

---

May 2003

## BIOTERRORISM

# Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies



Highlights of GAO-03-139, a report to Congressional Requesters

## Why GAO Did This Study

The October 2001 anthrax attacks, the recent outbreak of the virulent Severe Acute Respiratory Syndrome (SARS), and increased awareness that terrorist groups may be capable of releasing life-threatening biological agents have prompted efforts to improve our nation's preparedness for, and response to, public health emergencies—including bioterrorism. GAO was asked, among other things, to identify federal agencies' information technology (IT) initiatives to support our nation's readiness to deal with bioterrorism. Specifically, we compiled an inventory of such activities, determined the range of these coordination activities with other agencies, and identified the use of health care standards in these efforts.

## What GAO Recommends

In order to enhance American preparedness for public health emergencies—especially those involving bioterrorism—GAO recommends that the Secretary of Health and Human Services (HHS), in coordination with other key stakeholders, develop a strategy that includes setting priorities for IT initiatives and coordinating the development of IT standards for the health care industry.

In commenting on a draft of this report, agencies concurred with our results but did not comment on the recommendations. Technical comments were incorporated as appropriate.

[www.gao.gov/cgi-bin/getrpt?GAO-03-139](http://www.gao.gov/cgi-bin/getrpt?GAO-03-139).

To view the full report, including the scope and methodology, click on the link above. For more information, contact David A. Powner at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov).

May 2003

# BIOTERRORISM

## Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies

### What GAO Found

The six key federal agencies involved in bioterrorism preparedness and response identified about 70 planned and operational information systems in several IT categories associated with supporting a public health emergency. These encompass detection (systems that collect and identify potential biological agents from environmental samples), surveillance (systems that facilitate ongoing data collection, analysis, and interpretation of disease-related data), communications (systems that facilitate the secure and timely delivery of information to the relevant responders and decision makers), and supporting technologies (tools or systems that provide information for the other categories of systems)—see table below. For example, the Centers for Disease Control and Prevention (CDC) is currently implementing its Health Alert Network, an early warning and response system intended to provide federal, state, and local agencies with better communications during public health emergencies, and the Department of Defense is using its Electronic Surveillance System for the Early Notification of Community-based Epidemics to support early identification of infectious disease outbreaks in the military by comparing analyses of data collected daily with historical trends. The extent of coordination or interaction of these systems among agencies covered a wide range—from an absence of coordination, to awareness among the agencies with no formal coordination, to formal coordination, to joint development of initiatives.

### Summary of the Systems Inventory by Agency

IT Categories	HHS	Defense	Energy	Agriculture	EPA	VA	Total
Detection	0	4	6	0	0	0	10
Surveillance	18	7	2	6	0	1	34
Communications	5	2	0	3	0	0	10
Supporting Tech	5	1	6	1	5	0	18
<b>Total</b>	<b>28</b>	<b>14</b>	<b>14</b>	<b>10</b>	<b>5</b>	<b>1</b>	<b>72</b>

Source: GAO.

IT can more effectively facilitate emergency response if standards are developed and implemented that allow systems to be interoperable. The need for common, agreed-upon standards is widely acknowledged in the health community, and activities to strengthen and increase the use of applicable standards are ongoing. For example, CDC has defined a public health information architecture, which identifies data, communication, and security standards needed to ensure the interoperability of related systems. Despite these ongoing efforts to address IT standards, many issues remain to be worked out, including coordinating the various standards-setting initiatives and monitoring the implementation of standards for health care delivery and public health. An underlying challenge for establishing and implementing such standards is the lack of an overall strategy guiding IT development and initiatives. Without such a strategy to address the development and implementation of standards, agencies may not be well positioned to take advantage of IT that could facilitate better preparation for and response to public health emergencies—including bioterrorism.

---

# Contents

---

<b>Letter</b>		1
Results in Brief		3
Background		5
About 70 Bioterrorism-Related Information Technology Activities Identified at Six Federal Agencies		17
Health Care Sector Making Progress on Defining Standards, but Implementation Challenges Remain for Effective Information Sharing		21
Emerging Information Technologies Could Enhance Agencies' Abilities to Prepare for and Respond to Public Health Emergencies		26
Conclusions		29
Recommendations		30
Agency Comments and Our Evaluation		31
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	34
<b>Appendix II</b>	<b>CDC Biological Diseases/Agents List</b>	37
<b>Appendix III</b>	<b>Categories of Information Technology for Bioterrorism-Related Systems</b>	39
Detection		39
Surveillance		41
Diagnostic and Clinical Management		45
Communications		46
Supporting Technology		48
Other Clinical Systems		50
<b>Appendix IV</b>	<b>Department of Agriculture's Systems Inventory</b>	51
<b>Appendix V</b>	<b>Department of Defense's Systems Inventory</b>	56
<b>Appendix VI</b>	<b>Department of Energy's Systems Inventory</b>	62

---

<b>Appendix VII</b>	<b>Department of Health and Human Services' Systems Inventory</b>	68
<b>Appendix VIII</b>	<b>Department of Veterans Affairs' Systems Inventory</b>	79
<b>Appendix IX</b>	<b>Environmental Protection Agency's Systems Inventory</b>	80
<b>Appendix X</b>	<b>Federal Agencies' Information Technology Initiatives</b>	83
<b>Appendix XI</b>	<b>List of Selected Health Care Standards</b>	87
<b>Appendix XII</b>	<b>Comments from the Department of Defense</b>	88
<b>Appendix XIII</b>	<b>Comments from the Department of Energy</b>	89
<b>Appendix XIV</b>	<b>Comments from the Department of Health and Human Services</b>	90
<b>Appendix XV</b>	<b>Comments from the Department of Veterans Affairs</b>	95
<b>Appendix XVI:</b>	<b>GAO Contacts and Acknowledgments</b>	96
	GAO Contacts	96
	Acknowledgments	96

---

---

## Tables

Table 1: Summary of the Systems Inventory by Agency	18
Table 2: Summary of Detection Systems by Agency	40
Table 3: Summary of Surveillance Systems by Agency	44
Table 4: Summary of Communications Systems by Agency	47
Table 5: Summary of Supporting Technologies by Agency	50

---

## Figures

Figure 1: Local, State, and Federal Agencies Involved in Response to the Release of a Biological Agent	6
Figure 2: IT Needs during a Public Health Emergency	17

---

---

## Abbreviations

AHRQ	Agency for Healthcare Research and Quality
BASIS	Biological Aerosol Sentry and Information System
CDC	Centers for Disease Control and Prevention
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
EPA	Environmental Protection Agency
ESSENCE	Electronic Surveillance System for Early Notification of Community-based Epidemics
FDA	Food and Drug Administration
HAN	Health Alert Network
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IOM	Institute of Medicine
IT	information technology
NCVHS	National Committee on Vital and Health Statistics
NEDSS	National Electronic Disease Surveillance System
NHII	National Health Information Infrastructure
SARS	Severe Acute Respiratory Syndrome
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs
WHO	World Health Organization

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



**United States General Accounting Office  
Washington, DC 20548**

May 30, 2003

Congressional Requesters:

The October 2001 anthrax attacks highlighted long-standing weaknesses in the current public health infrastructure<sup>1</sup> and prompted efforts to improve our nation's preparedness for and response to public health emergencies, including bioterrorism.<sup>2</sup> More recent events have further heightened awareness of and anxiety related to the consequences of potential bioterrorism or other public health emergencies. For example, on March 15, 2003, the World Health Organization issued an emergency travel advisory due to an unknown form of pneumonia now known as Severe Acute Respiratory Syndrome (SARS). Originating in China, it has infected over 7,900 people and caused at least 662 deaths worldwide—with 67 probable cases reported in the United States as of May 20, 2003. Further, terrorist organizations, such as al Qaeda, may be capable of releasing life-threatening biological agents through covert or overt attacks. These events and possibilities illustrate not only the increased chances that harmful biological agents could be intentionally released into the environment, but also the rapid and widespread effects of naturally occurring infectious diseases.

Many of the activities under way to prepare for and respond to public health emergencies—including bioterrorism—are supported by information technology (IT), which can better enable public health agencies to identify naturally occurring or intentionally caused disease outbreaks and can support communications related to public health. Recent events, such as those mentioned, have led to increased action and funding for undertakings related to bioterrorism throughout the federal government. In these undertakings, it is important that the IT

---

<sup>1</sup>The public health infrastructure is the foundation that supports the planning, delivery, and evaluation of public health activities and is comprised of a well-trained workforce, effective program and policy evaluation, sufficient epidemiology and surveillance capability to detect outbreaks and monitor incidence of diseases, appropriate response capacity for public health emergencies, effective laboratories, secure information systems, and advanced communications systems.

<sup>2</sup>Bioterrorism is the threat or intentional release of biological agents (viruses, bacteria, or their toxins) for the purpose of influencing the conduct of government, or intimidating or coercing a civilian population.

---

responsibilities and activities of federal public health entities be well planned and coordinated to effectively address the response to bioterrorism, reducing the risk of duplicating efforts and creating incompatible systems.

You asked us to review federal agencies' IT efforts to support bioterrorism preparedness and response. Specifically, our objectives were to

- compile an inventory of federal agencies' current and planned IT systems and initiatives related to bioterrorism, and to identify the range of coordination activities;
- identify and describe the development and use of health care IT standards for bioterrorism-related systems; and
- review the potential use of emerging information technologies to support bioterrorism preparedness and response.

We focused our review on six key federal agencies that are responsible for supporting the response to bioterrorism and other public health emergencies using IT: the Department of Agriculture (USDA), the Department of Defense (DOD), the Department of Energy (DOE), the Department of Health and Human Services (HHS), the Department of Veterans Affairs (VA), and the Environmental Protection Agency (EPA). Further details about our objectives, scope, and methodology are provided in appendix I.

We performed our work at USDA, DOD, HHS, VA, and EPA offices in Washington, DC; the Centers for Disease Control and Prevention (CDC) in Atlanta, GA; DeKalb County Board of Health in Decatur, GA; Lawrence Livermore and Sandia National Laboratories in Livermore, CA; Sandia National Laboratory in Albuquerque, NM; Los Alamos National Laboratory in Los Alamos, NM; Denver County Department of Health in Denver, CO; and Monroe County Department of Health in Rochester, NY, from June 2002 through March 2003, in accordance with generally accepted government auditing standards.

---

## Results in Brief

The six key federal agencies involved in bioterrorism preparedness and response have a large number of existing and planned bioterrorism-related information systems. Specifically, these agencies identified 72 information systems and supporting technologies, as well as 12 other IT initiatives. Of the 72 systems, 34 are surveillance systems, 18 are supporting technologies, 10 are communications systems, and 10 are detection systems.<sup>3</sup> For example, CDC is currently implementing its Health Alert Network, an early warning and response system intended to provide federal, state, and local agencies with better communications during public health emergencies. DOD is using its Electronic Surveillance System for the Early Notification of Community-based Epidemics to support early identification of infectious disease outbreaks in the military by comparing analyses of data collected daily with historical trends. In planning or operating each of these information systems and IT initiatives, the extent of coordination or interaction between the lead agency and other related government agencies covered a wide range. Such coordination ranged from an absence of contact with other agencies, to awareness among the agencies, to formal coordination, to joint development of initiatives. For example, about 30 percent of the systems and initiatives are formally coordinated or jointly developed with other agencies.

The identification and implementation of health care data, communications, and security standards—which are necessary to support the compatibility and interoperability of agencies' various IT systems—remain incomplete across the health care sector. However, efforts in the federal government are under way to strengthen and increase the use of applicable standards throughout the nation's health information infrastructure. For example, CDC has defined a public health information architecture, which identifies public health data, communications, and security standards that are needed to ensure the interoperability of related systems. At the same time, this architecture is still evolving, and many issues—such as coordination of the various efforts to ensure consensus on standards, establishment of milestones, and implementation

---

<sup>3</sup>*Surveillance* systems facilitate the performance of ongoing collection, analysis, and interpretation of disease-related data. *Supporting technologies* are tools or systems that provide information for the other categories of systems. *Communications* systems facilitate the secure and timely delivery of information to the relevant responders and decision makers. *Detection* systems consist of devices for the collection and identification of potential biological agents from environmental samples that include an IT component that facilitates the collection of data for surveillance.

---

mechanisms—remain to be worked out. Consequently, federal agencies and others associated with the public health infrastructure cannot ensure their systems' abilities to exchange data with other systems when needed and cannot ensure effective preparation for and response to bioterrorism and other public health emergencies. For example, according to CDC officials, one of the IT challenges encountered by public health officials responding to the anthrax events of October 2001 was the issue of exchanging data between the many participants involved in the response—clinical sites, local health departments, emergency responders, state health departments, public health laboratories, and federal agencies. During this event, participants accumulated dissimilar data and principally exchanged it manually. An underlying challenge for establishing and implementing standards is that no overall strategy guides IT development and initiatives.

The use of emerging information technologies to support the public health infrastructure could help to improve federal agencies' abilities to prepare for and respond to public health emergencies. Agencies have taken steps to adopt such emerging technologies. For example, Los Alamos National Laboratory is working on a Web-based system called the Forensics Internet Research Exchange, which supports the sharing of biothreat information among research and government agencies and uses public networks to securely transport private intra-agency and interagency information. However, barriers exist, such as the lack of a mechanism for identifying and prioritizing appropriate emerging information technologies for their transition into the public health community.

We are making recommendations to the Secretary of Health and Human Services, in coordination with other key stakeholders, to develop a strategy for public health preparedness and response that includes setting priorities for IT initiatives and coordinating the development of IT standards for the health care industry.

We received written comments on a draft of this report from the Deputy Assistant Secretary of Defense for Chemical/Biological Defense at DOD, the Acting Associate Administrator for Management and Administration at DOE, the Acting Principal Deputy Inspector General at HHS, and the Secretary of Veterans Affairs. These four agencies generally concurred with our results but did not comment specifically on the recommendations. Technical comments were incorporated in this report as appropriate. USDA and EPA officials provided oral comments, which were also technical in nature and have been incorporated as appropriate. While DHS was not included as one of the agencies in our review because

---

it did not exist until the end of this engagement, we provided DHS officials with the opportunity to comment on the draft of this report, which they declined. In their comments, HHS officials stated that the focus of this report on IT overemphasized its role and does not address other components of the public health infrastructure and may simplify a complex issue. As we describe in the background section of this report, IT is a tool that enables personnel to fulfill their mission. We recognize that there are other important issues about the public health infrastructure that merit attention, such as workforce capacity and training, capacity of the public health laboratories, and variation in state public health laws, among others.

---

## Background

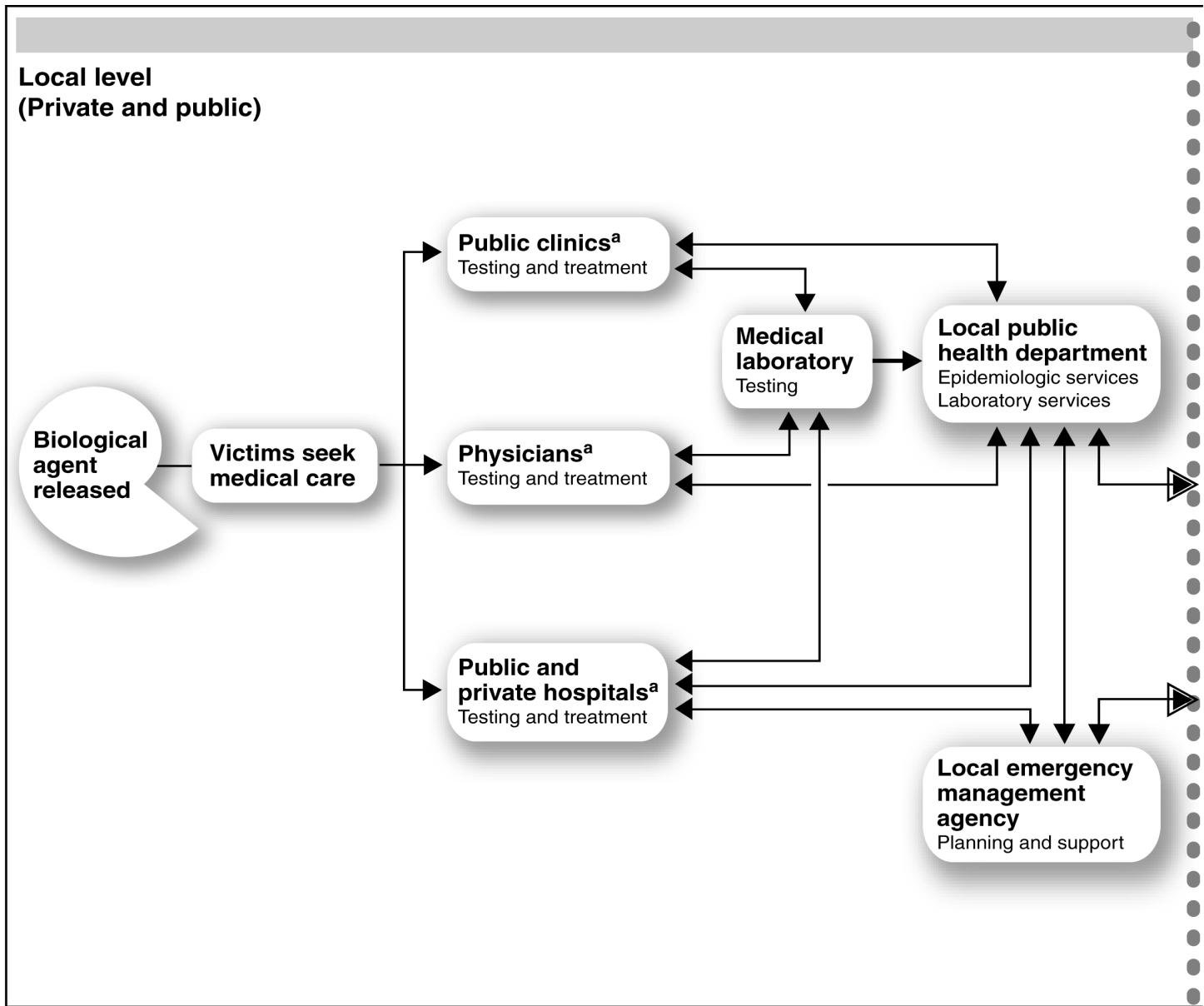
Harmful biological agents can be released by way of the air, food, water, or insects. Their release may not be recognized for several days, during which time a communicable disease—such as smallpox—can spread to others who were not initially exposed. Some biological agents—such as anthrax and plague—produce symptoms that can easily be confused with influenza or other, less virulent illnesses, leading to a delay in diagnosis or identification. For example, the recent outbreak of the new infectious disease, SARS, whose onset includes common symptoms such as high fever, coughing, and difficulty in breathing, was not recognized until about 4 months after the first known case.

