

RAND

*A Framework for the
Information Technology
Infrastructure for
Bioterrorism: Results of the
1st Summit*

Helga Rippen

DRU-2761-STPI

December 2001

Science and Technology Policy Institute

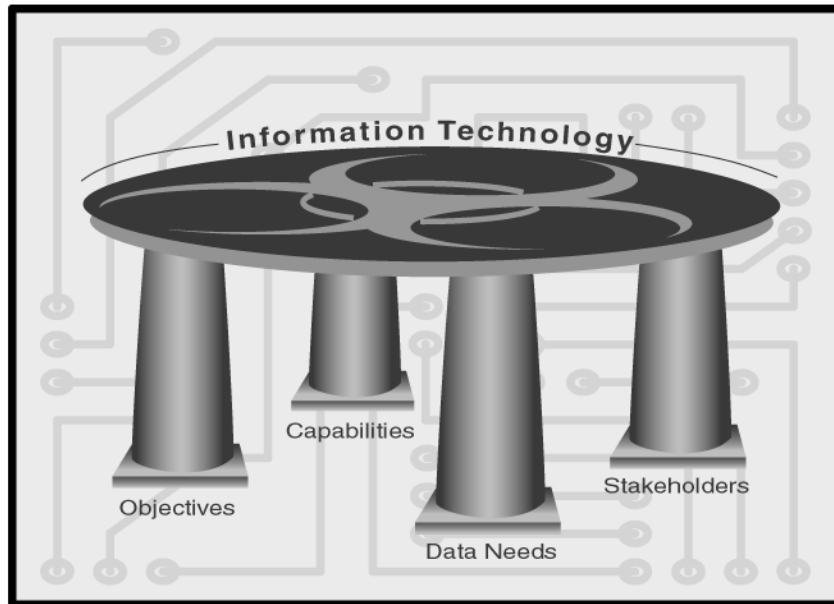
The RAND unrestricted draft series is intended to transmit preliminary results of RAND research. Unrestricted drafts have not been formally reviewed or edited. The views and conclusions expressed are tentative. A draft should not be cited or quoted without permission of the author, unless the preface grants such permission.

DRAFT
12/7/2001

DRAFT

**A Framework for the Information Technology Infrastructure
for Bioterrorism**

Results of the 1st SUMMIT



December 7, 2001

For more information please contact Helga_Rippen@rand.org

A Framework for the Information Technology Infrastructure for Bioterrorism.

Summary

This white paper is a result of the first RAND Science and Technology Policy Institute Summit on Information Technology (IT) Infrastructure for bioterrorism. There is broad-based consensus that a robust, well-conceived, state-of-the-art technology information and communication infrastructure is a core component for successful biodefense response and preparedness. The foundation for this infrastructure requires four components: OBJECTIVES, CAPABILITIES, DATA NEEDS, and STAKEHOLDERS. Building a successful IT infrastructure requires the continued participation and consensus of all the major stakeholders from conceptualization through implementation.

Introduction

Over the past few years, judicial, defense, and health agencies, among others, have grappled with the challenge of improving U.S. readiness for bioterrorist attacks. The massive devastation associated with the events of September 11th and subsequent anthrax episodes have heightened the urgency of meeting this challenge. A core element in biopreparedness is an IT infrastructure that enables the collection, analysis, and dissemination of critical information in real time to prevent or mitigate the effects on populations from a bioweapons event. This IT infrastructure does not exist¹.

On November 14, 2001, a Summit was convened by RAND's Science and Technology Policy Institute as part of its mission to address scientific and technological issues of national importance (see Appendix A for a listing of participants). The purpose of the Summit was to bring together a diverse set of stakeholders to begin the process of developing a conceptual framework needed for an IT infrastructure that could support bioterrorism preparedness efforts across the country. Cosponsors included the American College of Preventive Medicine and IEEE-USA Medical Technology Policy Committee.

Purpose

The purpose of this initiative is to build a framework for a bioterrorism IT infrastructure that will facilitate multi-sector preparedness and coordinate response efforts. Building such a framework is a three-step process.

- Step I: Define the scope and lay the foundation for building the IT infrastructure. This is the focus of Summit 1 and this document.
- Step II: Begin the process of building the framework for the IT infrastructure (Summit II and resulting white paper). The focus of this activity will be on two

¹ Report to the President: Transforming health Care Through Information Technology, President's Information Technology Advisory Committee, February 2001.

