraged. They emphasized near-term activities. The results of such activities will help to shape subsequent R&D effort in the mid- and long-term.

Table 3.4 summarizes the estimated annual resource requirements for the five infrastructure sectors. A sixth area — Interdependency and Complexity — is also shown. As described in Section 3.3, this area includes R&D that transcends the more narrowly focused R&D in the individual infrastructure sectors.

As Table 3.4 shows, the information and communications sector has the largest R&D portfolio — requiring approximately one-half of the total estimated near-term resources. More than one-fourth of the near-term resources focus on R&D for the energy

Table 3.4 Estimated Annual (Fiscal Year) Infrastructure Assurance Resource Requirements for Recommended R&D Topics

	Resource Requirements ($ Millions/Fiscal Year)						
	Near-Term			Mid-Term			Long-Term
Infrastructure Sector	2000	2001	2002	2003	2004	2005	2006–2010
Banking and Finance	55	50	45	25	15	10	5
Energy	160	180	180	200	200	200	200
Information and Communications	260	350	350	350	350	350	320
Transportation	10	40	40	40	40	40	10
Vital Human Services	50	80	95	95	95	95	70
Interdependency and Complexity	20	30	35	50	45	35	20
Total	555	730	745	760	745	730	625

infrastructure. Research and development for the other sectors range from approximately 5% to 10% of the total portfolio. Interdependency and complexity R&D requires about 5% of the total portfolio.

Overall, estimated near- and mid-term resource requirements total approximately $2 billion each, while long-term requirements are estimated to be approximately $3 billion. Total estimated resource requirements are approximately $7 billion.

Figure 3.3 displays a breakdown of near-term resource requirements by theme. As shown, information-assurance-related R&D requires approximately one-third of the total estimated resources. Monitoring and detection R&D represents about 15% of the portfolio, while vulnerability assessment and modeling and simulation each represent approximately 10%.

As discussed in Section 3.2, elements of some of the recommended R&D topics potentially could be combined to capitalize on synergies and to reduce investment requirements. Identifying such elements and estimating associated cost reductions need to be priorities of future roadmapping efforts. The common R&D themes discussed in Section 3.1 provide a starting point for identifying such elements and opportunities for synergy.

The sector investment profiles generally show that resource requirements increase during the near term, as the R&D programs gain momentum and achieve critical mass in terms of researchers and innovative research ideas. Critical requirements-definition and information-collection activities are typical front-end, critical path activities for most R&D topics.

The investment requirements shown in Table 3.4 are generally of the same order-of-magnitude as those recommended in the Commission's *Critical Foundations* report. They show that a significant increase in investment is needed to "jump start" a focused, coordinated, and goal-oriented national infrastructure assurance R&D effort. The timeframes associated with national goals, when established, will determine the scope, priority, and pace of the R&D activities. Annual investment levels must be adjusted accordingly.

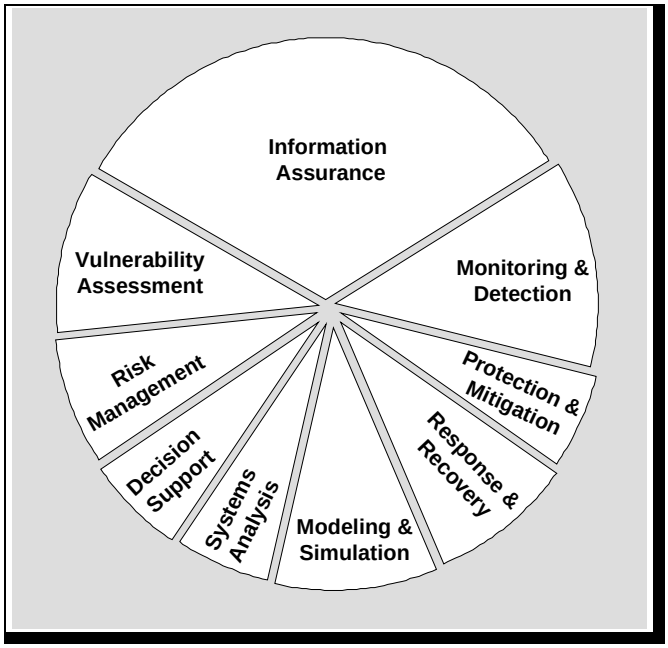


Figure 3.3 Near-term Resource Requirements by Theme

Section 4
Next Steps

The "next steps" observations and recommendations presented in this section focus on the roadmapping process and preliminary roadmapping results. Organizational issues relative to how the U.S. government should implement and structure a public-private R&D partnership to reduce the vulnerability of our infrastructures are not addressed. Rather, these issues are the focus of interagency deliberations and high-level policy directives. Clearly, however, extensive coordination, cooperation, education and awareness training, and information sharing are required. Establishing and coordinating R&D agendas and programs to encourage the introduction of increasingly capable methods for protecting our infrastructure will be especially challenging.