Initial response to a public health emergency, including an act of bioterrorism, is generally a local responsibility that could involve multiple jurisdictions in a region, with states providing additional support when needed. Since clinicians at the local level are most likely to be the first ones to detect an incident, they and local public health officials are expected to report incidents or symptoms of suspicious illness to the state health department and other designated parties. States can provide supporting personnel, financial resources, laboratory capacity, and other assistance to local responders. Because of the many participants involved, the identification and management of bioterrorism and other public health emergencies call for effective communication and collaboration across all levels of government and the private sector. Figure 1 presents the probable series of responses to the release of a biological agent by the various players.<sup>4</sup>

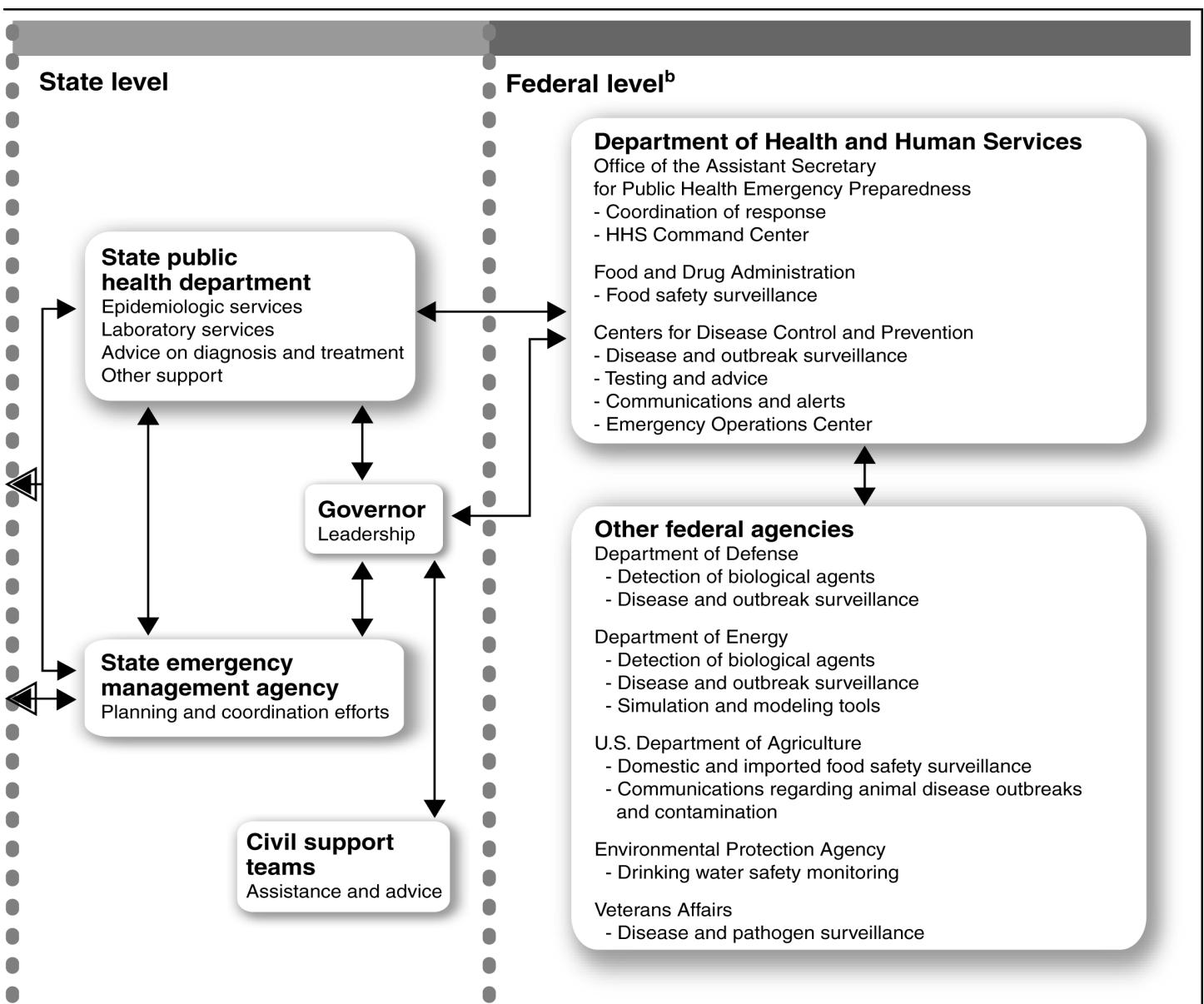
---

<sup>4</sup>U.S. General Accounting Office, *Bioterrorism: Preparedness Varied Across State and Local Jurisdictions*, GAO-03-373 (Washington, D.C.: April 7, 2003).

**Figure 1: Local, State, and Federal Agencies Involved in Response to the Release of a Biological Agent**



Source: GAO.



<sup>a</sup>Health care providers can also contact state entities directly.

<sup>b</sup>Federal departments and agencies can also respond directly to local and state entities.

<sup>c</sup>The Strategic National Stockpile, formerly the National Pharmaceutical Stockpile, is a repository of pharmaceuticals, antidotes, and medical supplies that can be delivered to the site of a biological (or other) attack.

---

Prior to the anthrax incidents in October 2001, a number of threats and hoaxes involving biological agents, and at least one successful bioterrorist act, had occurred domestically.<sup>5</sup> Since that time, health care and public health officials at the federal, state, tribal, local, and international levels, as well as the private sector—part of a complex network of people, systems, and organizations—have examined their readiness to respond to acts of bioterrorism and have found weaknesses. Among others, these weaknesses include (1) vulnerable and outdated health information systems and technologies, (2) lack of real-time surveillance and epidemiological systems, (3) ineffective and fragmented communications networks, (4) incomplete domestic preparedness and emergency response capability, and (5) communities without access to essential public health services.<sup>6</sup> These reported deficiencies at local, state, and federal levels may hinder the effective detection and identification of a potentially harmful biological agent.

The broad scope of bioterrorism activities brings together different professional communities with very diverse areas of expertise—the public health and medical community, the scientific community, and the intelligence and law enforcement community. The public health and medical community—consisting of public health officials, clinicians, traditional first responders, and veterinary and agricultural communities—is responsible for protecting the health of people, animals, and agricultural products. The scientific community—consisting of human, microbial, animal, plant, and environmental researchers, among others—characterizes, develops detection systems for, and creates vaccines and treatments for diseases caused by biological agents. The intelligence and law enforcement community—consisting of intelligence analysts, law enforcement officers, diplomatic officials, and military officers—monitor and deter terrorist movement and activity.<sup>7</sup> In addition, other professions, such as drug store pharmacists and school administrators, are being identified as new players in bioterrorism preparedness and response.

---

<sup>5</sup>In 1984 a group intentionally contaminated salad bars in local restaurants in Oregon with salmonella bacteria to prevent people from voting in a local election.

<sup>6</sup>Institute of Medicine of the National Academies, *The Future of the Public's Health in the 21st Century* (Washington, D.C.: November 11, 2002).

<sup>7</sup>RAND Science and Technology Policy Institute, *Summit on Information Technology Infrastructure for Bioterrorism* (Arlington, VA).

---

Public health and private laboratories are another vital part of the surveillance network because only laboratory results can definitively identify pathogens.<sup>8</sup> Every state has at least one public health laboratory to support its disease surveillance activities and other public health programs. State laboratories conduct testing for routine surveillance or as part of special clinical or epidemiological studies. Independent commercial and hospital laboratories may also share with public health agencies information they have gathered through their private surveillance efforts, such as studies of patterns of antibiotic resistance or of the spread of diseases within a hospital. In addition, commercial and hospital laboratories may be required by state law or regulation to report certain findings for public health surveillance.

Federal agencies have key responsibilities for bioterrorism preparedness and response. HHS has primary responsibility for coordinating the nation's response to public health emergencies, including bioterrorism. HHS divisions responsible for bioterrorism preparedness and response, and their primary responsibilities include:

- The Office of the Assistant Secretary for Public Health Emergency Preparedness coordinates the department's work to oversee and protect public health, including cooperative agreements with states and local governments. States and local governments can apply for funding to upgrade public health infrastructure and health care systems to better prepare for and respond to bioterrorism and other public health emergencies. On May 9, 2003, HHS announced that guidelines have been released for the use of \$1.4 billion allocated for bioterrorism cooperative agreements. It maintains a recently built command center, where it can coordinate the response to public health emergencies from one centralized location. This center is equipped with satellite teleconferencing capacity, broadband Internet hookups, and analysis and tracking software.
- CDC has primary responsibility for nationwide disease surveillance for specific biological agents, and it also provides an array of scientific and financial support for state infectious disease surveillance, prevention, and control. For example, CDC administers cooperative agreements for public health preparedness totaling \$870 million for fiscal year 2003. CDC has been addressing bioterrorism preparedness and response

---

<sup>8</sup>Pathogens are bacteria, viruses, parasites, or fungi that have the capability to cause disease in humans.

---

explicitly since 1998. In April 2003, CDC opened a new emergency operations center to organize and manage all emergency operations at CDC, allowing for immediate communication between CDC, HHS, DHS, as well as federal intelligence and emergency response officials, and state and local public health officials. CDC also provides testing services and consultation that are not available at the state level; training on infectious diseases and laboratory topics, such as testing methods and outbreak investigations; and grants to help states conduct disease surveillance. In addition, CDC provides state and local health departments with a wide range of technical, financial, and staff resources to help maintain or improve their ability to detect and respond to disease threats.

CDC laboratories provide highly specialized tests that are not always available in state public health or commercial laboratories, and they assist states with testing during outbreaks. These laboratories help diagnose life-threatening, unusual, or exotic infectious diseases, including those that may be caused by bioterrorist attacks, such as smallpox. CDC also conducts research to develop improved diagnostic methods, and it trains laboratory staff to use them.

- The Agency for Healthcare Research and Quality (AHRQ) is responsible for supporting research designed to improve the outcomes and quality of health care, reduce its costs, address safety and medical errors, and broaden access to effective services, including anti-bioterrorism research. AHRQ has initiated several major projects and activities designed to assess and enhance the linkages between the clinical care delivery system and the public health infrastructure. AHRQ-supported research focuses on emergency preparedness of hospitals and health care systems for bioterrorism and other public health events; technologies and methods to improve the linkages between the personal health care system, emergency response networks, and public health agencies; and training and information needed to prepare clinicians to recognize the symptoms of bioterrorist agents and manage patients appropriately.
- The Food and Drug Administration (FDA) is responsible for safeguarding the food supply, ensuring that new vaccines and drugs are safe and effective, and conducting research on diagnostic tools and treatment of disease outbreaks. It is increasing its food safety responsibilities by improving its laboratory preparedness and food monitoring inspections in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

- 
- The National Institutes of Health (NIH) is responsible for conducting medical research in its own laboratories and for supporting the research of nonfederal scientists in universities, medical schools, hospitals, and research institutions throughout the United States and abroad. Its National Institute of Allergy and Infectious Diseases has a program to support research related to organisms that are likely to be used as biological weapons. NIH is planning to implement a strategic plan for research on CDC's category A, B, and C biological agents.<sup>9</sup> A complete list of these agents is included in appendix II.
  - The Health Resources Services Administration (HRSA) is responsible for improving the nation's health by ensuring equal access to comprehensive, culturally competent, quality health care. Its Bioterrorism Hospital Preparedness program administers cooperative agreements, totaling \$498 million, to state and local governments to support hospitals' efforts toward bioterrorism preparedness and response.

Besides HHS, other federal departments and agencies are involved in bioterrorism preparedness and response efforts, including the following:

- DOD, while primarily responsible for the health and protection of its service members on the battlefield, conducts research on bioterrorism preparedness and response through agencies such as the Defense Advanced Research Projects Agency. This research supports force protection and is shared with other agencies when it may benefit the civilian population. It also has civil support responsibilities through the Joint Task Force for Civil Support, the National Guard, and the Army.
- DOE's national laboratories are developing new capabilities for countering chemical and biological threats, including biological detection, modeling, and prediction.
- EPA is responsible for protecting the nation's water supply from terrorist attack. In January 2003, it established a new homeland

---

<sup>9</sup>Category A agents include organisms that pose a risk to national security because they can be easily disseminated or transmitted from person to person; result in high mortality rates and have the potential for major public health impact; and require special action for public health preparedness. Category B agents include those that are moderately easy to disseminate and result in moderate morbidity rates and low mortality rates. Category C agents include emerging pathogens that could be engineered for mass dissemination in the future because of availability, ease of production and dissemination, and potential for high morbidity and mortality rates and major health impact.

---

security research center. The center is assessing threat management for the water supply and environmental detectors for potential use in protecting the water supply.

- USDA has become involved in bioterrorism preparedness and response because of the increasing realization that the food supply may become a vehicle for a biological attack. Biological attacks on the health of animals and plants are important because animals and plants can spread diseases and toxins that may be harmful to humans.
- VA manages one of the nation's largest health care systems and is the nation's largest drug purchaser. The department purchases pharmaceuticals and medical supplies for the Strategic National Stockpile and the National Medical Response Team stockpile. The Department of Veterans Affairs Emergency Preparedness Act of 2002<sup>10</sup> recently directed VA to establish at least four medical emergency preparedness centers to (1) carry out research and develop methods of detection, diagnosis, prevention, and treatment for biological and other public health and safety threats; (2) provide education, training, and advice to health care professionals inside and outside VA; and (3) provide laboratory and other assistance to local health care authorities in the event of a national emergency. At least one of VA's new centers is to focus on biological threats.

On June 12, 2002, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.<sup>11</sup> The legislation requires specific activities related to bioterrorism preparedness and response. For example, it calls for steps to improve the nation's preparedness for bioterrorism and other public health emergencies by increasing coordination and planning for such events; developing priority countermeasures, such as the Strategic National Stockpile; and improving state, local, and hospital preparedness for and response to bioterrorism and other public health emergencies. It also requires HHS and USDA to enhance controls on dangerous biological agents and toxins to protect the safety of food, drugs, and drinking water.

On November 25, 2002, Congress enacted legislation creating the new Department of Homeland Security (DHS).<sup>12</sup> Consolidating the functions of

---

<sup>10</sup>Public Law 107-287 (November 7, 2002).

<sup>11</sup>Public Law 107-188 (June 12, 2002).

<sup>12</sup>Public Law 107-296 (November 25, 2002).

---

22 federal agencies, DHS's primary missions include (1) preventing terrorist attacks in the United States, (2) reducing America's vulnerability to terrorism, and (3) minimizing the damage from potential attacks and natural disasters. DHS was established on January 24, 2003; most of the agencies were transferred effective March 1, 2003. According to DHS, the Secretary has until January 2004 to bring all 22 agencies into the new organization.

The new department is responsible for assisting all levels of government in meeting their responsibilities in domestic emergencies and other challenges—especially in dealing with incidents that are chemical or biological in nature—through planning, mitigation, preparedness, response, and recovery activities. DHS is to develop and deploy countermeasures to current and emerging terrorist threats. In conjunction with HHS, it is to coordinate the nation's preparedness and response to bioterrorism. Two of DHS's five divisions are to address preparedness and response to bioterrorism. The Emergency Preparedness and Response Division's mission includes assisting all levels of government, and others, in responding to domestic emergencies; the Science and Technology program's mission includes developing and deploying countermeasures to current and emerging terrorist threats, including bioterrorism. For fiscal year 2004, the President's budget requested \$365 million to develop and implement integrated systems to reduce the probability and consequences of a biological attack on the nation's civilian population and agricultural system. DHS has inherited programs from other departments that have a bioterrorism role, such as USDA's Agricultural Research Service and Animal and Plant Health Inspection Service.

We have designated the implementation and transformation of DHS as high risk and have added it to our 2003 high risk list. This designation is based on three factors. First, the implementation and transformation of DHS is an enormous undertaking that will take time to achieve in an effective and efficient manner. Second, DHS's prospective components already face a wide array of existing management and operational challenges. Finally, failure to effectively carry out DHS's mission would expose the nation to potentially very serious consequences.<sup>13</sup>

---

<sup>13</sup>U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 1, 2003).

---

## Role of Information Technology for Bioterrorism Preparedness and Response

IT can play an essential role in supporting federal, state, local, and tribal governments in bioterrorism readiness efforts. Development of IT builds upon the existing systems capabilities of local and state public health agencies, not only to provide routine public health functions but also to support public health emergencies, including bioterrorism. For public health emergencies in particular, the ability to quickly exchange data from provider to public health agency—or from provider to provider—is crucial in detecting and responding to naturally occurring or intentional disease outbreaks. It allows physicians to share individually identifiable information with public health agencies for use in performing public health activities.