- priority areas to address bioterrorism, examining specific IT requirements (current capabilities, gaps, users, and issues).
- Step III: Examine commonalities among the IT requirements in light of the larger IT infrastructure (Summit III and the resulting white paper).

The convening of these Summits will also serve to facilitate innovative solutions for overcoming barriers. Moreover, this work will provide a comprehensive and long-term vision for building a lasting, effective IT infrastructure for national biodefense.

Methodology

Public and private stakeholders, primarily from the health, public health, and information technology sectors, were identified and invited to attend the Summit. Prior to the meeting, attendees completed a survey containing several questions that included defining an IT infrastructure, identifying barriers, and describing key users and stakeholders.² These responses formed the basis for a draft conceptual framework. The results of the survey and the Summit notes provided the basis for this document.

The Scope of Bioterrorism and Information Technology Needs

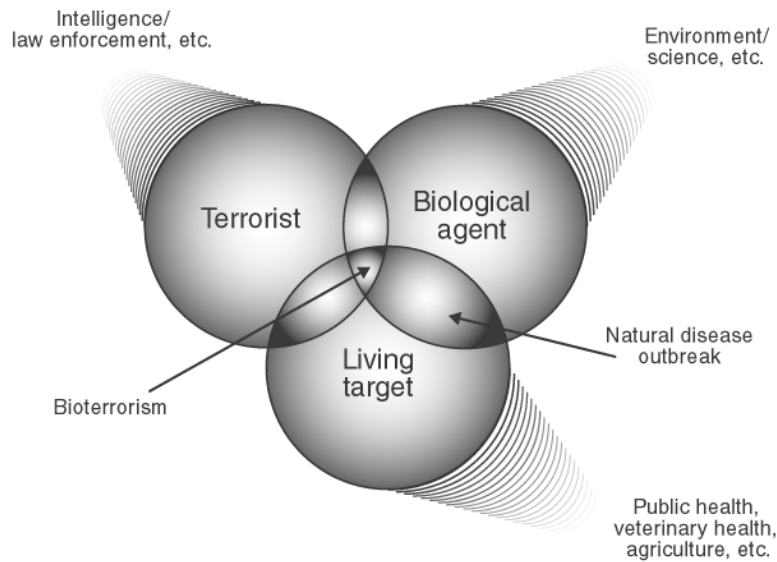
The scope of bioterrorism is vast. It brings together three distinctive elements (terrorist, biological agent, and living target) that are the responsibility of diverse professional communities, with very different areas of expertise (see Figure 1). These communities normally operate independently of one another. During a bioterrorism event these professional communities suddenly must find ways to cooperate in mutually beneficial ways, or risk jeopardizing their objectives. The national press coverage of the anthrax attacks brought these interactions to national attention and underscored the pressing need for a coordinated national approach to surveillance, communication, research, and resource management.

As highlighted in Figure 1, each of the three elements (terrorist, biological agent, and living target) engages a different professional community that has the primary responsibility for minimizing the impact of a bioterrorism event.

- Intelligence, law enforcement, diplomatic, and military communities are responsible for the terrorists. They monitor and deter terrorist movement and activity.
- The scientific (human, microbial/viral, animal, plant, and environmental) communities are responsible for the biological agents. They characterize, develop detection systems for, create vaccines and treatments for, and at times even maintain biological agents.
- Public health, medical, first responders, veterinary, and agricultural communities are responsible for the living targets. They protect the health of people, animals, and agricultural products.

² See Appendix B for the questions.

Figure 1: Bioterrorism: Intersection of three elements: terrorist, biological agent and a living target.



The involvement of these three different professional communities, hereafter referred to as sectors, has significant implications for the requirements of an IT infrastructure. It will need to not only support intra-sector requirements, but it also must meet critical inter-sector needs. This is illustrated by the following examples:

Intra-sector

A local health department has received a call to provide mass immunization to an exposed population. This will require the coordinated efforts of the entire agency. Licensed health care professionals, field staff, support personnel and others will be required to sustain the flow of concerned citizens, maintain clinical supplies, administer vaccines, meet the demand for questions from the public and the media, and maintain overall order and efficiency. The coordination and continual updating of efforts and needs agency-wide (e.g., more supplies, additional personnel) will be sustained through a robust intra-sector electronic communication and information system.