4.1 Essential Elements of Information for Future Roadmapping

The preliminary roadmapping information was developed over a four-month period without the benefit of formally validated requirements (needs), a baseline inventory of ongoing infrastructure-assurance-related R&D activities, or full knowledge of applicable commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) technology. All of these elements are essential to ensure that:

- The R&D roadmap comprehensively validated requirements;
- Individual R&D topics are not addressed elsewhere; and
- New research efforts focus on critical R&D gaps.

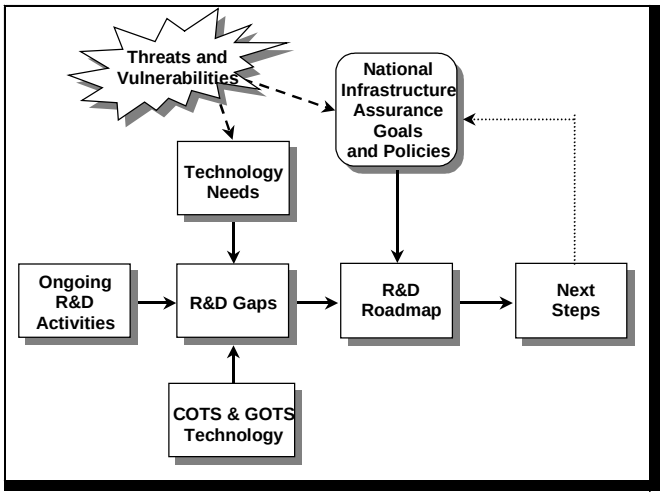


Figure 4.1 Essential Elements of Information for R&D Roadmapping

Figure 4.1 depicts the essential elements of information needed for developing a comprehensive and defensible R&D roadmap. The threats to, and the vulnerabilities of, our interdependent infrastructures drive the need for technology. Research and development gaps, or shortfalls, are determined by comparing needs with ongoing R&D activities, which may be directly or indirectly related to infrastructure assurance, and applicable COTS and GOTS technology. Clear national infrastructure

assurance goals and policies provide a basis for prioritizing, sequencing, and determining the pace of new R&D activities.

The study team recommends that all of the essential elements of information shown in Figure 4.1 should be assembled so that the preliminary roadmapping information can be critically reviewed and revised, as needed, to develop an R&D plan to meet national infrastructure assurance goals. To accomplish this recommendation may necessitate a formal requirements analysis process along with a survey to identify ongoing R&D activities within the various departments and agencies. Existing program plans and databases may contain some of these data. Although the study team members used their considerable knowledge, insight, and judgment concerning these elements of information, further study in this area is warranted so that defensible decisions can be made regarding resource allocation and scheduling.

4.2 Portfolio Considerations

From a national perspective, the relevant ongoing and new R&D activities should be viewed as an integrated portfolio designed to meet specified infrastructure assurance goals. As such, this portfolio should meet supporting strategic, technical, and programmatic objectives. Strategically, it should support the timely development of technologies that address the threats to, and vulnerabilities of, critical national infrastructures. Development of such technologies requires working effectively with the private sector (Figure 1.1). Technically, this portfolio should include basic, applied, advanced technology development, and proof-of-principle and validation research. This research should balance funding and development timeframes with degrees of technical risk. Programmatically, the portfolio should include diverse R&D projects that, to the extent possible, comprehensively address the requirements of the various infrastructures. These portfolio considerations should be debated at the interagency level.

4.3 Policy Considerations

As depicted in Figure 4.1, R&D must be consistent with, and responsive to, national infrastructure assurance policy (e.g., as promulgated through Presidential Decision Directives), which is intended to assure the continuity and viability of our nation's critical infrastructures. Such policy provides a framework for establishing R&D objectives, setting R&D priorities, and shaping a multiyear, multifaceted R&D portfolio that is commensurate in scope and scale with the physical and cyber challenges of the twenty-first century. It also provides a framework for establishing education and awareness programs, building partnerships with industry, and developing legislative initiatives intended to reduce vulnerabilities. It is essential, therefore, that R&D be viewed in a policy context as one element of an integrated national strategy, and that the effects of policies on private-sector actions (e.g., the commercialization of technologies to reduce vulnerabilities) be understood more fully and considered in developing an R&D plan.