In March 2001, CDC's *Public Health's Infrastructure: A Status Report* acknowledged several IT limitations in the public health infrastructure. For example, basic capability for disease surveillance systems to detect and analyze disease outbreaks is lacking for several reasons. First, health care providers have traditionally used paper- or telephone-based systems to report disease outbreaks to approximately 3,000 public health agencies. This is a labor-intensive, burdensome process for local health care providers and public health officials, often resulting in incomplete and untimely data. Second, not all public health agencies have access to the Internet or to secure channels for electronically transmitting sensitive data.

Several categories of IT can play vital roles during the course of an event. These categories are described in a technology assessment for AHRQ that was completed by the University of California San Francisco-Stanford Evidence-based Practice Center.<sup>14</sup> These categories of IT serve different but related functions and include the following:

- **Detection**—systems that consist of devices for the collection and identification of potential biological agents from environmental samples, which make use of IT to record and send data to a network.
- **Surveillance**—systems that facilitate the performance of ongoing collection, analysis, and interpretation of disease-related data to plan, implement, and evaluate public health actions.

---

<sup>14</sup>University of California San Francisco-Stanford Evidence-based Practice Center, *Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems* (Stanford, CA: June 2002). A copy of the report can be downloaded at [www.ahrq.gov/clinic/evrptfiles.htm#bio-it](http://www.ahrq.gov/clinic/evrptfiles.htm#bio-it).

- 
- **Diagnostic and clinical management**—systems with potential utility for enhancing the likelihood that clinicians will consider the possibility of bioterrorism-related illness. These systems are generally designed to assist clinicians in developing a differential diagnosis for a patient who has an unusual clinical presentation.
  - **Communications**—systems that facilitate the secure and timely delivery of information to the relevant responders and decision makers so that appropriate action can be taken.
  - **Supporting technologies**—tools or systems that provide information for the other categories of systems (e.g., detection, surveillance, etc.).<sup>15</sup>

Recognizing the importance of IT to strengthening the public health infrastructure, RAND's Science and Technology Policy Institute held a series of workshops between November 2001 and April 2002. The workshops brought together a diverse set of stakeholders to begin the process of developing an IT infrastructure that could support bioterrorism preparedness efforts across the country.<sup>16</sup> During these workshops, consensus was reached on the need for an overarching IT infrastructure to prepare for and respond to bioterrorism and other public health emergencies. RAND described the different phases of a bioterrorism event and the intensity of need for IT during each phase, and it proposed that a bioterrorism event could consist of the following phases:

- **Prevention and preparedness**—includes reducing the possibility of a biological event by methods such as developing vaccines, conducting desktop exercises, and heightening alert status.
- **Event recognition**—includes monitoring and detecting the release of a biological agent or identifying the first case of an illness, by methods such as using detection devices and surveillance systems and diagnosing the first case of smallpox.
- **Early and sustained response**—includes initiating the response to the initial event and then continuing the measures required to address the longer-term impact of the exposure, such as deploying resources to

---

<sup>15</sup>Categorized to take into consideration research and development projects that may offer promising techniques; not part of UCSF-Stanford Technology Assessment.

<sup>16</sup>RAND Science and Technology Policy Institute, *Summit on Information Technology Infrastructure for Bioterrorism* (Arlington, VA).

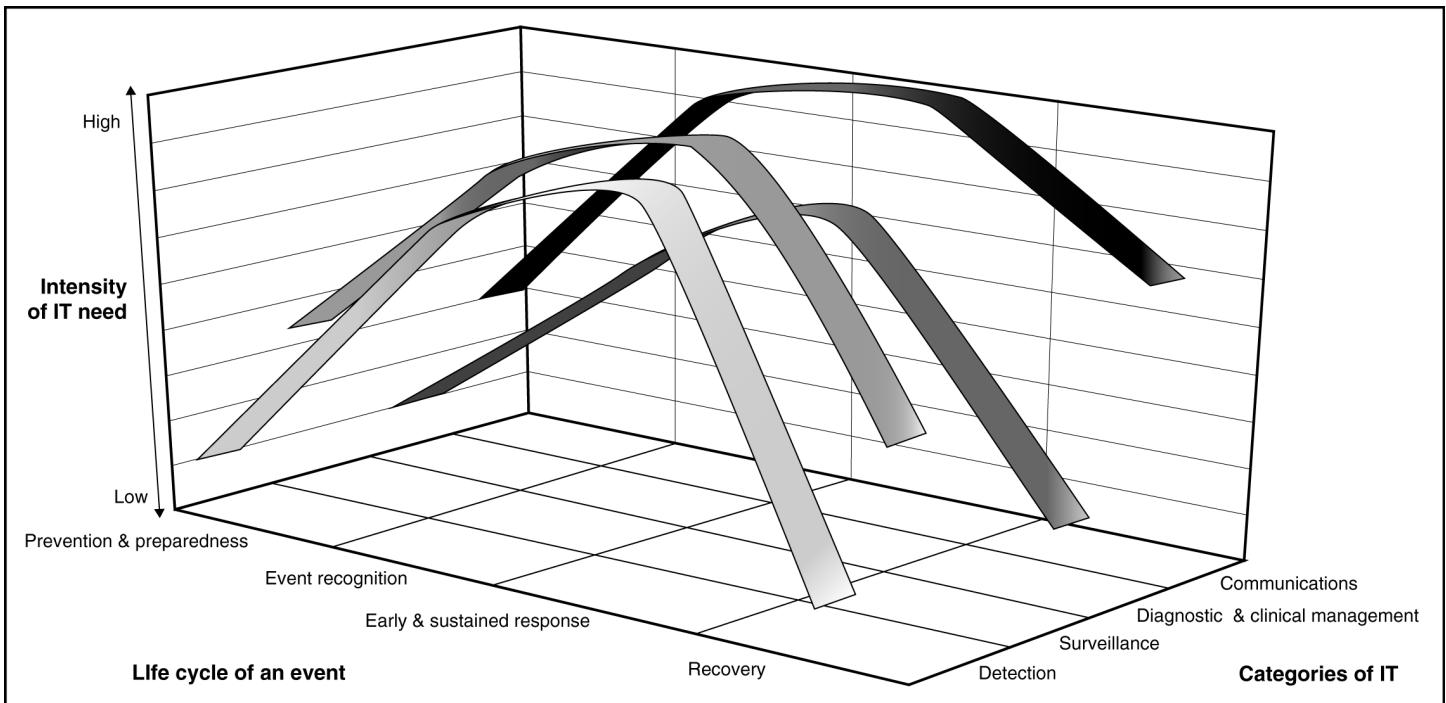
---

contain a biological agent, identifying the source, replenishing medical supplies, ensuring surge capacity for the treatment of victims, and monitoring exposed individuals.

- **Recovery**—includes recovering after the biological threat is under control, by measures such as providing mental health support, restocking vaccine and drug reserves, and identifying lessons learned to improve future responses.

According to RAND, during the course of a bioterrorism event, IT should be capable of addressing all phases of the event. Because of the dynamic and unpredictable nature of public health emergencies, various types of IT are needed during the course of an event. These systems and the intensity of their need for IT may vary from event to event, depending on the circumstances. In addition, IT components that are required for one phase may also be critical for other phases, but the intensity of need for them may vary. These needs include consideration of the phase being supported, required capabilities for each phase, and the data required at various points in time. Figure 2 illustrates the probable intensity of need for each category of IT across the different phases.

**Figure 2: IT Needs during a Public Health Emergency**



Source: RAND, UCSF-Stanford.

## About 70 Bioterrorism-Related Information Technology Activities Identified at Six Federal Agencies

The six key federal agencies involved in bioterrorism preparedness and response have a large number of existing and planned bioterrorism-related information systems. Specifically, these agencies identified 72 information systems and supporting technologies, as well as 12 other IT initiatives. Of the 72 information systems, 34 are surveillance systems, 18 are supporting technologies, 10 are communications systems, and 10 are detection systems. Additionally, in planning or operating each of these systems and IT initiatives, the extent of coordination or interaction performed by the lead agency with other related government agencies covered a wide range of activity. Coordination varied by system and IT initiative, ranging from absence of coordination, to awareness without coordination, to formal coordination, to joint development of initiatives. For example, about 30 percent of the information systems and IT initiatives are being either formally coordinated or jointly developed with another agency.

---

## Bioterrorism-Related Systems and Initiatives Identified at Six Federal Agencies

The six federal agencies with key roles in bioterrorism preparedness and response identified 72 existing or planned information systems and supporting technologies, as well as 12 other IT initiatives.<sup>17</sup> About 74 percent of these systems and IT initiatives are currently operational. The estimated costs reported for these systems exceed \$63 million for fiscal year 2003.<sup>18</sup> Of the 72 information systems identified, 34 are surveillance systems, 18 are supporting technologies, 10 are communications systems, and 10 are detection systems. Of the 12 IT initiatives, HHS identified 4, DOD and DOE identified 3 each, and USDA identified 2. Table 1 summarizes the number of systems by agency and IT category.

---

**Table 1: Summary of the Systems Inventory by Agency**

IT categories	HHS	DOD	DOE	USDA	EPA	VA	Total
Detection	0	4 <sup>b</sup>	6	0	0	0	10
Surveillance	18 <sup>a</sup>	7	2 <sup>a</sup>	6	0	1	34
Diagnostic and clinical management	0	0	0	0	0	0	0
Communications	5	2	0	3	0	0	10
Supporting technology	5	1	6	1	5	0	18
<b>Total</b>	<b>28</b>	<b>14</b>	<b>14</b>	<b>10</b>	<b>5</b>	<b>1</b>	<b>72</b>

Source: GAO.

<sup>a</sup>Includes integrated surveillance/communications systems.

<sup>b</sup>Includes an integrated detection/communication system.

Agencies identified a variety of information systems and IT initiatives, such as the following:

- HHS's 28 systems are largely in operation and are used for surveillance of diseases and illnesses, as well as for communications. As the lead federal agency for protecting the health and safety of the public, CDC is responsible for most of the systems included in the HHS inventory. For

---

<sup>17</sup>The NEDSS Base System is included in the systems inventory and the NEDSS architecture is included as an IT initiative.

<sup>18</sup>We did not validate cost information reported by the agencies. Additionally, cost information was not reported for all the systems included in our review.

---

example, CDC is currently implementing the Health Alert Network (HAN), an early warning and response system that is intended to provide federal, state, and local health agencies with better communications during public health emergencies; additional details are provided in appendix III.

- DOD, while primarily responsible for the health of its service members on the battlefield, conducts research on bioterrorism preparedness and response for force protection and shares that research with other agencies when it may benefit the civilian population. Because of the broad nature of DOD's responsibilities, it identified 14 systems in all categories. One example of a DOD system is the Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE), which supports early identification of infectious disease outbreaks in the military by comparing analyses of data collected daily with historical trends; additional details are provided in appendix III.
- DOE—specifically its national laboratories—has identified 14 research and development efforts for technologies to support detection systems, among others. An example is the Biological Aerosol Sentry and Information System (BASIS), a portable system of networked air-sampling units that are capable of detecting airborne biological incidents at large gatherings such as political conventions and major indoor and outdoor sporting events; additional details are provided in appendix III.
- USDA's Food Safety and Inspection Service is using IT to support methods of inspection to better protect the public from foodborne illness.
- EPA has five systems defined as supporting technologies—two that could potentially support surveillance activities on the safety of drinking water and three modeling and simulation tools that are used to simulate the dispersions of contaminants in water and indoor air.<sup>19</sup>
- VA has one information system that was developed for surveillance within its health care facilities.

---

<sup>19</sup>EPA relies largely on local water authorities to monitor the safety of water supplies and report the information to them.

---

Appendix III provides a detailed description of the IT categories and additional information on each, while appendixes IV through IX contain detailed descriptions of the information systems and supporting technologies by agency. Appendix X contains detailed descriptions of the IT initiatives.

---

### **Coordination Mixed Among the Information Systems and Initiatives Identified**

In planning or operating each of these information systems and IT initiatives, the extent of coordination or interaction among the lead agency and other related government agencies covered a wide range. Such coordination ranged from a lack of contact with other agencies, to awareness, to formal coordination, to joint development of initiatives. According to CDC officials, while collaboration has improved, there are still organizational difficulties related to combining resources from multiple sources to meet common goals. It is typical for staff or contractual resources funded through one mechanism to be kept separate from those funded through another mechanism.

Agencies reported that about 30 percent of systems and initiatives are being either formally coordinated or jointly developed with another agency. Of the six agencies in our review, CDC and DOE's national laboratories accounted for the majority of information systems and IT initiatives that identified formally coordinated or jointly developed initiatives. One example of a jointly developed information system is FDA's eLEXNET system. It is a secure Web-based database for sharing laboratory data on food safety among FDA, USDA, DOD, state agriculture, and state and local health laboratories. FDA also shares data with other HHS operating divisions, as well as with Customs (now part of DHS) and the Federal Bureau of Investigations (FBI). This joint effort, which is currently in the planning stage, could improve these agencies' abilities to address foodborne illnesses. In addition, CDC has several IT initiatives in coordination with state and local public health agencies.

---

## Health Care Sector Making Progress on Defining Standards, but Implementation Challenges Remain for Effective Information Sharing

To support the compatibility, interoperability, and security of federal agencies' many planned and operational IT systems, the identification and implementation of data, communications, and security standards for health care delivery and public health are essential. Although federal efforts are now under way to strengthen and increase the use of these standards, the identification and implementation of these standards remain incomplete. Several implementation challenges remain, including coordination of the various efforts to ensure consensus on standards, and establishment of milestones. Until these challenges are addressed, federal agencies cannot ensure their systems' abilities to exchange data with other systems when needed. A major consequence of not implementing such standards is the promulgation of piecemeal systems, which results in disparate systems that cannot exchange data. An underlying challenge for establishing and implementing standards is that no overall strategy guides IT development and initiatives.

---

### Key Standards for Health Care

IT standards, including data standards, enable the interoperability and portability of systems within and across organizations.<sup>20</sup> As we have reported in the past, many different standards are required to develop interoperable health information systems, which reflect the complex nature of health care delivery in the United States.<sup>21</sup>

Vocabulary standards, which provide common definitions and codes for medical terms and determine how information will be documented for diagnoses and procedures, are one type of data standard. Vocabulary standards are intended to lead to consistent descriptions of a patient's medical condition by all practitioners. The use of common terminology helps in the clinical care delivery process, enables consistent data analysis from organization to organization, and facilitates transmission of information. Without such standards, the terms used to describe the same diagnoses and procedures sometimes vary. For example, the condition known as hepatitis may also be described as a liver inflammation. The use

---

<sup>20</sup> *Interoperability* is the ability of two or more systems or components to exchange information and to use the information that has been exchanged. *Portability* is the degree to which a computer program can be transferred from one hardware configuration or software environment to another.

<sup>21</sup> U.S. General Accounting Office, *Automated Medical Records: Leadership Needed to Expedite Standards Development*, GAO/IMTEC-93-17 (Washington, D.C.: April 30, 1993).

---

of different terms to indicate the same condition or treatment complicates retrieval and reduces the reliability and consistency of data.

In addition to vocabulary standards, messaging standards are also important because they provide for the uniform and predictable electronic exchange of data by establishing the order and sequence of data during transmission. Medical messaging standards dictate the segments in a specific medical transmission. For example, they might require the first segment to include the patient's name, hospital number, and birth date. A series of subsequent segments might transmit the results of a complete blood count, one result (e.g., iron content) per segment. Messaging standards can be adopted to enable intelligible communication between organizations via the Internet or some other communications pathway. Without these standards, the interoperability of federal agencies' systems may be limited and may limit the exchange of data that are available for information sharing. In addition to vocabulary and messaging standards, there is also the need for a high degree of security and confidentiality to protect medical information from unauthorized disclosure. More detail on these and other key standards is provided in appendix XI.

---

### Need for Standards Has Been Recognized and Federal Actions are Under Way to Define and Implement Them

The need for health care data standards has been recognized for a number of years and progress has been made in defining these standards. Yet, despite these efforts, the identification and implementation of these standards remains incomplete. CDC acknowledged the need for standards specific to public health systems, and in 1995 it established the National Electronic Disease Surveillance System (NEDSS) initiative to address the limitations of current surveillance systems. These limitations included (1) the multiplicity of program-specific information systems, (2) incomplete and untimely data, (3) the unacceptable burden on health care system respondents, (4) the overwhelming volume of data to be managed by state and local health departments, and (5) the lack of state-of-the-art IT. As part of the NEDSS initiative, CDC, in collaboration with others, agreed to encourage the use of data, communications, and security standards that are required for building interoperable public health systems. CDC expects that the implementation of NEDSS will improve the reporting of disease outbreaks from the states by increasing the timeliness, accuracy, and completeness of data. According to CDC, once fully implemented, these standards are to provide the ability to merge data from laboratories with epidemiological data, in addition to providing the ability to obtain information on cross-jurisdictional outbreaks.