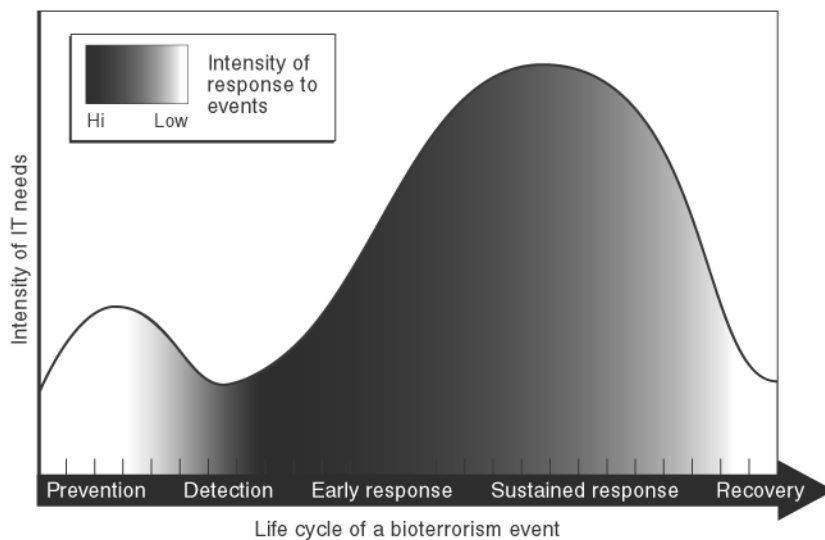
Inter-sector

The intelligence community determines that a terrorist in City A has the smallpox virus and is planning a release. This and other relevant information must immediately be passed to the public health and healthcare communities. If there is an outbreak, information regarding the numbers and pattern of illness and exposure must immediately be provided to the intelligence community to support its efforts to identify and apprehend the perpetrators. The scientific community needs to provide information to both the intelligence and public health and healthcare communities to confirm diagnosis, characterize the pathogen and provide

information regarding treatments such as vaccines, antibiotics, and investigational drugs and therapies.

The IT needs will evolve as the life cycle of a bioterrorism event unfolds. The phases of the cycle will include prevention & preparedness, detection, early response, sustained response, and recovery as illustrated in Figure 2. The IT needs relate to the objectives being supported (e.g., communications, resource management), the required capabilities (e.g., data management, procedures), data needs (e.g., number of cases) and users (e.g., public health officials, general public). Since the life cycle of an attack unfolds over time, this IT infrastructure needs to support all phases of a bioterrorism event to provide continuity.

Figure 2: Conceptualization of IT needs during the phases of a bioterrorism event.



For the purposes of discussion and planning, the life-cycle of a bioterrorism event has been divided into the following five phases:

1. Prevention & Preparedness – eliminating the possibility of a biological event (e.g., ensuring that no smallpox virus exists; developing vaccines; testing of system; heightened alert status).
2. Detection – detecting the release of a biological agent or identifying a first case (e.g., detection devices; diagnosis of first case of smallpox; early warning systems).
3. Early response – initiating the response to the initial event (e.g., deployment of resources to contain biological agent; identify source; contain damage; minimize impact).

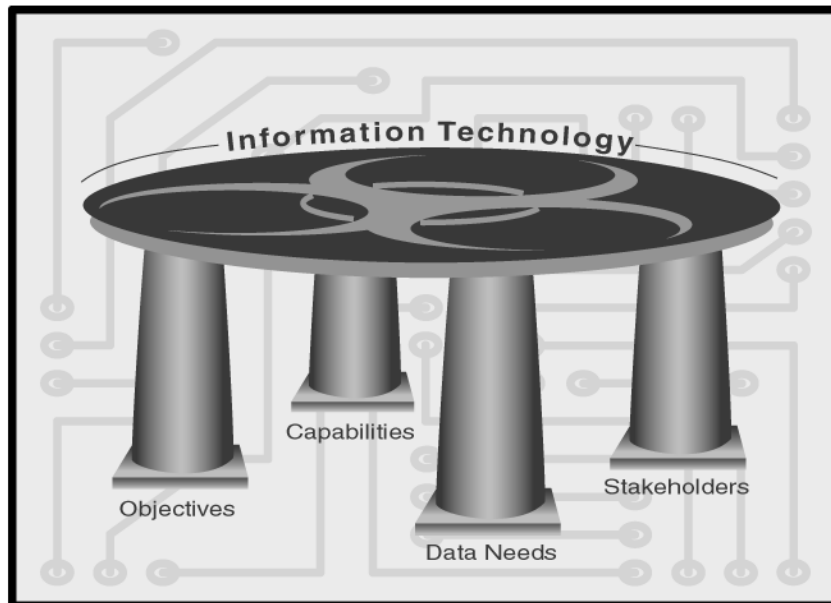
4. Sustained response – continuing the measures required to address the longer term impact of the exposure (e.g., replenishing medical supplies; providing mental health support; ensuring surge capacity for the treatment of numerous victims; monitoring exposed individuals).
5. Recovery – recovering after the biological agent is eliminated (e.g., providing mental health support; restocking vaccine and drug reserves; identifying lessons learned to improve future responses).