4.4 Technology Transfer Considerations

Technology transfer and embedding should be an integral part of the R&D process. The spectrum of R&D identified in this roadmap — basic, applied, advanced technology development, and proof-of-principle and validation — must be accompanied by technology development within the private sector to ensure that useful, usable, and used products are developed. The R&D activities must be linked with commercialization activities, including engineering and manufacturing development, technical integration, testing, and fielding (Figure 1.1). Such linkages require effective partnerships with the private sector, sensitivity to economic and other barriers faced by industry in commercializing technologies, and the involvement of infrastructure owners and operators. A technology transfer plan should be prepared along with an R&D plan to elevate awareness of the issues and accelerate the introduction of infrastructure assurance technologies.

4.5 Interdependency and Complexity Considerations

A new "science" of interdependent, complex systems should be developed. This science would provide the theoretical foundation for developing the diverse vulnerability assessment, monitoring, predictive modeling, and consequence analysis technologies needed for addressing infrastructure assurance issues as they relate to the critical national infrastructures. Concepts, such as system complexity, interaction, and coupling, should be examined.

In-depth research on the complexities and interdependencies in the national infrastructure is needed. Each of our national infrastructures depends to varying degrees on the other infrastructures. Some dependencies are readily apparent, such as the strong reliance of the infrastructures on information and communications systems and electric power. Other dependencies are second or third order and appear only after long time periods or under extreme conditions. Researchers should identify and characterize such interdependencies and the associated dynamic feedback and response mechanisms. Research that evaluates historical incidents and probes possible scenarios would lead to a more focused research agenda.

A national repository of validated infrastructure-related models and data (including GIS information) should be established and linked closely to test beds. The test beds would be used to test the nation's infrastructure under actual working conditions, and test analysis, assessment, advanced predictive modeling, and other modeling and simulation systems and tools. Such a repository would support prevention, mitigation, incident response, and recovery objectives in both planning and analysis and crisis situations.

4.6 Other Ingredients for a Successful R&D Program

Various forums, such as conferences, workshops, and joint planning meetings, should be established. These forums would bring together researchers, private-sector infrastructure owners and operators, and government agencies to discuss common problems and requirements, to establish research agenda, and to promote creative thinking on solutions to infrastructure problems.

R&D-related training, education, and awareness programs should be established. These programs would enhance our "intellectual" infrastructure by helping to build a cadre of knowledgeable people ("infrastructure practitioners") within the federal government and the private sector. Also, they would ensure that the new technologies, methods, and tools that result from R&D efforts are implemented and used properly.

Section 5
Subject-matter Experts and Reviewers

The individuals listed below assisted the study team by helping to identify R&D topics and technical and programmatic issues; by providing background materials and studies for review; by facilitating coordination and outreach activities; and by providing insight into the value of R&D for protecting and assuring our critical national infrastructures. Many also provided valuable review comments on earlier drafts of this report.

Banking and Finance

Dennis Dutterer — *BOT Clearing Corporation*
Bill Finnamore — *INTEGRION*
Don Hawkins — *TCF Bank Holding Company*
Don Karmzian — *Chicago Board of Trade*
Joe Kubat — *Security Information Automation Corporation*
Edward Kufeldt — *Defense Finance and Accounting Service*
Bruce W. Moulton — *Fidelity Investments*
Kit Nedham — *Banking Information Technology Secretariat*
John Petersen — *LaSalle National Bank*
Dan Schutzer — *Citibank*
John Shelton — *On-Line Banking Association*
Tom Vartanian — *Fried, Frank, Harris, Shriver & Jacobson*

Energy

John Bartenhagen — *Defense Energy Support Center, Defense Logistics Agency*
Don Bennett — *Department of Defense*
Dennis Berry — *Sandia National Laboratories*
Stanley S. Borys — *Institute of Gas Technology*
David Cauffman — *Idaho National Engineering and Environmental Laboratory*
Michael Delurey — *Booz-Allen & Hamilton, Inc.*
David Diehl — *Joint Program Office for Special Technology Countermeasures*
Jerry Hadder — *Oak Ridge National Laboratory*
Mark Hanson — *Energy Center of Wisconsin*
Terry Hawkins — *Los Alamos National Laboratory*
William D. Ingle — *Gas Research Institute*
Maurice Katz — *Department of Energy*
James Mackey — *National Infrastructure Protection Center/Dept. of Energy*
Frank Olken — *Lawrence Berkeley National Laboratory*
Carl Piechowski — *Department of Energy*
Leslie Poch — *Argonne National Laboratory*
David Reichle — *Oak Ridge National Laboratory*