---

In August 1996, Congress also recognized the need for standards to improve the Medicare and Medicaid programs in particular and the efficiency and effectiveness of the health care system in general. It passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA),<sup>22</sup> which calls for the industry to control the distribution and exchange of health care data and begin to adopt electronic data exchange standards to uniformly and securely exchange patient information. According to the National Committee on Vital and Health Statistics (NCVHS),<sup>23</sup> significant progress has occurred on several HIPAA standards, however, the full economic benefits of administrative simplification will be realized only when all of the standards are in place.<sup>24</sup>

In July 2000, the NCVHS again reported on the need for standards, this time highlighting the need for uniform standards for patient medical record information. They found that major impediments to electronic exchange of patient medical information were the limited interoperability of health information systems; the limited comparability of data exchanged among providers; and the need for better data quality, accountability, and integrity.<sup>25</sup> In November 2001, NCVHS issued another report outlining a strategy, which includes developing and using standards. According to NCVHS, the public health infrastructure could be strengthened through more rapid identification and implementation of existing standards and other new standards. The Institute of Medicine (IOM) and others are also reporting on the lack of national standards for the coding and classification of clinical and other health care data, and for the secure transmission and sharing of such data.

Complementary to the work of NEDSS on identifying standards for public health systems, in 2001 the Office of Management and Budget created the Consolidated Health Informatics (CHI) initiative as one of its e-government projects to facilitate the adoption of data standards, among others, for health care systems within the federal government. The CHI

---

<sup>22</sup>Public Law 104-191 (August 21, 1996).

<sup>23</sup>A public advisory committee statutorily authorized to advise the Secretary of HHS on national health information policy.

<sup>24</sup>National Committee on Vital and Health Statistics, *Fifth Annual Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act* (Washington, D.C.: November 12, 2002).

<sup>25</sup>National Committee on Vital and Health Statistics, *Report on Uniform Patient Medical Records Information* (Washington, D.C.: July 6, 2000).

---

initiative is an interagency work group led by HHS and composed of representatives from DOD, VA, and other agencies. Recognizing the need for standards to be incorporated across federal health care systems, HHS, DOD, and VA recently announced its first set of standards (e.g., HL7, LOINC) for the electronic exchange of health information to be implemented across the federal government. Once federal agencies adopt the recommended standards, they are expected to include the standards in their architectures and to build systems accordingly. This commitment is to apply to all new systems acquisition and development projects. The CHI initiative plans to announce additional standards for federal systems as the working group agrees upon them, but does not have time frames established for making these announcements.

---

### Several Standards Implementation Challenges Remain

Despite progress in defining health care IT standards, several implementation challenges—such as coordination of the various initiatives to achieve consensus on the use of standards, establishment of milestones, and development of implementation mechanisms—remain to be worked out. Currently, there are no activities or mechanisms defined to ensure coordination and consensus between these initiatives at the national level. HHS officials agree that leadership and direction are still needed to coordinate the various standards-setting initiatives and to ensure consistent implementation of standards for health care delivery and public health. Coordination of these initiatives is essential to ensure that the completion of standards development is accelerated and that consensus is obtained from all stakeholders. According to NCVHS, the process of developing health care data standards involves many diverse entities, such as individual and group practices, software developers, domain-specific professional associations, and allied health services. This fragmentation has slowed the dissemination and adoption of standards by making it difficult to convene all of the relevant stakeholders and subject matter experts in standards development meetings and to reach consensus within a reasonable period of time.

Another challenge is that not all of the federal government's standards-setting initiatives have milestones associated with efforts to define and implement standards. For example, while the CHI initiative—the primary federal initiative to establish standards—has announced such initial standards and implementation requirements for health care information exchange, it has not yet established milestones for future announcements. Accordingly, it is not clear when these announcements will occur.

---

Another challenge is that there is no mechanism to monitor the implementation of standards throughout the health care industry. In November 2001, NCVHS reported a need for a mechanism, such as compliance testing, to ensure that health care standards are uniformly adopted as part of a national strategy. NCVHS added that without an implementation mechanism and leadership at the national level, problems associated with systems' incompatibility and lack of interoperability will persist throughout the different levels of government and the private sector and, consequently, throughout the health care sector. Since that time, however, no national monitoring mechanism has yet been established.

A major consequence of not implementing such standards is the promulgation of piecemeal systems, which result in disparate systems that cannot exchange data. This leads to information gaps, hindering the prompt and accurate identification of emerging biological threats—consequently, timely detection of major public health threats is limited. For example, according to CDC officials, one of the IT challenges encountered by public health officials responding to the anthrax events of October 2001 was the issue of exchanging data among the many participants involved in the response—clinical sites, local health departments, emergency responders, state health departments, public health laboratories, and federal agencies. During this event, participants accumulated dissimilar data and principally exchanged it manually.

An underlying challenge for establishing and implementing such standards is that no overall strategy guides IT development and initiatives. With no overall strategy that addresses the development and implementation of standards and associated milestones, federal agencies cannot ensure their systems' abilities to exchange data with other systems when needed and cannot ensure effective preparation for and response to bioterrorism and other public health emergencies.

---

## Emerging Information Technologies Could Enhance Agencies' Abilities to Prepare for and Respond to Public Health Emergencies

Within the public health sector, the implementation of emerging information technologies could help to strengthen agencies' technological capabilities to support the nation's ability to prepare for and respond to bioterrorism and other public health emergencies. Agencies identified several activities to research, develop, and implement emerging technologies, which were generally initiated to meet agencies' specific needs. However, barriers exist that may hinder the public health community from benefiting from the implementation of emerging information technologies.

---

### Examples of Public Health's Use of Emerging Information Technology

An emerging technology is one in which research has progressed far enough to indicate a high probability of technical success for new products and applications that might have substantial markets within approximately 10 years. Agencies identified several IT applications that incorporate the use of emerging technologies. They include commercial IT and communications solutions, along with IT that was developed specifically for the health care sector. Examples of emerging information technologies for use in public health applications include the following:

- **Geographic information system (GIS):**<sup>26</sup> GIS is being used by federal agencies to support disease and outbreak surveillance. CDC uses GIS to track the spread of infection through a community, to identify geographic areas of particular health concern, and to identify susceptible populations. The resulting information can be used in support of surveillance systems to help identify spatial clustering of abnormal events as the data are collected. GIS was used in 2001 to map data related to CDC's emergency response to the anthrax bioterrorism event, and it was used in 2002 to aid the FBI's investigation of the anthrax attack in Florida. FDA is currently using GIS technology in its food safety system, eLEXNET.
- **Web-based images for diagnosis:** Several of CDC's systems use the Internet to enhance reporting and communications capabilities. For

---

<sup>26</sup>GIS is a computer application for capturing, storing, checking, integrating, manipulating, analyzing, and displaying data related to positions on the earth's surface. Typically, a GIS is used for handling maps of one kind or another. These might be represented as several different layers where each layer holds data about a particular kind of feature (e.g., roads). Each feature is linked to a position on the graphical image of a map.

---

example, its DPDx system uses the Internet to strengthen the capabilities of laboratories to diagnose parasitic diseases. The function also enables users to obtain diagnostic assistance over the Internet by allowing laboratories to transmit images to CDC and obtain answers to inquiries, sometimes within minutes. The system increases the interaction between CDC and public health laboratories.

- **Data mining:**<sup>27</sup> DOD's ESSENCE system uses data mining technology to support early detection of infectious disease outbreaks or bioterrorism events. This system enhances public health officials' decision-making capabilities regarding events, which may be public health emergencies.
- **Grid computing:**<sup>28</sup> DOD's Army Medical Research Institute of Infectious Diseases is sponsoring a project with the support of several partner organizations to use grid-computing techniques to help find a treatment for smallpox after infection. The system will run simulated tests of molecules representing some 35 million potential drugs to see how they interact with the smallpox virus.
- **Computer-aided DNA signature development:** DOE's Lawrence Livermore National Laboratory is developing software called KPATH, which is a computer-aided DNA signature development tool. It analyzes pathogen DNA to identify unique signatures. Once identified, these signatures can be used to assist in the process of detecting biological incidents. The results of such development efforts support an enhanced capacity for rapid identification of biological agents.
- **Virtual private network (VPN):** DOE's Los Alamos National Laboratory is working on an Internet-based system called the Forensics Internet Research Exchange, which supports the sharing of biothreat information among research and government agencies. This system is secured through the use of a VPN. A VPN is a communication system that uses public networks to securely transport private intraorganizational and interorganizational information. While industry

---

<sup>27</sup>Data mining is the extraction of information from databases to discover hidden facts. Data mining finds patterns and relationships in data and infers rules that allow the prediction of future results.

<sup>28</sup>Grid computing ties together geographically disparate and distributed computers to create a single massive computing resource, taking advantage of their processing power.

---

use of VPNs is common, only four of the systems included in our inventory use VPNs for public health-specific applications.

- **Public key infrastructure (PKI):** CDC has begun using PKI for secure communications between public health officials using NEDSS. PKI is a system of hardware, software, policies, and people that, when fully implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions.<sup>29</sup>
- **Portable biological detection unit:** DOE's Sandia National Laboratory has made progress toward developing a small sampling and analysis instrument that is portable and does not require a chemist's expertise to operate. This system, μChemLab, is the first that reduces the size of large instruments to the extent that they can be taken into the field and used by first responders, such as firefighters. The device utilizes embedded software algorithms that indicate the level of threat present in the environment in which the instrument is deployed.

---

## Barriers to Better Use of Emerging Technologies

While the public health community may benefit by implementing emerging information technologies, several factors introduce barriers and risks to their successful implementation. One barrier is that emerging technologies likely have not been in use long enough for the developers to identify all areas for standardization, or for the technologies to have evolved to the point that they are interoperable with other already-existing technologies within public health.

Another barrier, according to Gartner, Inc., a leading private research firm, is that the use of emerging information technologies may likely change an organization's existing business model. Therefore their implementation may introduce a significant level of risk. For these reasons, the introduction of an emerging information technology may be disruptive to existing business processes.

A third possible barrier is the lack of a clearly defined mechanism for continuing research and development for emerging technologies once the results are turned over to the public health sector. For example, according

---

<sup>29</sup>U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: February 26, 2001).

---

to a CDC official, there is no mechanism to develop demonstration projects to identify and prove the usefulness and applicability of emerging technologies within the public health sector at the federal, state, and local levels. At the time of our review, funds for two research and development efforts that were initially identified as promising were discontinued without consideration of the project's value to the public health infrastructure.

Lastly, we observed that activities related to the use of emerging technologies are often the result of independent efforts for specific purposes. Consequently agencies may not be able to share successes or lessons learned. Effectively addressing each of these barriers will be essential if the health care industry is to take full advantage of emerging information technologies.

---

## Conclusions

As concerns about the possibility of bioterrorism have been elevated, federal, state, and local public health agencies have been increasing efforts to prepare for and respond to public health emergencies. Federal agencies identified over 70 existing information systems, supporting technologies, and IT initiatives that may better support the public health infrastructure. The extent of coordination or interaction among the lead agency and other related government agencies ranged from a lack of coordination, to awareness, to formal coordination, to jointly developed initiatives. As these and future systems are pursued, leadership will be essential to set priorities for information systems, supporting technologies, and other IT initiatives to enhance the effective preparation for and response to bioterrorism and other public health emergencies.

Although a number of efforts are under way, no comprehensive set of standards has been implemented sufficiently to fully support the public health infrastructure. Leadership and an overall IT strategy are important for ensuring that standards development organizations and federal agencies address remaining implementation challenges: (1) coordination of the various efforts and consensus on the use of standards, (2) establishment of milestones for defining and implementing standards, and (3) mechanisms for monitoring implementation of standards. Without a strategy to ensure coordinated efforts and consistent application of standards, federal agencies cannot ensure that their systems are compatible or interoperable and, therefore, cannot effectively support actions to manage public health emergencies through the timely and accurate exchange of information.

---

Finally, federal agencies have begun to implement emerging technologies to strengthen the public health infrastructure. While some emerging technologies have been implemented, and others are being researched and developed, agencies cannot take full advantage of these technologies because several barriers exist. Effectively addressing each of these barriers will be essential if the health care industry is to fully leverage these emerging information technologies. Leadership will be essential to address these barriers and also to establish mechanisms for identifying and prioritizing uses of emerging technologies to better support the nation's ability to prepare for and respond to public health emergencies.

---

## Recommendations

We recommend that the Secretary of Health and Human Services, in coordination with other key stakeholders—such as the Secretaries of Defense, Homeland Security, and Veterans Affairs—establish a national IT strategy for public health preparedness and response. This IT strategy should identify steps toward improving the nation's ability to use IT in support of the public health infrastructure. More specifically, it should

- identify all federal agencies' IT initiatives, using the results of our inventory as a starting point;
- set priorities for information systems, supporting technologies, and other IT initiatives;
- define activities for ensuring that the various standards-setting organizations coordinate their efforts and reach further consensus on the definition and use of standards;
- establish milestones for defining and implementing all standards;
- create a mechanism—consistent with HIPAA requirements—to monitor the implementation of standards throughout the health care industry; and
- address existing barriers and establish mechanisms for identifying and prioritizing uses of emerging technologies that are appropriate for ensuring continued improvements to the nation's ability to prepare for and respond to public health emergencies.

---

## Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Deputy Assistant Secretary of Defense for Chemical/Biological Defense at DOD, Acting Associate Administrator for Management and Administration at DOE, the Acting Principal Deputy Inspector General at HHS, and the Secretary of Veterans Affairs. These four agencies generally concurred with our results, but they did not comment specifically on the recommendations. They provided technical comments, which we have incorporated in this report as appropriate. USDA and EPA concurred with our results in their oral comments, which were primarily technical comments and incorporated as appropriate. Technical comments were generally limited to additional information or correction of information on the description of their systems included in the appendixes. While DHS was not included as one of the agencies in our review because they did not exist until the end of this engagement, we provided DHS officials with the opportunity to comment on the draft of this report, which they declined. Written comments from DOD, DOE, HHS, and VA are reproduced in appendixes XII to XV.

Among its comments, HHS officials stated that the focus of this report on IT overemphasized its role and does not address other components of the public health infrastructure. As we describe in the background section of the report, IT is a tool that enables personnel to fulfill their mission. We recognize that the United States health care and public health infrastructure is a complex network of people, systems, and organizations, with participation at all levels—federal, state, tribal, local, international, and the private sector. We also recognize that there are other important issues about the public health infrastructure that merit attention, such as workforce capacity and training, capacity of the public health laboratories, variation in state public health laws, capacity of the health care delivery systems, and communication strategies for addressing the public.

---

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date on the report. At that time, we will send copies of the report to other congressional committees. We will also send copies of this report to the Secretaries of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, and Veterans Affairs, and to the Administrator of the Environmental Protection Agency. Copies will also be made available at no charge on our Web site at [www.gao.gov](http://www.gao.gov).

---

If you have any questions on matters discussed in this report, please contact me at (202) 512-9286 or M. Yvonne Sanchez, Assistant Director, at (202) 512-6274. We can also be reached by E-mail at pownerd@gao.gov and sanchezm@gao.gov, respectively. Other contacts and key contributors to this report are listed in appendix XVI.

A handwritten signature in black ink, appearing to read "David A. Powner".

David A. Powner  
Director (Acting), Information Technology  
Management Issues

---

---

*List of Requesters*

**Tom Davis**  
Chairman, Committee on Government Reform,  
House of Representatives

**Christopher Shays**  
Chairman, Subcommittee on National Security, Emerging Threats, and  
International Relations,  
Committee on Government Reform,  
House of Representatives

**Mary Bono**  
Member, House of Representatives

**Jane Harman**  
Member, House of Representatives

**Charles Norwood**  
Member, House of Representatives

**Charles Pickering**  
Member, House of Representatives

**Mac Thornberry**  
Member, House of Representatives

**Edolphus Towns**  
Member, House of Representatives

**Jim Turner**  
Member, House of Representatives

**Edward Whitfield**  
Member, House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

The objectives of our review were to

- compile an inventory of current and planned bioterrorism information technology (IT) initiatives at selected federal agencies and identify the range of coordination efforts,
- identify and describe the development and use of health care IT standards for bioterrorism-related systems, and
- review the potential use of emerging information technologies for bioterrorism preparedness and response.

To address these objectives, we conducted our audit work at six selected federal agencies—United States Department of Agriculture (USDA), Department of Defense (DOD), Department of Energy (DOE), Department of Health and Human Services (HHS), Department of Veterans Affairs (VA), and the Environmental Protection Agency (EPA)—that we previously reported were involved with supporting public health and bioterrorism preparedness and response, which included the use of IT.<sup>1</sup> We excluded federal agencies that are responsible only for law enforcement and consequence management related to other types of terrorism.

To compile the inventory of current and planned IT initiatives related to bioterrorism, we met with agency officials and identified the categories of systems (e.g., detection, surveillance, diagnostic and clinical management, communications, and supporting technologies) to be included in the inventory and the data to be collected about each system. The inventory includes information systems with applications related to both public health and bioterrorism, since most systems were developed for routine public health purposes but are potentially useful during a bioterrorism event. We also created a database for collecting and analyzing the data from the selected agencies. Next we collected and compiled the inventory data and validated the consistency of the data with each agency. We also included systems that were not necessarily designed for public health purposes, but might be adapted for that function. We included other technologies, such as detection devices that include an IT component that facilitates the collection of data for surveillance systems or otherwise

---

<sup>1</sup>U.S. General Accounting Office, *Bioterrorism: Federal Research and Preparedness Activities*, GAO-01-915 (Washington, D.C.: September 28, 2001).

enable IT to perform diagnosis, management, prevention, surveillance, reporting, and communication functions. Our inventory includes information systems that support detection, surveillance, diagnostic and clinical management, communications, and supporting technologies.

The inventory specifically excludes the following types of IT:

- law enforcement and intelligence systems,
- classified systems,
- international initiatives,
- military systems with no applicability to civilian populations (e.g., combat-specific systems),
- distance learning and other training systems,
- disease-specific surveillance systems with no potential to support bioterrorism preparedness and response,
- systems designed to track agricultural terrorism, and
- consequence management systems for traditional first responders (e.g., police and firefighters).