If one were to develop an IT infrastructure focusing on only one phase of a bioterrorism event, it would be incomplete. That said, it is important to realize that many components of an IT infrastructure required for one phase also may be critical for other stages.

Components of the foundation of an IT Infrastructure

The previous section provides an overview of the environment that the IT infrastructure will operate and support. This section describes the foundation necessary for the building of the framework.

Figure 3: The foundation for defining an IT Infrastructure.



The framework for the IT infrastructure for bioterrorism requires a foundation made up of the following four components:

- I. Objectives *What objectives will it support?*
- II. Capabilities *What capabilities will it need to support these objectives?*

III. Data *What data are needed? How will the data be organized (architecture) and communicated (standards)?*

IV. Stakeholders *Who are the stakeholders and users?*

Each of these components plays a critical role in providing part of the foundation for the development of the IT infrastructure for bioterrorism, and omitting any will cause the entire system to fail (Figure 3). Below, these components are further subdivided into appropriate categories for bioterrorism. These lists demonstrate the breadth of the components; they do not demonstrate their links (which is the focus of the next white paper).

I. Objective

The IT infrastructure needs to support the objectives of biodefense preparedness, so defining these objectives provides the foundation for the conceptual framework. The eight objectives identified to date are: strategic planning, deterrence, surveillance, communications, coordination, resource management, education and training, and research and development (see Table 1).

Table 1: Proposed objectives to address bioterrorism.

Objective	Examples
1. Strategic planning	<ul style="list-style-type: none">• Assessing lessons learned• Developing a coherent plan• Modeling to help predict future needs• Defining roles and responsibilities• Establishing governance (i.e., chain of command)
2. Deterrence	<ul style="list-style-type: none">• Participating in international activities to mitigate the recruitment of terrorists• Law enforcement and military action to halt terrorist activities• Controlling the movement of biologic and relevant equipment• Intelligence gathering (satellite, etc.) to identify terrorist plots
3. Surveillance (detection and monitoring)	<ul style="list-style-type: none">• Quick assessment capabilities to permit a rapid response• Integration of detection data with other data systems• Ability to analyze and interpret data, case finding, automatic flags for suspect events or patterns

	<ul style="list-style-type: none"> • Detection of disease trends using algorithms and automated alerting mechanisms • Exposed, treatments, forensics • Resource use (e.g., pharmacy data) • Data collection, identification of cases, surveillance • Monitoring agent movement
4. Communications	<ul style="list-style-type: none"> • Getting the right data to the right people at all levels at the right time (e.g., federal, state, local, primary care providers, first responders, public, media) • Risk communication • Links to all stakeholders
5. Coordination (e.g., response)	<ul style="list-style-type: none"> • Incident command system • Supply management system • Research and development coordination
6. Resource management	<ul style="list-style-type: none"> • Getting materials to the appropriate site at the right time • Tracking experts in field, antidotes, vaccines, and treatments
7. Education and training	<ul style="list-style-type: none"> • Early recognition and warning signs • Treatment • Threat scenarios, training and testing • Protocols for an event • How to use IT
8. Research and development	<ul style="list-style-type: none"> • Pulling in data from biogenetic research and fingerprinting • Modeling, simulation, forecasting, accountability • User interface, usability

II. Capabilities

In order to support an objective, the IT infrastructure has to provide a set of capabilities. Using the term *capabilities*, as opposed to *technologies*, avoids the pitfalls associated with favoring a specific, potentially dated, technology. These capabilities have been grouped into six major areas – connectivity, data, procedures and applications, systems, security, and operations/management. These may expand based on stakeholder needs.