Fred Roach — *Los Alamos National Laboratory*
Ron Skelton — *Private consultant*
Jared R. Smith — *Institute of Gas Technology*
Robert Thomas — *Cornell University*
Jim VanCoevering — *Oak Ridge National Laboratory*
Gregory V. Welch — *Commonwealth Edison*
Sonny White — *Department of Defense*

Information and Communications

Michael Ackerman — *National Library of Medicine/National Institutes of Health*
Kathleen Bailey — *Lawrence Livermore National Laboratory*
Matt Bishop — *University of California – Davis*
Larry Brandt — *National Science Foundation*
Wayne Bryant — *NASA Langley Research Center*
Tom Burke — *General Services Administration*
Blaine Burnham — *National Security Agency*
Mel Ciment — *National Science Foundation*
Harry DeMaio — *Deloitte and Touche Security Services*
Virgil D. Gligor — *University of Maryland*
John Grimes — *Raytheon*
Bill Hunteman — *Los Alamos National Laboratory*
Bijan Jabbari — *George Mason University*
William E. Johnston — *Lawrence Berkeley National Laboratory*
Butler Lampson — *Microsoft Corporation*
Karl Levitt — *University of California – Davis*
Teresa Lunt — *Defense Advanced Research Projects Agency*
John McLean — *Naval Research Laboratory*
Robert Meushaw — *National Security Agency*
Larry Nelson — *AT&T*
Deborah Phillips — *Defense Information Systems Agency*
Mel Sobotka — *Booz-Allen & Hamilton, Inc.*
Stephen L. Squires — *Defense Advanced Research Projects Agency*
Dennis D. Steinauer — *National Institute of Standards and Technology*
David Tennenhouse — *Defense Advanced Research Projects Agency*
Fred Wentland — *Department of Commerce*

Transportation

Roy Allen — *Transportation Technology Center, Inc.*
Douglas Anson — *Los Alamos National Laboratory*
Allison Conway-Smith — *Amtrak*
Mark S. Daskin — *Northwestern University*
Richard Davis — *Oak Ridge National Laboratory*
Jerry Edwards — *U.S. Army Physical Security Equipment Management Office*

Thomas Falvey — *Department of Transportation*
Dan Foth — *American Public Transit Association*
Kevin Harnett — *Volpe National Transportation Systems Center*
Susan Hower — *Science and Engineering Associates*
Bill Hubbard — *National Institute for Environmental Renewal*
Paul Johnson — *Oak Ridge National Laboratory*
Pat Maier — *Boyd Maier and Associates*
Michael Maston — *Oak Ridge National Laboratory*
Howard Moody — *Association of American Railroads*
Gary Murphy — *Microsensors, Inc*.
Anita Parker — *Computer Sciences Corporation*
Rin Saunders — *Computer Sciences Corporation*
David Schulz — *Northwestern University*
LeRon Smith — *Los Alamos National Laboratory*
John Sorenson — *Oak Ridge National Laboratory*
Frank Southworth — *Oak Ridge National Laboratory*
Maurice Stewart — *Department of Defense*
Pat Student — *Union Pacific Railroad*
Richard A. Swanson — *Computer Science Corporation*
William C. Thompson — *Union Pacific Railroad*
Joyce Wegner — *Battelle Pacific Northwest Laboratory*
Athanasios Ziliaskopoulos — *Northwestern University*

Vital Human Services

Philip H. Burgi — *U.S. Bureau of Reclamation*
Paul E. Davies — *Boston Police Department*
Richard W. Hutchinson — *Chemical and Biological Defense Command*
William G. Nagle — *New York City/Mayor's Office of Emergency Management*
Donald E. Newsom — *Argonne National Laboratory*
Irwin M. Pikus, Commissioner — *Department of Commerce*
Stanley Ponce — *U.S. Bureau of Reclamation*
Geary W. Sikich — *Logistical Management Systems Corporation*
Elaine M. Sudanowicz — *Boston Emergency Management Agency*
David Tomasko — *Argonne National Laboratory*

Summary Report

Anita Jones — *University of Virginia*
Doug Sergent — *Joint Program Office for Special Technology Countermeasures*
Larry Schwartz — *University of California*
(Many of the subject-matter experts listed above also reviewed the summary report.)

Coordination Support

Don Bennett — *Department of Defense*
Maureen Clapper — *Department of Energy, New Brunswick Laboratory*