We met with and obtained documentation from representatives of several nonprofit, research, and public health professional organizations, such as the RAND Corporation, the University of California at San Francisco-Stanford Evidence-based Practice Center, and the National Association of County and City Health Officials. Based on our research and the information provided by those parties, we identified categories of IT that support public health and bioterrorism preparedness and response. To illustrate the role of different categories of IT, we also collected more detailed information about selected systems efforts.

During our discussions with agency officials about the results of their inventory data, we asked about an agency's interaction and involvement with information systems and IT initiatives being led by other federal agencies. We also collected data as part of the systems inventory about jointly developed projects that included a partner outside their agency.

To identify and describe the development, use, and progress of health care data, communications, and security standards, we identified ongoing federal efforts and public/private collaborations to implement standards for IT systems that could be used to support the public health infrastructure. In addition, we met with HHS officials to discuss ongoing activities and progress being made to implement the National Committee on Vital and Health Statistics' recommendations on the National Health Information Infrastructure and other standards-related initiatives. We also met with other experts from the Centers for Disease Control and Prevention and Stanford University and discussed with them the use and applicability of health care standards within the public health infrastructure.

To review the potential use of emerging information technologies for bioterrorism preparedness and response, we used research from the Department of Commerce and private-sector consultants to define the term "emerging technologies" as it pertains to information technology. During discussions with agency officials, we asked about their uses and experiences with emerging information technologies, as well as barriers to their implementation. Then, we reviewed the selected agencies' use of and plans for applications specific to public health that were included in the systems inventory.

# Appendix II: CDC Biological Diseases/Agents List

---

According to CDC, the United States public health system and primary health care providers must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. CDC defines three categories of biological diseases or agents based upon the public health impact and the level of risk to the nation's security that the transmission of these agents may introduce. The categories and the associated agents are described below:

**Category A Diseases/Agents:** High-priority agents include organisms that pose a risk to national security because they can be easily disseminated or transmitted from person to person, result in high mortality rates and have the potential for major public health impact, might cause public panic and social disruption, and require special action for public health preparedness.

- Anthrax (*Bacillus anthracis*)
- Botulism (*Clostridium botulinum* toxin)
- Plague (*Yersinia pestis*)
- Smallpox (*Variola major*)
- Tularemia (*Francisella tularensis*)
- Viral hemorrhagic fevers (filoviruses [e.g., Ebola, Marburg] and arenaviruses [e.g., Lassa, Machupo])

**Category B Diseases/Agents:** Second highest priority agents include those that are moderately easy to disseminate, result in moderate morbidity rates and low mortality rates, and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance.

- Brucellosis (*Brucella* species)
- Epsilon toxin of *Clostridium perfringens*
- Food safety threats (e.g., *Salmonella* species, *Escherichia coli* O157:H7, *Shigella*)
- Glanders (*Burkholderia mallei*)

- 
- Melioidosis (*Burkholderia pseudomallei*)
  - Psittacosis (*Chlamydia psittaci*)
  - Q fever (*Coxiella burnetii*)
  - Ricin toxin from *Ricinus communis* (castor beans)
  - Staphylococcal enterotoxin B
  - Typhus fever (*Rickettsia prowazekii*)
  - Viral encephalitis (alphaviruses [e.g., Venezuelan equine encephalitis, eastern equine encephalitis, western equine encephalitis])
  - Water safety threats (e.g., *Vibrio cholerae*, *Cryptosporidium parvum*)

**Category C Diseases/Agents:** Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of availability, ease of production and dissemination, and potential for high morbidity and mortality rates and major health impact.

- Emerging infectious disease threats such as Nipah virus and hantavirus

# Appendix III: Categories of Information Technology for Bioterrorism-Related Systems

---

In addition to the phases of an event (i.e., prevention and preparedness, event recognition, early and sustained response, and recovery) there are corresponding categories of IT, which play a vital role as the event progresses. These categories of IT serve different but related functions. For the purposes of this report, we categorized systems according to their primary purposes, as defined in a technology assessment for the Agency for Healthcare Research and Quality that was completed by the University of California San Francisco-Stanford Evidence-based Practice Center.<sup>1</sup>

## Detection

While not all detectors include IT components, detection systems collect and identify potential biological agents in environmental samples, regardless of whether anyone has been exposed to a harmful level of a contaminant. Components of a detection system can include collection systems, particulate counters or biomass indicators, rapid identification systems, and integrated collection and identification systems. In general, detection systems have three parts: (1) a sampler or collector to concentrate the aerosol and preserve samples for further analysis, (2) a trigger component (often a particulate counter or a biomass indicator) that can identify the presence of a potentially harmful biological agent, and (3) an identifier to provide specific identification of the biological agent.

Biological detection technologies are in a much less mature stage of development than chemical detectors. According to a February 2001 report by the North American Technology and Industrial Base Organization (NATIBO), no single sensor detects or identifies all biological agents of interest.<sup>2</sup> Several different technologies may be needed as components of a layered detection network. It is difficult to distinguish specific biological agents from naturally occurring background materials. Real-time detection and measurement of biological agents in the environment is challenging because of the number of potential agents to be identified, the complex nature of the agents themselves, the countless number of similar micro-organisms that are a constant presence in the environment, and the minute quantities of pathogen that can initiate

---

<sup>1</sup>University of California San Francisco-Stanford Evidence-based Practice Center, *Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems*, (Stanford, CA, June 2002).

<sup>2</sup>North American Technology and Industrial Base Organization, *A Primer on Biological Detection Technologies*, (Fairfax, VA: February 2001).

infection. Most available systems are point detection systems that are either in the field-testing stage or still in the laboratory. The NATIBO assessment also reported that current systems for detecting biological agents are large, complex, expensive, and subject to false results.

The 10 detection systems identified in the inventory include IT components. These systems make use of IT to record and send data to a network. Table 2 shows systems included in the inventory that were developed and operated by DOE and DOD for use in both military and civilian settings.

---

**Table 2: Summary of Detection Systems by Agency**

Type of detector	Agency	Number of systems	Status	Current/proposed monitored populations
Collector	N/A	0	N/A	N/A
Identifier	DOE	1	Pilot	Local and event-specific
Trigger	DOE	1	In development	Not available
Integrated collector, identifier, and trigger	DOE	4	In development	Local, environment, and large-scale civilian events
	DOD	4	2 – Operational 2 – Pilot	Military facilities and personnel

Source: GAO.

Note: N/A means not applicable.

One example of a detection system is the Biological Aerosol Sentry and Information System (BASIS). This is a portable system of networked air sampling units that is capable of detecting airborne biological incidents at large gatherings such as political conventions and major indoor and outdoor sporting events. In the mid-1990s, DOE's national laboratories began work to detect and prevent bioterrorism under the Chemical-Biological National Security Program. As part of that work, Lawrence Livermore and Los Alamos laboratories developed BASIS, which has been used during the Olympics and other events to collect air samples and provide information on the time, duration, amount, and types of biological releases. It uses barcodes to maintain data that link samples to filters taken from specific sampling units. These data are analyzed at field laboratories and tracked with BASIS. If a biological agent is detected, it will provide information about the type of agent as well as where and when it was collected. BASIS also estimates exposure levels and durations

---

to assist public health officials in identifying the population that requires treatment. It was adapted to process samples from the BioWatch program beginning in February 2003.

---

## **Surveillance**

Surveillance is the ongoing collection, analysis, and interpretation of disease-related data to plan, implement, and evaluate public health actions. Surveillance systems differ from detection systems in that they monitor the actual incidence of disease or illness. Without an adequate surveillance system, officials cannot know the true scope of existing health problems and may not recognize new diseases until many people have been affected. The surveillance network relies on the participation of health care providers, laboratories, state and local health departments, and other nontraditional data sources across the nation. Surveillance systems monitor and track abnormal situations that require epidemiological actions and that direct preventive measures by guiding resource allocation and assessing interventions. The most important aspect of a surveillance system is its ability to detect an outbreak at a stage when intervention may affect the expected course of events. It is the public health officials' most important tool for detecting and monitoring both existing and emerging infectious diseases.

Surveillance activities may be either active or passive. Passive surveillance relies on physicians, laboratory and hospital staff, and others to take the initiative in reporting data to health departments. Passive systems may be inadequate to identify a rapidly spreading outbreak in its earliest and most manageable stage because there is a chronic history of underreporting and a time lag between diagnosis of a condition and the health department's receipt of a report. Active surveillance relies on public health officials to take the initiative to periodically contact laboratory officials to gather data. Active surveillance produces more complete information than passive, but is more costly to use for data collection activities.

Timely and reliable data are essential components of public health assessment, policy development, and assurance at all levels of government; however, the current capacity of public health surveillance is weakened by gaps and fragmentation. Fragmentation has developed in surveillance systems in part because states and localities have not developed uniform data collection procedures, storage, and transmission. In February 1999, we reported on gaps in the nation's public health surveillance network for important emerging infectious diseases; and we recommended that CDC, in collaboration with state, local, and other public health officials, reach consensus on the core capabilities needed at

---

each level of government, including IT capabilities.<sup>3</sup> Another key factor shaping the development of surveillance systems is that, historically, investment in these systems has been targeted to specific programs (e.g., tuberculosis, sexually transmitted diseases, etc.), resulting in a patchwork of surveillance efforts across the spectrum of infectious disease threats and other programs.

Most surveillance systems are identified by the type of data they collect; there are eight categories of surveillance:

1. **Foodborne illness surveillance**—systems that collect, process, and disseminate information on foodborne pathogens or illness. In September 2001, we reported weaknesses in several of CDC's surveillance systems for foodborne illness; we reported that these systems had limited usefulness because there were gaps in the data and because CDC did not release the data in a timely manner.<sup>4</sup>
2. **Hospital-based surveillance**—systems that collect data on hospital-acquired infections for hospital infection control officers. Their primary purpose is to track hospital acquired infections, not to identify undiagnosed infections from the community. However, hospital-based surveillance systems could play two roles in the early detection of emerging infections: the identification of a cluster of recently admitted patients, which might suggest a community-based outbreak, and the identification of a cluster of cases within the hospital that may suggest inpatients with an unrecognized communicable disease.
3. **Influenza surveillance**—systems that collect data on influenza-like illness. These systems are relevant to bioterrorism surveillance because many bioterrorism-related illnesses present with flu-like symptoms. Influenza surveillance could also serve as a model because these systems integrate clinical and laboratory data for the detection of influenza outbreaks and are coordinated global efforts; they fulfill needs similar to those of surveillance for bioterrorism.

---

<sup>3</sup>U.S. General Accounting Office, *Emerging Infectious Diseases: Consensus on Needed Laboratory Capacity Could Strengthen Surveillance*, HEHS-99-26 (Washington D.C.: February 5, 1999).

<sup>4</sup>U.S. General Accounting Office, *Food Safety: CDC Is Working to Address Limitations in Several of Its Foodborne Disease Surveillance Systems*, GAO-01-973 (Washington, D.C.: September 7, 2001).

4. **Laboratory and antimicrobial resistance<sup>5</sup> surveillance**—systems that facilitate the collection, analysis, and reporting of notifiable pathogens and of antimicrobial resistance data that could potentially facilitate the rapid detection of a biological agent. Laboratory surveillance systems are an essential component of any system for the detection of a covert bioterrorism event, both for the detection of uncommon organisms (e.g., smallpox, anthrax, and Ebola) and common organisms with unusual patterns of antimicrobial resistance.
5. **Network of clinical reports**—systems that collect and analyze clinical reports from individual clinicians and sentinel networks.<sup>6</sup> The growth of such networks has generated a demand for information systems capable of automating data collection, analysis, reporting, and communication.
6. **Syndromal surveillance**—systems that collect data on the earliest signs and symptoms caused by most biological agents.<sup>7</sup> Therefore, patients with these syndromes are the targets of syndromal surveillance programs. These systems are still considered experimental, and there is no widely accepted definition for any of these syndromes. As a result, syndromal surveillance systems are widely heterogeneous with respect to the syndromes under surveillance and how each syndrome is defined.
7. **Zoonotic and animal disease surveillance**—systems that collect, process, and disseminate information on zoonotic and animal diseases. There are concerns that a bioterrorist attack could involve the dissemination of a zoonotic illness among animal populations with the intention of infecting humans or livestock and causing economic and political/economic chaos. Early detection of such an event requires effective rapid detection systems for use by farm workers, meat inspectors, and veterinarians, with real-time reporting capabilities to public health officials.

---

<sup>5</sup>Antimicrobial resistance is the result of microbes changing in ways that reduce or eliminate the effectiveness of drugs, chemicals, or other agents to cure or prevent infections.

<sup>6</sup>A sentinel network is a disease surveillance program that involves the collection of health data on a routine basis by clinicians with some training in reporting communicable disease.

<sup>7</sup>Symptoms include flu-like illness, acute respiratory distress, gastrointestinal symptoms, febrile hemorrhagic syndromes, and febrile illnesses with either dermatological or neurological findings.

- 
8. **Other**—systems that collect sufficiently different surveillance data that they do not fit into the described categories. These systems could be valuable additions to surveillance networks that integrate data from clinicians, hospitals, and laboratories.

Our inventory identifies 34 surveillance systems, which monitor and track specific categories of illness and disease. Some of CDC's surveillance systems have been used for several years and only consist of a database, while others, such as NEDSS, are more comprehensive. As table 3 indicates, 4 systems are in development, 2 are currently being evaluated as pilots, 1 is being planned, and 27 are operational.

**Table 3: Summary of Surveillance Systems by Agency**

Type of surveillance system	Agency	Number of systems	Status	Current/proposed monitored populations
Foodborne illnesses	HHS	4	Operational	Local populations
	USDA	3	Operational	Slaughter, food processing, retail, and import establishments
Hospital-based surveillance		0		
Influenza	HHS	1	Operational	People with reported cases of influenza-like illness
Laboratory and antimicrobial resistance	HHS	4	Operational	Local and national
	VA	1	Operational	VA hospital population
	USDA	1	Planning	National population
Networks of clinical reports	DOD	1	Operational	Navy enlisted personnel
	HHS	3	2 – Operational 1 – Pilot	Local, national, and international populations
Syndromal	DOD	6	2 – In development 3 – Operational 1 – Pilot	Military personnel and national populations
	DOE	1	Operational	Local, state, and regional populations
	HHS	3	1 – In development 2 – Operational	Individuals crossing US-Mexico border
Zoonotic diseases	USDA	2	Operational	Participating disease control programs or slaughter test subjects
	HHS	1	Operational	National population

Type of surveillance system	Agency	Number of systems	Status	Current/proposed monitored populations
Other	DOE	1	In development	Local populations
	HHS	2	Operational	Local populations

Source: GAO.

One example of a surveillance system is DOD's Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE). ESSENCE was developed to support early identification of infectious disease outbreaks in the military, and to provide epidemiological tools for improved investigation. ESSENCE uses ambulatory data that are collected from its military hospitals and clinics and transmitted daily to a central database. By comparing the daily analyses to historical trends, it can identify patterns that suggest an infectious disease outbreak. ESSENCE uses geo-spatial data<sup>8</sup> to cluster syndromic groupings based on the locations of occurrences. By getting daily reports and automatic alerts, epidemiologists can track, in near real-time, the syndromes that are being reported in a given region. It incorporates privacy algorithms and supports agent-based response using artificial intelligence software, reasoning, data mining, and visualization tools. DOD's use of electronic medical records enhances its ability to quickly collect data for syndromic surveillance. In the future, the department plans to find, analyze, and add new data sources to the system.

---

## Diagnostic and Clinical Management

For the purposes of this report, we defined these as systems with potential utility for enhancing the likelihood that clinicians consider the possibility of bioterrorism-related illness and treat patients accordingly.

Diagnostic systems are generally designed to assist clinicians in developing a differential diagnosis for a patient who has an unusual clinical presentation and consist of three different types: general diagnostic decision support systems (DSS), radiology interpretation systems, and natural language processing techniques.<sup>9</sup> General diagnostic

---

<sup>8</sup>Geo-spatial data is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth. This information may be derived from, among other things, remote sensing, mapping, and surveying technologies.

<sup>9</sup>*Radiology interpretation systems* are those technologies that could be used to automate the interpretation of radiological images. *Natural language processing* is the process of converting information expressed in spoken and written human languages into computer input via specialized software.

---

DSS are those designed to assist clinicians in developing a specific diagnosis for a patient who has unusual signs and symptoms. For these systems to be useful in the event of a covert bioterrorist attack, they should prompt clinicians to consider the possibility of bioterrorism-related illness as a potential cause of the symptoms, thereby increasing the probability that the clinician will perform appropriate diagnostic testing. In addition, since many biothreat agents can cause pulmonary disease, x-rays or other radiological tests would be a common diagnostic procedure performed on patients who might benefit from either the use of radiology interpretation systems that can increase the diagnostic accuracy of radiology reports, or the use of natural language processing techniques to automate the identification of disease concepts in the free text found in diagnostic reports.

Clinical management systems can also make recommendations to clinicians by abstracting clinical information from electronic medical records, applying a set of rules, and generating patient-specific management and prevention recommendations. In general, these systems are limited to institutions with electronic medical records and robust medical informatics programs. There are no known systems specifically designed to provide recommendations to clinicians or public health officials for management of a bioterrorism event. Of the systems that are known to exist, they provide recommendations at the point of care, typically when the clinician enters the electronic medical record of the patient in question.

These diagnostic and clinical management systems are similar in that they both use clinical information about a patient, apply information from a knowledge base, and generate a list of possible diagnoses or a list of management recommendations. Based on this similarity, we have included them in the same category of IT.