Table 2: Proposed IT infrastructure capabilities for bioterrorism

Capability	Examples
1. Connectivity	<ul style="list-style-type: none"> • Global connectivity (to all stakeholders) internationally • Interoperability • Networks • Multi-lateral conferencing • Links between databases, information sources, information systems
2. Data management	<ul style="list-style-type: none"> • Data standards and vocabularies • Capture data from many sources, eliminating replicate data while optimizing data capture from multiple sources (pharmacy, surveillance systems, medical records) • Multiple languages • Integration of tools, e.g., Graphical interface (GIS, etc.) • Integration of data (e.g., geographic, health and time (for trending)) • Standard measures
3. Procedures and applications	<ul style="list-style-type: none"> • Proactive surveillance tools • Trending tools • Quality assurance • Protocols • Profiling (match information to user group) and push technology (e.g., move information to the desktop) • Resource management tools
4. Systems	<ul style="list-style-type: none"> • Multiple use infrastructure • Common language • Hardware • 24 hours, 7 days a week for 365 days • Redundancy (including different technologies) • Integrity, Availability, and Reliability • Testing
5. Security	<ul style="list-style-type: none"> • Access • Hardened against cyberattacks (and hacking) • Use of biometrics
6. Operations/Management	Maintenance of systems

III. Data

With the objective and capabilities components of the framework in place, the specific data/information needs to constitute the third component. Data are categorized in the following eight general areas: content, procedural, health, behavior, resource, environmental, research, and quality. These may expand based on stakeholder requirements.

Table 3: Proposed IT infrastructure data needs for bioterrorism

Data Needs	Examples
1. Content	<ul style="list-style-type: none"> • Information for stakeholders (e.g., journal articles, educational materials)
2. Procedural	<ul style="list-style-type: none"> • Protocols
3. Health	<ul style="list-style-type: none"> • Medical data (e.g., chief complaint, demographics, exposure history, current medications, selected laboratory values, selected symptoms, markers for disease, digital images, underlying conditions) • Baseline • Immunization records • Contact information for responders
4. Behavioral	<ul style="list-style-type: none"> • Immigration • Travel, financial • Absenteeism • Transportation patterns • 911 calls • Retail purchases of key items • Web requests for information (e.g., queries on web sites on flu symptoms)
5. Resource	<ul style="list-style-type: none"> • Utilization (e.g., hospital stays) • What is available (e.g., antibiotics, vaccines, ICU, emergency response, body bags, blood products) • Inventory and tracking of agents, labs and individuals • Biogenetics (e.g., genetic fingerprints), equipment, supplies • Workforce (e.g., healthcare, public health, experts)
6. Environmental	<ul style="list-style-type: none"> • Geographic information • Monitoring data for biological agent • International and economic forces • Weather patterns
7. Research	<ul style="list-style-type: none"> • Economic model • Testing

8. Technology	<ul style="list-style-type: none"> • Software, hardware inventory • Data integrity data • Reliability data
---------------	---

IV. Stakeholders & Users

The success of any IT infrastructure depends upon the participation of the stakeholders early in the process. The participation of the stakeholder groups listed below – either through attendance at the Summit or by soliciting their feedback – will be a part of this effort.

Table 4: Proposed IT Infrastructure Stakeholders & Users

Stakeholder and Users	Examples
1. General Public	<ul style="list-style-type: none"> • National Consumers League
2. Health and healthcare	<ul style="list-style-type: none"> • Public Health (ASTHO, NACCHO, CSTE, CDC) • Healthcare providers (physicians, nurses, pharmacists, mental health, etc.) • Health care delivery systems (hospital, health clinics, nursing homes, etc.) • Trade and professional organizations • Drug, vaccine, biotech & device manufacturers • Laboratories • International health organizations (WHO, PAHO, etc.)
3. First responders	<ul style="list-style-type: none"> • Fire and law enforcement officials, FEMA, EMS, public health • Red Cross
4. Agricultural	<ul style="list-style-type: none"> • Farmers • Veterinarians
5. Environmental	<ul style="list-style-type: none"> • Geographic information • Monitoring data for biological agent
6. Private Sector	<ul style="list-style-type: none"> • Businesses • Unions
7. Education	<ul style="list-style-type: none"> • School system • University • Trade associations
8. Communications industry	<ul style="list-style-type: none"> • Media • Technology (trade associations) • Telecommunications (trade associations)
9. Standards organizations	<ul style="list-style-type: none"> • HL-7, ICD-9 CNM, SnoMed • National Uniform Billing and Claim CTTE