Of the federal agencies included in our review that utilize other diagnostic and clinical management systems for their health care delivery operations—DOD, VA, and HHS's Indian Health Services—none has implemented these particular applications as defined above.

---

## Communications

The purpose of communications and reporting systems is to facilitate the secure and timely delivery of information in the midst of a public health emergency to the relevant responders and decision makers, so that appropriate action can be undertaken. During a public health emergency, clinicians must be able to communicate rapidly with their patients; public

---

health officials must be able to communicate with other local, state, and federal officials, and laboratories must be able to communicate diagnostic test results. Robust security measures that ensure patient confidentiality and resist cyber attacks are also a necessary component of any health-related communication system.

Our systems inventory contains 10 communications systems. While communications within the public health community still depend largely on telephone- and paper-based systems, they are moving to Web-based and electronic data transmission. CDC is responsible for many of the communications systems under development in HHS; however, some of the systems are not yet fully implemented at the state or local levels, and this could negatively affect communication of health information to the public. As table 4 shows, all 10 of these systems are operational.

---

**Table 4: Summary of Communications Systems by Agency**

Agency	Number of systems	Targeted users	Status	Frequency of data exchange	Method of data capture and exchange
DOD	2	Navy and Marine medical officials	Operational	1 – Monthly 1 – As needed	Electronic
HHS	5	Public health officials, epidemiologists, and veterinarians	Operational	2 – Continuous 1 – Every 10 minutes 2 – Daily	Predominantly Web-based
USDA	3	USDA officials and state/federal animal health agencies	Operational	3 – Continuous	Web-based, paper, and electronic

Source: GAO.

The Health Alert Network (HAN) is one example of a nationwide communications system that is currently being developed by CDC. HAN is to serve as a platform for (1) distribution of health alerts, (2) dissemination of prevention guidelines and other information, (3) distance learning, (4) national disease surveillance, (5) electronic laboratory reporting, and (6) communication of bioterrorism-related initiatives to strengthen preparedness at the local and state levels. HAN is intended to strengthen the capacity of state and local health departments by serving as an early warning and response system for bioterrorism and other health events. HAN provides the capacity to send urgent health alerts to local agencies via broadcast technologies, such as fax services and autodialing.

HHS has awarded grants to all 50 states, 3 large cities, 3 counties, 8 territories, and the District of Columbia for HAN implementation. When

---

completed, HAN is to provide high-speed, secure Internet connections for local health officials; on-line, Internet- and satellite-based distance learning systems; and early warning broadcast alert systems. HAN currently provides secure Internet access to two-thirds of the nation's counties, and at least 13 states have high-speed Internet access to all of their counties. State and local governments may also use CDC funding to expand HAN to community partners such as health organizations and major hospital networks.

In addition to enhancing state and local communications, at the time of our review, CDC had provided grants to three local centers for public health preparedness. The centers are considered models of integrated communications and information systems across multiple sectors, advanced operational readiness assessment, and comprehensive training and evaluation. New York's Monroe County Center uses its own health alert network to link hospitals, insurers, and county health care agencies to doctors, pharmacies, and clinics for emergency and routine communications. Monroe County also developed a unified platform for the community to view and track the status of their emergency departments and the number of available beds for a specialty unit within a hospital. In addition to working on syndromic surveillance, Colorado's Denver County Center has developed a bi-directional alert communication and notification system for its public health partners and has explored the use of redundant response system tools for rapidly notifying key local public health partners in the event that traditional phone service is lost.

---

## **Supporting Technology**

Supporting technologies are tools or systems that provide information for the other categories of systems (e.g., detection, surveillance, etc.). During our discussions with federal officials, we found that many projects still in applied research and development are intended to support a particular component associated with a type of system, such as detection devices. These projects offer promising techniques that are not currently in use. For example, DOE's national laboratories conduct research into new detection and surveillance techniques that, when developed, may be fully deployed into the public health infrastructure. DOE's Los Alamos National Laboratory (LANL) is conducting the Enabling Analytical and Modeling Tools for Enhanced Disease Surveillance research project. Its objective is to develop analytical tools to support public health officials in quickly identifying emerging threats so they can respond accordingly. Subsets of this research are incorporated into ongoing projects. The Forensics Internet Research Exchange is another LANL research project that is intended to connect a network of laboratories and government agencies

through a secure virtual private network (VPN) so that they can share genetic sequencing data for identifying strains of biological organisms. In addition, the Defense Advanced Research Projects Agency's Bio-ALIRT program is a research project to further enable early detection of biological events from artificial or natural causes. Its objective is to scientifically determine which nontraditional data sources (e.g., human behavior) are useful in enabling early detection of potential biological attacks. More detailed descriptions of these projects are included in appendixes IV through X.

Simulation and computational modeling is another important—and still developing—technology for supporting bioterrorism preparedness and response. With the increase of computational power available in today's technology, and the increasing availability of data, we may soon be able to predict the course of emerging infectious diseases. LANL is piloting the Bioreactor Simulation Tools project, which models and analyzes biological systems in order to create models for predicting the spread of a biological agent. The DOD Chemical and Biological Defense program's Joint Effects Model incorporates simulation tools (used to create a hazard prediction model) that are expected to predict environmental effects. Another DOD project, the Joint Operational Effects Federation, is leveraging existing simulation capabilities to support the prediction of chemical and biological effects at various levels of operation. DOD's simulation tools were developed for military purposes.

Our inventory includes 18 systems that are identified as supporting technologies. Twelve of these systems are operational, 3 are in development and 3 are being evaluated as pilots.

---

**Table 5: Summary of Supporting Technologies by Agency**

Agency	Number of systems	Status
USDA	1	Operational
DOD	1	In development
DOE	6	1 – Operational 2 – In development 3 – Pilot
HHS	5	Operational
EPA	5	Operational

Source: GAO.

---

## Other Clinical Systems

While they are not included within the scope of our systems inventory, there are other systems that will facilitate health care delivery during an act of bioterrorism or other public health emergency. These systems—such as electronic medical records—were excluded from the scope of this review because they are neither public health systems nor were they primarily developed for biodefense. Both DOD and VA have electronic medical information systems (i.e., Composite Health Care System and Veterans Health Information Systems and Technology Architecture), which enhance their ability to automate the collection of surveillance data for systems such as ESSENCE. Automated medical information systems can play an important role for clinicians during their response to a medical emergency, in documenting the treatment of illness and its outcome, and in collecting and sharing diagnostic test results. Electronic medical records can play a role during routine surveillance by serving as important data sources for public health surveillance. The use of electronic medical records could reduce the burdensome and costly use of paper-based processes, facilitating rapid access to data critical for near real-time public health surveillance.

---

# Appendix IV: Department of Agriculture's Systems Inventory

---

USDA became involved in activities concerning bioterrorism because of the increasing realization that the food supply may become a vehicle for a biological attack against the civilian population. Biological attacks on the health of animals and plants are also important to recognize because there are a number of diseases and toxins harmful to humans that can be spread by animals and plants. USDA's Homeland Security staff within the Office of the Secretary is responsible for coordinating activities on terrorism across USDA. In addition, three of USDA's services have been involved in bioterrorism research and preparedness:<sup>1</sup>

- Agricultural Research Service (ARS),
- Animal and Plant Health Inspection Service (APHIS), and
- Food Safety Inspection Service (FSIS).

ARS has conducted research to improve onsite rapid detection of biological agents in animals, plants, and food and has improved its detection capacity for diseases and toxins that could affect animals and humans. APHIS has a role in responding to biological agents that are zoonotic (i.e., capable of affecting both animals and humans). APHIS has veterinary epidemiologists to trace the source of animal exposures to diseases. FSIS provides emergency preparedness for foodborne incidents, including bioterrorism.

USDA identified 10 information systems and supporting technologies.

---

<sup>1</sup>Portions of ARS and APHIS are now part of DHS.

## **Department of Agriculture**

### **Animal and Plant Health Inspection Service**

<b>Emergency Response Management System (EMRS)</b>	<b>Type of system:</b> Surveillance
--	--

EMRS is used to manage and investigate outbreaks of animal diseases in the United States. This Web-based task management system was designed to automate many of the tasks that are routinely associated with disease outbreaks and animal emergencies. EMRS is used for routine reporting of foreign investigations of animal disease, state-specific disease outbreaks or control programs, classic national responses, or natural disasters involving animals. EMRS also has a mapping feature, which allows for real-time identification of outbreaks to enable responders to respond more quickly by providing high-resolution maps to decision makers, government agencies, and the public. The system interfaces with state and federal diagnostic laboratories for reporting test results.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state and federal animal health agencies	<b>FY 2002 IT cost:</b> \$565,000	<b>Est. FY 2003 IT cost:</b> \$615,000
---	-----------------------	--	--------------------------------------	---

**Future plans:** Integrate with U.S. Forest Service's ROSS system.

<b>Generic Disease Data Base (GDB)</b>	<b>Type of system:</b> Surveillance
--	--

GDB monitors progress in disease control programs, such as the brucellosis and tuberculosis programs. GDB is a core national database for animal health information. Each state has its own local GDB that is limited to its own data, unless it has obtained permission from other states to access their GDB data. There is also a national GDB at Ft. Collins, CO, which is used for the National Scrapie program. GDB is used for both domestic disease control programs and foreign animal disease investigations.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state and federal animal health agencies	<b>FY 2002 IT cost:</b> \$550,000	<b>Est. FY 2003 IT cost:</b> \$700,000
---	-----------------------	--	--------------------------------------	---

**Future plans:** Improvements to make GDB more user-friendly to better serve APHIS's needs.

---

## **Food Safety Inspection Service**

---

<b>Automated Import Information System (AIIS)</b>		<b>Type of system:</b> Supporting technology
AIIS assigns reinspection tasks to import inspectors who are stationed at ports of entry. Reinspection of imported goods is based upon foreign product, plant, and country compliance histories. Restrictions on imported products ensure that various species and products do not enter the United States food supply.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by import inspectors at ports of entry and circuit supervisors
<b>Future plans:</b> Subsequent enhancements to AIIS will include an Intranet application for reports and systems administration, a replicated database view to support future reporting requirements, and incorporation of additional business requirements when they are defined. USDA should complete these enhancements by the end of fiscal year 2003.		
<b>Consumer Complaint Monitoring System (CCMS)</b>		<b>Type of system:</b> Surveillance
CCMS is a database used to record, evaluate, and track all consumer complaints reported to the agency. This includes consumer complaints reported by a state or local health departments or other federal agencies. It also includes complaints that involve imported products recalled from the market. Several program areas have access to CCMS and are responsible for entering any consumer complaints that they receive into the system, including those from district offices and compliance officers, as well as the Food Safety Education and Communication staff.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by USDA officials
<b>Future plans:</b> Enhancing CCMS so that it will be able to exchange electronic data with state and local public health agencies in a secure manner using the Internet. This enhancement is expected to decrease the amount of time it takes to identify and respond to possible bioterrorism attacks and to other foodborne outbreaks. Syndromic surveillance capability will be programmed into CCMS for common foodborne illnesses and for possible bioterrorism attacks.		
<b>Fast Antimicrobial Screen Test (FAST)</b>		<b>Type of system:</b> Surveillance
FAST stores information on tested samples and provides information on antimicrobial residues in animal tissues. Test results are used for risk assessment and decision support purposes, early detection of problem products, active food safety surveillance, and evaluation of potential threats to the American food supply.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by USDA officials
<b>Future plans:</b> FAST will be replaced by the implementation of eSample, a system for direct data entry by inspection personnel, and by a corporate database system.		

---

**Appendix IV: Department of Agriculture's  
Systems Inventory**

---

<b>Meat and Poultry Hotline (HOTLINE)</b>	<b>Type of system:</b> Communications
---	--

The purpose of the HOTLINE database is to collect, store, and report data on consumer food safety information requests and complaints. Information for the system is obtained from the consumer via telephone. Administrators of the Consumer Complaint Monitoring System periodically poll the HOTLINE database and extract data about issues of concern.

<b>External collaborating partner:</b> None	System is operational	Used primarily by meat and poultry hotline technical information specialists	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	--	--	---

**Future plans:** The possible integration of a call distribution system with the database. The upgrade could take 5 to 10 years.

<b>Laboratory Electronic Application for Results Notification (LEARN)</b>	<b>Type of system:</b> Communications
---	--

LEARN transmits laboratory test results that detect the presence of pathogens and residues of drugs, pesticides, and other chemicals on specimens taken from meat, poultry, and egg products. The system facilitates and expedites the reporting of food product contamination to agency personnel and the industry, reducing the chances of public consumption. Products are randomly sampled or collected based upon suspected health hazards, and results are reported through the LEARN system.

<b>External collaborating partner:</b> None	System is operational	Used primarily by USDA officials	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> \$92,185
---	-----------------------	----------------------------------	--	--

**Future plans:** Continued enhancements to the existing application to improve user-friendliness and to add information and reports that are not currently included in the application. Plans also include integration of the system with a new laboratory information system and a new headquarters sample information system.

<b>Microbiological and Residue Computer Information System (MARCIS)</b>	<b>Type of system:</b> Surveillance
---	--

MARCIS contains sample identification information and results for analyses submitted by inspection personnel to laboratories. These samples consist of meat, poultry, and egg products; and they are analyzed to ensure that they are safe, wholesome, unadulterated, and properly labeled. The samples are tested because they bear or contain residues of drugs, pesticides, other chemicals, and microbiological pathogens. Test results are used to alert agency personnel and the industry of contaminations and threats to consumer health and the need for protective actions such as product recalls. MARCIS is also used for risk assessment and decision support purposes, improving early detection of problem products, enabling active food safety surveillance, and evaluating potential threats to the food supply.

<b>External collaborating partner:</b> None	System is operational	Used primarily by USDA, FDA, and EPA officials	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	--	--	---

**Future plans:** Replacement of MARCIS with the Laboratory Information Management System. This replacement system will serve an analytical purpose and will populate a corporate sampling database with laboratory information.

---

**Appendix IV: Department of Agriculture's  
Systems Inventory**

---

<b>Pathogen Reduction Enforcement Program (PREP)</b>	<b>Type of system:</b> Communications
--	--

PREP schedules tests, tracks samples, and generates a series of reports concerning testing eligibility and the status of test results. It collects and stores establishment address and product information as well as establishment food safety performance. It uses the information for scheduling and requesting the collection of food samples for microbiological pathogen testing. Test results are used to alert agency personnel and the industry of contaminations and threats to consumer health and the need for protective actions, such as product recalls. PREP is also used for risk assessment and decision support purposes, improving early detection of problem products, enabling active food safety surveillance, and evaluating potential threats to the American food supply.

<b>External collaborating partner:</b> None	System is operational	Used primarily by USDA officials	<b>FY 2002 IT cost:</b> Not Available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	----------------------------------	--	---

**Future plans:** Complete testing of new modules (e.g., eggs, retail, and special surveys).

<b>National Animal Health Laboratory Network (NAHLN)</b>	<b>Type of system:</b> Surveillance
--	--

NAHLN is to link federal and state diagnostic labs for the reporting of cases with certain clinical signs or definite diagnosis. The types of case reported will be coordinated with CDC and include the use of data messaging and transfer standards.

<b>External collaborating partner:</b> HHS/CDC	System is in planning	To be used primarily by diagnostic laboratories, and CDC and USDA officials	<b>FY 2002 IT cost:</b> \$0	<b>Est. FY 2003 IT cost:</b> \$250,000
--	-----------------------	---	--------------------------------	---

**Future plans:** Continue development of the database for 13 laboratories in fiscal year 2003, then further development for other diagnostic laboratories in fiscal years 2004 and 2005.

---

Source: GAO analysis of USDA data.

# Appendix V: Department of Defense's Systems Inventory

Although DOD is primarily responsible for service members in the battlefield, the department often shares its research with other agencies to benefit the civilian population. DOD's Defense Advanced Research Projects Agency has been the central research and development organization for DOD, managing and directing basic and applied research and development projects for the department. In addition, the United States Army Medical Research Institute of Infectious Diseases (USAMRIID) conducts biological research dealing with militarily relevant infectious diseases and biological agents. USAMRIID provides professional expertise on issues related to technologies and other tools to support readiness for a bioterrorist incident, and also confirms diagnostic laboratory results for CDC's Laboratory Response Network. Some of DOD's systems, particularly those developed by the Joint Program Office, are shared between the services.

DOD identified 14 information systems and supporting technologies.

## Department of Defense

### Air Force

<b>Global Expeditionary Medical System (GEMS)</b>	<b>Type of system:</b> Surveillance		
<p>GEMS provides an integrated biohazard surveillance system that is capable of maintaining a global watch over Air Force personnel. It incorporates an electronic medical record as a basis for real-time data analysis. GEMS establishes records of medical encounters and rapid identification and notification of clinical events, and it integrates the symptom level surveillance that is critical for early detection of disease outbreaks and illnesses. With ongoing site and regional data review, population-specific analysis picks up disease trends to provide early warning of disease outbreaks or biological attacks. GEMS serves as the foundation for an Air Force-wide, integrated medical surveillance and command and control network. GEMS has four modules: patient encounter, theater occupational, public health deployed, and theater epidemiology.</p>			
<b>External collaborating partner:</b> None	<b>System is operational</b>  Used primarily by military health care providers, public health, and command and control	<b>FY 2002 IT cost:</b> \$500,000	<b>Est. FY 2003 IT cost:</b> Not available

**Future plans:** Complete infrastructure development.

**Appendix V: Department of Defense's Systems Inventory**

<b>Lightweight Epidemiology Advanced, Detection and Emergency Response System (LEADERS)</b>	<b>Type of system:</b> Surveillance			
LEADERS is expected to improve the ability to identify and confirm covert biological warfare incidents or significant natural disease outbreaks. LEADERS is to be a comprehensive system that supports joint military and civilian medical surveillance initiatives.				
<b>External collaborating partner:</b> None	System is in development	Used primarily by military health care providers, public health, and command and control	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> \$3,000,000

**Future plans:** To complete infrastructure development and to attain funding for clinical interface. The next phase will focus on development of medical surveillance algorithms for specified diseases representing the most serious bioterrorism threats.