10. Government	<ul style="list-style-type: none"> • International • Federal <ul style="list-style-type: none"> ○ Executive (agencies and advisory groups, e.g., NCVHS, PITAC) ○ Legislative ○ Judicial • State and local <ul style="list-style-type: none"> ○ Executive ○ Legislative ○ Judicial
----------------	--

Issues, Gaps and Barriers

The successful implementation of a bioterrorism preparedness-directed IT infrastructure necessitates the consideration of many issues, gaps, and barriers. Though some may require lengthy periods of transition, many can be solved with appropriate and creative interventions. The participants of the first Summit listed a significant number of issues, gaps and barriers that could be addressed (Table 5). These are aggregated into six major categories: jurisdictional/cultural, societal, technology, resources, knowledge, and workforce. Many may cut across categories and some may expand or contract over time.

Table 5: Issues, Gaps and Barriers

Issue, Gap or Barrier	Examples
1. Jurisdictional/cultural	<ul style="list-style-type: none"> • Cultural resistance to change • Lack of a common language across stakeholders • International issues (e.g., legal, language) • Paper-based culture • Lack of appreciation of IT • Lack of vision • Need definition of problem • Stove pipe approaches • Distrust • Possessiveness/control
2. Societal	<ul style="list-style-type: none"> • Managing public reaction to threat • Privacy (e.g., personal identifier, access) • Media influence • Legal issues (e.g., liability) • Economics (e.g., who will pay for damages) • Lack a common vision for an IT infrastructure for health

3. Technological	<ul style="list-style-type: none"> • Not capable of capturing health information from a population level • Evidence of effectiveness • Limited data • Lack of quality and completeness of data • Duplication of effort and resources • Lack of Scalability • Unknown surge capabilities • Lack of data on current infrastructure • Incompatibility, lack of standards (e.g., vocabularies)
4. Resource	<ul style="list-style-type: none"> • Lack of resources (e.g., personnel, equipment) • Cost of false alarms • Technology costs • Financial to address the attack • Surge capacity, stockpiling • Manufacturing capabilities
5. Knowledge	<ul style="list-style-type: none"> • Understanding of public health • Efficacy of vaccines • Biological agents and treatment • Algorithms, protocols, guidelines, simulations
6. Workforce	<ul style="list-style-type: none"> • IT training • Retention (compensation, training, skills, etc.)

Recommendations

- Continue this process to develop a consistent, consolidated effort to develop an IT infrastructure for national biodefense preparedness and response.
- Assure broad and inclusive representation from all stakeholder groups.
- Build consensus among stakeholders.
- Disseminate findings widely and provide a public forum for review.
- Develop a high-level requirements document that is technology-neutral to support evolving technologies.
- Aim for sufficient flexibility in the IT infrastructure to support unanticipated terrorist attacks and bioterrorist weapons.
- Build an IT infrastructure that can grow incrementally to meet future needs.
- Encourage the participation of industry to insure that the plan is implementable (e.g., cost-effective, technologically feasible, user friendly).
- Identify or create an appropriate governance mechanism to ensure appropriate planning and development of this IT infrastructure.

Next Steps:

- Dissemination and further refinement of this conceptual framework through open discussions and comments.
- Development of a list of priority areas and assessment of current capabilities.
- Evaluation of capabilities and gaps to begin building an IT framework.

Note

This is a draft document. Your comments are welcome.

Helga E. Rippen, MD, PhD, MPH
Director
Science and Technology Policy Institute
RAND
1200 Hayes Street
Arlington, VA 22202-5050
703 413-1100 Ext. 5574
703 414 4785 (fax)
Helga_Rippen@rand.org
<http://www.rand.org/scitech/stpi/>

Definitions:

- IT infrastructure in this paper combines the hardware (computers) and connectivity (network connections) that allows deployment of information and communication systems and the IT architecture - the totality of the data, processes, and technology used in an enterprise, and the relationships between them, including databases, applications, procedures, hardware, software, and networks
- Prevention - the act of preventing or hindering³; stopping an event before it happens
- Detection - the act of detecting; the state or fact of being detected⁴; determining that an event has occurred
- Monitoring - to watch, keep track of, or check usually for a special purpose⁵
- Surveillance - close watch kept over someone or something⁶
- Communications - a system (as of telephones) for communicating⁷
- Coordination - the act or action of coordinating; the harmonious functioning of parts for effective results⁸

³ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

⁴ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

⁵ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

⁶ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

⁷ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

⁸ Merriam-Webster Dictionary, <http://www.m-w.com/cgi-bin/dictionary>, November 2001

Appendix A: List of Participants

Mark Abdy, House Committee on Science
Jacquelyn Admire, American Academy of Family Physicians (AAFP)
Dixie Baker, Science Applications International Corporation
Ed Balkovich, RAND
Dwight Bartholome, Hawaii
Mary Benner, Pennsylvania
Carol J. Bickford, American Nurses Association (ANA)
Claire Bloome, Center for Disease Control (CDC)
Galen Boch, Ohio
Willis Bradwell, Washington, DC
Carol K. Brown, National Association of County and City Health Officials (NACCHO)
K. Lynn Cates, The Dr. Spock Company
Anthony Chan, American Academy of Pediatrics (AAP)
Bob Childs, Rhode Island
Virginia Dato, American Association of Public Health Physicians (AAPHP)
Peter L. Elkin, Mayo Medical School
Frank Ferrante, IEEE-USA
Seth Foldy, Milwaukee Health Department/NACCHO
Brian E. Formato, Training Resources Group, Inc. (TRG)
Jack Frost, Maryland
Rosemary Gibson, The Robert Wood Johnson Foundation
Scott Giles, Committee on Science
Elin Gursky, Johns Hopkins Center for Civilian Biodefense Studies
Larry Hammerhan, Wisconsin
Ed Hammond, American Medical Informatics Association (AMIA)/Duke University
Peter L. Kitch, KIPHS Project Office
Alana D. Knudson-Buresh, Association of State and Territorial Health Officials (ASTHO)
Luis G. Kun, IEEE-USA
Martin Libicki, RAND
Art Limacher, Vermont
Scott Loomis, Training Resources Group, Inc. (TRG)
Denise Love, National Association of Health Data Organization (NAHDO)
Janet M. Marchibroda, eHealth Initiative
Margaret Moorehouse, Training Resources Group, Inc. (TRG)
Fran Muskopf, Washington
Rosemary Nelson, United States Military Cancer Institute, Healthcare Information and Management Systems Society (HIMMS)
Eduardo Ortiz, Agency for Healthcare Research and Quality (AHRQ)
J. Marc Overhage, American Medical Informatics Association (AMIA)
Denton, Peterson, APHCIO
Carl Picconatto, Office of Representative Constance Morella
Ronald K. Poropatich, American Telemedicine Association (ATA)
Dena Puskin, Department of Health and Human Services (DHHS)
Robert Rehm, American Association of Health Plans (AAHP)

DRAFT
12/7/2001

Jordan Richland, American College of Preventive Medicine (ACPM)
Helga E. Rippen, Science and Technology Policy Institute, RAND
Dan Rode, American Health Information Management Association (AHIMA)
David A. Ross, Center for Innovation in Health Information Systems
Harvey Rottier, Wisconsin
Monnitue Sencmudmal, Florida
Joyce Sensmeier, HIMSS
Lisa Sheldone, RAND
Tim Stephens, National Association for Public Health Statistics and Information Systems
(NAPHSIS)
Gary W. Strong, National Science Foundation
David N. Sundwall, American Clinical Laboratory Association (ACLA)
David Trinkle, Office of Management Budget (OMB)
Leslie A. Tucker, ACPM
Mike Wagner, Center for Biomedical Informatics, University of Pittsburgh
Jeff Walter, ASTHO
Bill Yasnoff, CDC

Appendix B: Questions asked of participants.

1. What problems should the IT infrastructure for bioterrorism address? (e.g., surveillance, education)
2. How would you (or your organization) define an IT infrastructure for bioterrorism? Who would be the users of the IT infrastructure? What information would they need/want? How timely and reliable does the information need to be? What would be the key components of the infrastructure? Be as specific as possible.
3. Where are there gaps in the current IT infrastructure?
4. What are major barriers to success?
5. What other organizations should be included in the discussion?