**Army**

<b>Airbase/Port Detector System (Portal Shield)</b>	<b>Type of system:</b> Detection			
The Portal Shield sensor system was developed to provide early and definitive warning of biological threats for high-value, fixed-site assets, such as air bases and port facilities. Portal Shield can detect and identify up to eight biological warfare agents simultaneously, within 25 minutes. Portal Shield uses a "smart logic" algorithm to help reduce false positives and consumables. The network can operate in a surveillance mode as well as a random or manual sample mode. In addition to the biological detection hardware, each sensor is equipped with its own meteorological station and global positioning system.				
<b>External collaborating partner:</b> None	System is operational	Used primarily by military personnel at fixed asset sites (e.g., air bases and port facilities)	<b>FY 2002 IT cost:</b> \$150,000	<b>Est. FY 2003 IT cost:</b> \$0

**Future plans:** Not available.

<b>Biological Integrated Detection System (BIDS)</b>	<b>Type of system:</b> Detection			
BIDS provides early warning and identification capability in response to a large area biological warfare attack. It is a detection suite in a shelter that is mounted on a dedicated vehicle with an independent power supply. Other BIDS elements include collective protection, environmental control, and storage for supplies such as a global positioning system and radios. BIDS was designed to utilize multiple biological detection technologies in a layered, complementary manner to maximize detection and presumptive identification capabilities. BIDS is used for warning and for confirming that a biological attack has occurred. It provides presumptive identification of the biological agent being used and produces a sample for laboratory analysis.				
<b>External collaborating partner:</b> None	System is operational	Used primarily by Army reserve and active chemical companies	<b>FY 2002 IT cost:</b> \$425,000	<b>Est. FY 2003 IT cost:</b> \$0

**Future plans:** Replacement by JBPDS in fiscal year 2004 and full automation of real-time detection and identification of the full range of biological agents.

**Appendix V: Department of Defense's Systems Inventory**

<b>Early Warning Outbreak and Response System (EWORS)</b>	<b>Type of system:</b> Surveillance
---	--

EWORS aids in the collection of standardized medical data, particularly for making area-specific and regional comparisons for trend analysis of the data in order to target early warning outbreak recognition of infectious diseases. EWORS provides for timely and accurate dissemination of outbreak information, leading to effective intervention measures, including investigative and containment activities. It establishes baseline measures for trend analysis that is used to differentiate outbreak from non-outbreak disease occurrence; employs a syndromic approach in contrast to disease-specific reporting classifications; and disseminates real-time information and key-function data analysis for instant and programmed interpretation. EWORS integrates public health and hospital networks and was designed as a complementary system for conventional surveillance methodologies.

<b>External collaborating partner:</b> Indonesia's Ministry of Health	System is operational	Used primarily by national outbreak response agencies	<b>FY 2002 IT cost:</b> \$200,000	<b>Est. FY 2003 IT cost:</b> \$300,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** Establishment of the system in the Americas and continued expansion in Southeast Asia.

<b>Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE)</b>	<b>Type of system:</b> Surveillance
---	--

ESSENCE is used in the early detection of infectious disease outbreaks and it provides epidemiological tools for improved investigation. It collects ambulatory data from hospitals and clinics in a central database on a daily basis. Epidemiologists can track—in near real-time—the syndromes being reported in a region through a daily feed of reported data. ESSENCE uses the daily data downloads, along with traditional epidemiological analyses that use historical data for baseline comparisons and more cutting edge analytic methods such as geographic information system. Analysts have implemented an alerting algorithm methodology to detect localized outbreaks and purely temporal methods for low-level, scattered threats. DOD public health professionals use information from ESSENCE to make crucial decisions about potential health emergencies, based on verified and current data.

<b>External collaborating partner:</b> None	System is operational	Used primarily by military health officials	<b>FY 2002 IT cost:</b> \$400,000	<b>Est. FY 2003 IT cost:</b> \$500,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** To improve the interface and find, analyze, and add new data sources. ESSENCE is being upgraded to incorporate the use of nontraditional civilian data sources; it is currently operational in the greater Washington, D.C. area. This expanded capability integrates both military and civilian health data with daily records of pharmacy sales, school absenteeism, and other sources, to allow for early warning of emerging infections.

<b>Embedded Common Technical Architecture (ECTA)</b>	<b>Type of system:</b> Supporting technology
--	---

ECTA will provide military personnel with sensor connectivity, analysis, and warning and reporting capability for Joint Service combat platforms, command and control centers, and fixed sites.

<b>External collaborating partner:</b> None	System is in development	Used primarily by defense nuclear, biological, and chemical specialists	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	--------------------------	---	--	---

**Future plans:** ECTA will merge the current capabilities of the Multipurpose Integrated Chemical Agent Alarm and the JWARN system and provide additional data processing, production of reports, and access to specific data to improve the efficiency of limited personnel assets. It will consist of the hardware and software required to provide sensor connectivity and analysis between detectors and service-specific systems. The JWARN-ECTA will transfer data automatically from and to the actual detector and will provide commanders, units, and systems with analyzed data for disseminating warnings down to the lowest level of the battlefield.

**Appendix V: Department of Defense's Systems Inventory**

<b>Joint Biological Point Detection System (JBPDs)</b>	<b>Type of system:</b> Detection
--	-------------------------------------

JBPDs detects, identifies, samples, collects, and communicates the presence of biological warfare agents in order to enhance the survivability of U.S. forces. It consists of complementary trigger, sampler, detector and identification technologies that allow it to rapidly and automatically detect and identify biological threat agents. Its suite of tools will be capable of identifying biological warfare agents in less than 15 minutes. JBPDs is in low-rate initial production and limited procurement through fiscal year 2006.

<b>External collaborating partner:</b> None	System is operational	Used by military health officials and other service personnel	<b>FY 2002 IT cost:</b> \$489,000	<b>Est. FY 2003 IT cost:</b> \$560,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** JBPDs is scheduled to begin full production in fiscal year 2007. The next stage will focus on reducing size, weight, and power consumption while increasing system reliability. JBPDs will also identify up to 26 agents simultaneously and will interface with JWARN.

<b>Joint Warning and Reporting Network (JWARN)</b>	<b>Type of system:</b> Detection/Communication
--	---

JWARN employs warning technology to collect, analyze, identify, locate, report, and disseminate information related to threats and potentially contaminated areas. It gathers information from detectors and uses this information to compute toxic corridors and attacks and to display near real-time results to onsite commanders. JWARN will be employed in making decisions about warning dissemination down to the lowest level on the battlefield and linked to a global command and control system.

<b>External collaborating partner:</b> Military forces	System is being piloted	Used primarily by defense specialists and other designated personnel located at command and control centers	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
--	-------------------------	---	--	---

**Future plans:** Fielding of JWARN will begin in fiscal year 2004. Plans include using the full JWARN capability to provide commanders with automatic data from sensors and detectors.

## Navy

<b>Epidemiological Interactive System (EPISYS)</b>	<b>Type of system:</b> Surveillance
--	--

EPISYS is a program that enables rapid assessment of disease trends in order to focus research efforts of epidemiologists. It was developed to integrate Navy inpatient hospitalization data with career history and demographic data to form a single system with a flexible interface. It is capable of detecting and flagging diagnostic categories that show rates in excess of their historical threshold values. This surveillance capability allows for the early detection of increased illness rates so that intervention can be started early. Using EPISYS, users can rapidly answer basic epidemiological questions regarding disease and injury rates.

<b>External collaborating partner:</b> None	System is operational	Used primarily by Navy health researchers	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	---	--	---

**Future plans:** Not available.

---

**Appendix V: Department of Defense's Systems Inventory**

---

<b>Epidemiology Wizard (EPIWIZ)</b>		<b>Type of system:</b> Communications
EPIWIZ is a research tool that was developed to organize SAMS data for further analysis of shipboard illness and injury data. EPIWIZ is expected to enhance the Navy's medical readiness by converting SAMS medical encounter data into surveillance information. It will provide Navy medical personnel easy access to shipboard sick-call information so they can monitor trends, prevent injuries and diseases, facilitate reporting, and enhance medical outcomes. EPIWIZ allows the user to display SAMS medical encounter data in a spreadsheet format to facilitate data analysis. This improved data analysis results in closing the gap between medical occurrence and preventative intervention.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by Navy health researchers  <b>FY 2002 IT cost:</b> Not available  <b>Est. FY 2003 IT cost:</b> Not available
<b>Future plans:</b> Not available.		
<b>Field Medical Surveillance System (FMSS)</b>		<b>Type of system:</b> Surveillance
FMSS is designed to help detect emerging health problems that might occur during foreign deployments or conflicts. FMSS can help field staff to determine incidence rates; project short-term trends; profile the characteristics of the affected population by person, time, and place; track the mode of disease transmission; and generate various graphs and reports. Once data are entered for a patient, the input is processed, and compatible diagnoses are presented in order of probability, with biological weapons agents highlighted. FMSS also provides on-line access to medical reference data and an interface to the GIDEON database—a well-known knowledge database designed to help diagnose most of the world's infectious diseases based on the patient's signs, symptoms, and laboratory findings. Many FMSS features have now transitioned over to the Navy's Medical Data Surveillance System and to other development projects.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by military health officials  <b>FY 2002 IT cost:</b> Not available  <b>Est. FY 2003 IT cost:</b> Not available
<b>Future plans:</b> Not available.		
<b>Medical Data Surveillance System (MDSS)</b>		<b>Type of system:</b> Surveillance
MDSS is an interactive Web application for collecting data and identifying changes in rates of naturally occurring injuries and illnesses found within routinely collected clinical data on active duty personnel. It compiles routine reports on disease and non-battle injury rates and generates special reports to assist medical staff to investigate the onset of disease and to evaluate the effectiveness of preventive measures. By applying advanced analytic techniques, MDSS can detect shifts in disease trends and outbreaks with minimal historical information on illness patterns characteristic of the area of interest, thereby making it particularly suitable for theater operations. These techniques also facilitate ad hoc analysis. MDSS is being configured to meet certification requirements so it can be deployed aboard Navy ships. MDSS is being pilot tested in the 18 <sup>th</sup> Medical Command in Korea and in Navy hospitals in Yokosuka, Japan and San Diego, California.		
<b>External collaborating partner:</b> None	System is being piloted	Used primarily by military health officials  <b>FY 2002 IT cost:</b> \$750,000  <b>Est. FY 2003 IT cost:</b> \$1,200,000
<b>Future plans:</b> Continued research and development at an advanced research level and testing in a deployed environment at fixed facilities and operational units.		

---

**Appendix V: Department of Defense's Systems Inventory**

---

<b>Navy Disease Reporting System (NDRS)</b>	<b>Type of system:</b> Communications
NDRS provides for expedient and efficient submissions of reportable events. It may also be used to track and report disease and non-battle injuries. Its main purpose is to improve the compliance, timeliness, and reliability of disease reporting. Functions have been included to assist local command with state reporting, prevention programs, and contract tracing. NDRS enables users to determine what diseases are present in a particular country, how many outbreaks have occurred, and what treatments were used. NDRS streamlines reporting and provides ready access to epidemiological data. NDRS data are used to conduct trend analysis and to pool findings with data from other services.	
<b>External collaborating partner:</b> None	System is operational
	Used primarily by Navy health officials
	<b>FY 2002 IT cost:</b> \$500,000
	<b>Est. FY 2003 IT cost:</b> \$500,000

**Future plans:** Integration into the Navy's database for tracking medical encounters, known as the Shipboard Non-Tactical Automated Data Processing Automated Medical System (SAMS).

---

Source: GAO analysis of DOD data

# Appendix VI: Department of Energy's Systems Inventory

DOE is developing new capabilities to counter chemical and biological threats. DOE expects the results of its research to be public and possibly lead to the development of commercial products in the domestic market. DOE's Chemical and Biological National Security Program has conducted research on biological detection, modeling and prediction, and biological foundations to support efforts in advanced detection, attribution, and medical countermeasures. Several of DOE's national research laboratories (e.g., Lawrence Livermore, Los Alamos, Oak Ridge, and Sandia) have conducted biological and environmental research related to bioterrorism preparedness and response.

DOE identified 14 information systems and supporting technologies.

## Department of Energy

### Lawrence Livermore National Laboratory (LLNL)

Autonomous Pathogen Detection System (APDS)	Type of system: Detection
APDS is an automated, podium-sized system that monitors the air for all three biological threat agents (bacteria, viruses, and toxins). The system has been developed to protect people in critical or high-traffic facilities and at special events. The system performs continuous aerosol collection, sample preparation, and multiplexed biological tests using advanced immunoassays to detect bacteria, viruses, and toxins. More than ten agents are assayed at once. Current research and development work is incorporating polymerase chain-reaction (PCR) techniques for detecting DNA. Single units can be operated to monitor a local space or a central conduit like an air-supply duct. In a more powerful application, a network of APDS units can be integrated with central command and control to protect larger areas. The APDS units can also be networked and integrated with other sensing and analysis systems to provide multifaceted detection and response capabilities.	
External collaborating partner: None	System is in development
	Used primarily for special events of high value and potential fixed targets
	FY 2002 IT cost: Not available
	Est. FY 2003 IT cost: Not available

**Future plans:** APDS will move into redesign and piloting in fiscal year 2004. There will be a significant effort in communications and IT for networked instruments in field-testing and beyond.

---

**Appendix VI: Department of Energy's Systems Inventory**

---

<b>Biological Aerosol Sentry and Information System (BASIS)</b>	<b>Type of system:</b> Detection
---	-------------------------------------

BASIS is a large-area aerosol pathogen detection system. BASIS will provide early detection of biological incidents for special events, such as large assemblies and major sporting events. Planned for civilian use, it will detect a biological incident within a few hours of attack, early enough to allow public health officials to mount an effective medical response. BASIS was developed in close cooperation with federal, state, and local public health agencies to ensure support for real world operational needs. This system was adapted to process samples from the BioWatch<sup>a</sup> program, beginning in February 2003.

<b>External collaborating partner:</b> None	System is operational	Used primarily for special events of high value and potential fixed targets	<b>FY 2002 IT cost:</b> \$800,000	<b>Est. FY 2003 IT cost:</b> \$350,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** BASIS funding ended in fiscal year 2002. The fate of BASIS for fiscal year 2003 was unknown. Given the likelihood of additional armed conflicts, LLNL anticipates seeing BASIS simultaneously deployed at multiple sites, such as cities.

<b>Computational Design of Pathogen Detection Assays (KPATH)</b>	<b>Type of system:</b> Supporting technology
--	---

KPATH is an automated system that analyzes pathogen DNA signatures to build and maintain unique polymerase chain reaction (PCR) detection signatures. Signatures are requested by collaborators and are used in BASIS. DNA signatures developed by KPATH are now in use in the BioWatch program.

<b>External collaborating partner:</b> HHS/CDC and FDA, USDA, and DOD/USAMRIID	System is being piloted	Used primarily by federal agencies (e.g., HHS, USDA, and DOD)	<b>FY 2002 IT cost:</b> \$2,201,200	<b>Est. FY 2003 IT cost:</b> \$1,000,000
--	-------------------------	---	--	---

**Future plans:** KPATH will be LLNL's lead system for PCR diagnostic signature design. LLNL will continue enhancements to KPATH's DNA signature capabilities and will work on its ability to computationally predict protein signatures.

---

<sup>a</sup>BioWatch is a multiagency program that involves air filter sampling to detect agents in certain cities. It is led by the Dept of Homeland Security and is supported by DOE, EPA, and HHS.

## **Los Alamos National Laboratory (LANL)**

<b>Biological Aerosol Sentry and Information System (BASIS)</b>	<b>Type of system:</b> Detection
---	-------------------------------------

See BASIS under Lawrence Livermore National Laboratory.

<b>External collaborating partner:</b> None	System is operational	Used by cities and special events	<b>FY 2002 IT cost:</b> \$3,000,000	<b>Est. FY 2003 IT cost:</b> \$3,000,000
---	-----------------------	-----------------------------------	--	---

**Future plans:** See LLNL.

<b>Bioreactor Simulation Tools</b>	<b>Type of system:</b> Supporting technology
------------------------------------	---

Bioreactor Simulation Tools model and analyze biological systems (i.e., genetic networks, metabolic networks, and signal transduction networks).

<b>External collaborating partner:</b> None	System is being piloted	Used primarily by molecular biologists and epidemiologists	<b>FY 2002 IT cost:</b> \$600,000	<b>Est. FY 2003 IT cost:</b> \$600,000
---	-------------------------	--	--------------------------------------	---

**Future plans:** Development of a forward-looking capability to create detailed models for fundamental processes in molecular biology.

<b>Bio-Surveillance Analysis Feedback Evaluation and Response (B-SAFER)</b>	<b>Type of system:</b> Surveillance
---	--

B-SAFER is a medical surveillance system using data from emergency departments, clinical laboratories, and nontraditional sources (e.g., RN hotline, drug information calls, ambulance services). B-SAFER recognizes an anomaly, either naturally occurring or caused by human intervention. B-SAFER is compliant with HIPAA and NEDSS.

<b>External collaborating partner:</b> DOD	System is in development	Used primarily by the state and local homeland security community	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	--------------------------	---	--	---

**Future plans:** To project potential outcomes of an outbreak and the potential benefit of intervention techniques.

---

**Appendix VI: Department of Energy's Systems Inventory**

---

<b>Flow Cytometry</b>	<b>Type of system:</b> Supporting technology
-----------------------	---

Flow cytometry is used in the detection and identification of pathogens. It is a device comprised of lenses, lasers, computers and other high-tech equipment. They allow researchers to analyze, characterize, and sort thousands of biological cells, chromosomes or molecules in minutes.

<b>External collaborating partner:</b> HHS/NIH	System is being piloted	Used primarily by public health officials, and diagnostic and research laboratory personnel	<b>FY 2002 IT cost:</b> \$300,000	<b>Est. FY 2003 IT cost:</b> \$100,000
--	-------------------------	---	--------------------------------------	---

**Future plans:** Database and data analysis tool development.

<b>OpenEMed</b>	<b>Type of system:</b> Supporting technology
-----------------	---

OpenEMed is a distributed, open architecture, open source system that supports image, audio, and graphical data, creating a virtual patient record. OpenEMed has been used with B-SAFER and New Mexico's NEDSS integrated data repository. OpenEMed includes standard service components for person lookup and identity management, dictionary queries, a clinical data repository, and HIPAA-compliant access control. This software is available for use by the public.

<b>External collaborating partner:</b> HHS	System is operational	Used primarily by public health officials and health care providers	<b>FY 2002 IT cost:</b> \$0	<b>Est. FY 2003 IT cost:</b> \$0
--	-----------------------	---	--------------------------------	-------------------------------------

**Future plans:** Not available.

<b>Reagentless Pathogen Biosensor</b>	<b>Type of system:</b> Detection
---------------------------------------	-------------------------------------

This project will develop a point sensor for the detection of pathogens. This biosensor is being developed for the rapid detection of disease markers to aid in early diagnosis and could also be used for environmental and medical surveillance for homeland security.

<b>External collaborating partner:</b> HHS/NIH, and World Health Organization (WHO)	System is in development	Used primarily by medical personnel and first responders	<b>FY 2002 IT cost:</b> \$2,000,000	<b>Est. FY 2003 IT cost:</b> \$1,800,000
---	--------------------------	--	--	---

**Future plans:** This biosensor is being adapted for early diagnosis of common infectious diseases including respiratory viruses and tuberculosis. There is a proposal pending to adapt it to medical surveillance for the Department of Homeland Security.

---

## Oak Ridge National Laboratory (ORNL)

### LandScan USA

**Type of system:**  
Supporting technology

LandScan USA is expected to be a high-resolution population distribution model that will provide timely and more spatially precise population and demographic information to support geographic analyses anywhere in the United States. In addition to its application for emergency planning in case of an attack or natural disaster, it has potential uses for socioenvironmental studies, including exposure and health risk assessment, and urban sprawl estimates. It can support improved development of emergency response plans in case of an attack or natural disaster, homeland security, environmental justice analyses, exposure/risk assessment, and evaluation of risks. The data it provides includes daytime and nighttime population distribution.

<b>External collaborating partner:</b> DOD, EPA, HHS	System is in development	Used primarily by incident commanders	<b>FY 2002 IT cost:</b> \$600,000	<b>Est. FY 2003 IT cost:</b> \$1,500,000
--	--------------------------	---------------------------------------	--------------------------------------	---

**Future plans:** Not available.

### SensorNet

**Type of system:**  
Detection

SensorNet is expected to be a comprehensive, national system for managing incidents for real-time detection, identification, and assessment of chemical, biological, radiological, and nuclear threats. It is intended to bring together and coordinate all necessary knowledge and response assets quickly and effectively. SensorNet is to consist of sensor technologies, real-time threat assessment, nationwide coverage, and nationwide real-time remote communications. SensorNet is currently under development as a standards-based architecture with encryption and access controls.

<b>External collaborating partner:</b> NOAA	System is in development	Used primarily by first responders and personnel in intelligence, regulatory agencies and transportation	<b>FY 2002 IT cost:</b> \$215,000	<b>Est. FY 2003 IT cost:</b> \$230,000
---	--------------------------	--	--------------------------------------	---

**Future plans:** To continue operational prototypes and refine design for nationwide system.

## Sandia National Laboratory (SNL)

### Enabling Analytical and Modeling Tools for Enhanced Disease Surveillance

**Type of system:**  
Supporting technology

Enabling Analytical and Modeling Tools for Enhanced Disease Surveillance are analytical tools to detect unusual events from a natural background. These tools have been tested with influenza, respiratory illnesses, and dengue fever and are expected to be incorporated into ongoing projects. The flexibility of this project allows for tailoring to specific diseases.

<b>External collaborating partner:</b> None	System is in development	Used primarily by public health officials	<b>FY 2002 IT cost:</b> \$440,000	<b>Est. FY 2003 IT cost:</b> \$0
---	--------------------------	---	--------------------------------------	-------------------------------------

**Future plans:** Provide a distributed software framework for integrating information from disparate sources; develop and integrate analytical tools for earlier detection of disease outbreaks.

---

**Appendix VI: Department of Energy's Systems Inventory**

---

<b>Intelligent Sensing Modules (ISMs)</b>	<b>Type of system:</b> Detection
---	-------------------------------------

ISMs are expected to be an intelligent integration of detection systems supporting wireless ad hoc networking. ISMs are intended to be used in support of DOD's BDI testbed, PROTECT, PROACT, and a project for the Mint.

<b>External collaborating partner:</b> None	System is in development	User information not available	<b>FY 2002 IT cost:</b> \$110,000	<b>Est. FY 2003 IT cost:</b> \$210,000
---	--------------------------	--------------------------------	--------------------------------------	---

**Future plans:** ISMs are currently under development; more capable computational components are to be integrated when available.

<b>µChemLab/CB</b>	<b>Type of system:</b> Detection
--------------------	-------------------------------------

µChemLab is a portable, hand-held chemical analysis system, which is fully self-contained and incorporates "lab on a chip" technologies. It is a sensitive device with fast response times in a low-power, compact package used for monitoring facilities. While µChemLab is currently being developed for chemical detection, it can also be used for biological agent detection. Portable, stand-alone devices for the analysis of chemical agents and protein biotoxins have been developed and tested at the research prototype stage. Current research is focused on improving the performance and expanding the capability of these and other such devices.

<b>External collaborating partner:</b> DOD/JSRG	System is being piloted	Used primarily by first responders	<b>FY 2002 IT cost:</b> \$2,732,000	<b>Est. FY 2003 IT cost:</b> \$3,100,000
---	-------------------------	------------------------------------	--	---

**Future plans:** Analysis of additional agents.

<b>Rapid Syndrome Validation Project (RSVP)</b>	<b>Type of system:</b> Surveillance/Communication
---	--

RSVP is designed to facilitate rapid communications. It provides early warning and response to emerging biological threats, as well as to emerging epidemics and diseases, by providing real-time clinical information about current symptoms, disease prevalence, and geographic location. RSVP provides a mechanism to inform health care providers about health alerts and to facilitate the process of collecting data on reportable diseases. RSVP is designed to overcome existing barriers to reporting suspicious or unusual symptoms in patients, and to capture clinician judgment regarding the severity of an illness and the likely category of the disease. RSVP fully supports on-line data entry, reducing the paperwork associated with reporting infectious diseases. RSVP immediately catalogs all reports in a summary, which is instantaneously available to local public health officials and physicians.

<b>External collaborating partner:</b> None	System is operational	Used primarily by family practice doctors	<b>FY 2002 IT cost:</b> \$403,000	<b>Est. FY 2003 IT cost:</b> \$560,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** Development of neural networks and maps.

Source: GAO analysis of DOE data.

---

# Appendix VII: Department of Health and Human Services' Systems Inventory

---

Within HHS, six agencies work on bioterrorism issues. Combined, these agencies have a budget of \$3.6 billion for bioterrorism in fiscal year 2004. HHS's Office of the Assistant Secretary for Public Health and Emergency Preparedness will have \$42 million in fiscal year 2004 to direct and coordinate the implementation of HHS's bioterrorism programs and to support the Department of Homeland Security by providing health and medical leadership. CDC's bioterrorism budget for fiscal year 2004 will be \$1.1 billion, \$940 million of which will fund CDC's ongoing state and local preparedness program, which supports state surveillance and epidemiology capacity, laboratory capacity, communication and IT infrastructure, education and training, and health information dissemination. In addition, CDC has its own office, the Office of Terrorism Preparedness and Response, to coordinate efforts. CDC plans to upgrade its own system and laboratory capacity and to expand oversight of inter-laboratory transfers of dangerous pathogens and toxins, laboratory safety inspections, and anthrax research. The Health Resources Services Administration also provides grants to hospitals for bioterrorism preparedness and response.

The Agency for Healthcare Research and Quality funded research on the use of information systems and decision support systems to enhance preparedness for the delivery of medical care in the event of a bioterrorist attack. FDA is increasing its food safety responsibilities by improving its laboratory preparedness and food monitoring and inspections in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The National Institutes of Health is planning to implement its strategic plan for biodefense research and research agenda for CDC Category A, B, and C agents.

HHS identified 28 information systems and supporting technologies.

## **Department of Health and Human Services**

### **Centers for Disease Control and Prevention**

#### **122 Cities Mortality Reporting System**

**Type of system:**  
Surveillance

As part of CDC's national influenza surveillance effort, CDC receives weekly mortality reports from 122 cities and metropolitan areas in the United States within 2-3 weeks from the date of death. These reports summarize the total number of deaths occurring in these cities/areas each week due to pneumonia and influenza. This system provides CDC with preliminary information with which to evaluate the impact of influenza on mortality in the United States and the severity of the currently circulating virus strains. The advantage of this system is that it provides timely data 2-3 years before finalized mortality data are available from CDC's National Center for Health Statistics. Deaths are reported to CDC by place of occurrence, not by residence. This system is part of BioWatch.

<b>External collaborating partner:</b> 122 Cities' Registrars	System is operational	Used primarily by epidemiologists	<b>FY 2002 IT cost:</b> \$49,070	<b>Est. FY 2003 IT cost:</b> \$61,202
---	-----------------------	-----------------------------------	-------------------------------------	--

**Future plans:** Not available.

#### **Active Bacterial Core Surveillance (ABCs)**

**Type of system:**  
Surveillance

As part of CDC's Emerging Infections Program, ABCs determines the incidence and epidemiological characteristics of invasive bacterial disease due to pathogens of public health importance, determines the molecular patterns and microbiological characteristics of disease-causing elements, and provides an infrastructure for nested special studies to identify risk factors and to evaluate prevention policies. ABCs is a population- and laboratory-based surveillance system.

<b>External collaborating partner:</b> None	System is operational	Used primarily by epidemiologists	<b>FY 2002 IT cost:</b> \$78,641	<b>Est. FY 2003 IT cost:</b> \$87,372
---	-----------------------	-----------------------------------	-------------------------------------	--

**Future plans:** Measuring the impact of newly licensed vaccines on disease and drug resistance and harnessing molecular techniques to characterize bacteria.

#### **Bioterrorism Event Notification**

**Type of system:**  
Communications

The Bioterrorism Event Notification system tracks emergency-related phone calls to CDC's Emergency Preparedness and Response Branch, which maintains the 24-by-7 emergency contact numbers for CDC. The system provides a data set that can be used to quantify the number and types of incoming requests for emergency assistance.

<b>External collaborating partner:</b> None	System is operational	Used primarily by CDC officials	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	---------------------------------	--	---

**Future plans:** Not available.

**Appendix VII: Department of Health and Human Services' Systems Inventory**

<b>Border Infectious Disease Surveillance Project (BIDS)</b>	<b>Type of system:</b> Surveillance
--	--

BIDS helps public health officials to better understand and detect important infectious diseases along the U.S.-Mexico border. The system conducts active, sentinel surveillance for syndromes consistent with hepatitis and febrile-rash illness at clinical facilities on both sides of the border. As an infectious disease surveillance system combining syndromal surveillance with appropriate laboratory diagnostic testing, BIDS can directly enhance bioterrorism surveillance in this key region.

<b>External collaborating partner:</b> Mexico Ministry of Health	System is operational	Used primarily by state and local public health epidemiologists at the U.S.-Mexico border	<b>FY 2002 IT cost:</b> \$30,000	<b>Est. FY 2003 IT cost:</b> \$35,000
--	-----------------------	---	-------------------------------------	--

**Future plans:** Expansion of the number of sites and syndromes and complete development of the next BIDS software version, involving Web-based data entry, which will be consistent with the National Notifiable Disease Surveillance System standards.

<b>CaliciNet</b>	<b>Type of system:</b> Surveillance
------------------	--

CaliciNet is used to assist public health officials to more quickly identify contaminated food products associated with outbreaks by allowing for the linking of epidemiological and laboratory information from specimens that are collected as part of outbreak investigations for viral gastroenteritis. While caliciviruses are not on the CDC list of bioterrorism agents, they could be used in an attack.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state public health officials	<b>FY 2002 IT cost:</b> \$57,783	<b>Est. FY 2003 IT cost:</b> \$6,586
--	-----------------------	---	-------------------------------------	---

**Future plans:** CaliciNet will be replaced by a larger system, which is still in the process of being named.

<b>DPDx</b>	<b>Type of system:</b> Supporting technology
-------------	---

DPDx uses the Internet to strengthen the level of laboratory professionals' expertise in diagnosing foodborne and other parasitic diseases. DPDx offers reference and training and diagnostic assistance. Laboratory professionals can transmit images to CDC and obtain answers to their inquiries in minutes to hours. This allows them to more efficiently address difficult diagnostic cases in normal or outbreak situations and to disseminate information more rapidly. In addition, this method substantially increases the interaction between CDC and public health laboratories.

<b>External collaborating partner:</b> None	System is operational	Used primarily by pathologists, laboratory technicians, and other health care workers	<b>FY 2002 IT cost:</b> \$7,000	<b>Est. FY 2003 IT cost:</b> \$7,000
--	-----------------------	---	------------------------------------	---

**Future plans:** Training and continuing education of laboratory professionals; provision to health facilities worldwide of diagnostic assistance by CDC staff supported, when needed, by experts from other institutions; diagnostic quizzes to assess the skills of laboratory professionals; and informal, early detection of unusually clustered, atypical, or emerging parasitic diseases. Plans also include ensuring communication and functionality with all state public health departments.

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Early Aberration Reporting System (EARS)</b>	<b>Type of system:</b> Communications
---	--

EARS is a SAS-based, Web-enabled reporting tool that allows the analysis of public health surveillance data using aberration detection methods. Its goal is to assist public health officials in the early identification of disease outbreaks, as well as bioterrorism events. It assesses whether the current number of reported cases of an event is higher than usual. EARS provides results from its aberration detection analysis, as well as quick data summaries and graphs.

<b>External collaborating partner:</b> None	System is operational	Used primarily by public health officials	<b>FY 2002 IT cost:</b> \$88,000	<b>Est. FY 2003 IT cost:</b> \$240,000
--	-----------------------	---	-------------------------------------	---

**Future plans:** Incorporating bioterrorism detection methods in future versions. Plans also include the implementation of a GIS system that will allow for maps of syndromic or disease events and the incorporation of additional methodologies.

<b>Electronic Foodborne Outbreak Reporting System (EFORS)</b>	<b>Type of system:</b> Surveillance
---	--

EFORS replaces the Foodborne Disease Outbreak Surveillance System. EFORS enables a Web-based application for states to report foodborne outbreaks electronically rather than on the former paper-based system. Data are then used for annual summary reports and monitoring for multi-state outbreaks.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state and county public health officials	<b>FY 2002 IT cost:</b> \$156,157	<b>Est. FY 2003 IT cost:</b> \$126,949
--	-----------------------	--	--------------------------------------	---

**Future plans:** Improving the database structure to allow immediate viewing of reports as changes occur. EFORS intends to provide data for estimates of the burden of foodborne illness by food commodity.

<b>Epidemic Information Exchange (Epi-X)</b>	<b>Type of system:</b> Communications
--	--

Epi-X connects state and local public health officials so that they can share information about outbreaks and other acute health events, including those possibly related to bioterrorism. It is intended to provide epidemiologists and others with a secure, Web-based platform that can be used for instant emergency notification of outbreaks and requests for CDC assistance. Epi-X provides tools for searching, tracking, discussing, and reporting on diseases. EPI-X is being used in DHS's BioWatch program.

<b>External collaborating partner:</b> None	System is operational	Used primarily by epidemiologists, veterinarians, and other relevant health professionals	<b>FY 2002 IT cost:</b> \$1,354,828	<b>Est. FY 2003 IT cost:</b> \$1,382,199
--	-----------------------	---	--	---

**Future plans:** Increasing its user base to ensure rapid, secure communications at all levels of public health, such as linking to CDC's Emergency Operations Center and to state and local public health departments. Plans also include linking with comparable state level systems, providing secure communication for multistate outbreak response teams, and automating the recognition of disease outbreaks across jurisdictions.

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Federal Facilities Information Management System (FFIMS)</b>	<b>Type of system:</b> Supporting technology
---	---

FFIMS aids in collecting, managing, and analyzing data that originate outside the agency. Its primary use is as an investigative system to aid in public health assessments at specific sites. It has been most useful in the collection and analysis of voluminous environmental sampling data. FFIMS can be used to investigate an anomaly after it has been identified and to help determine the source of health outcomes or the potential risk of adverse health outcomes.

<b>External collaborating partner:</b> None	System is operational	Used primarily by CDC epidemiologists	<b>FY 2002 IT cost:</b> \$1,004,986	<b>Est. FY 2003 IT cost:</b> \$1,129,483
---	-----------------------	---------------------------------------	--	---

**Future plans:** Addition of remote data collection and conversion to a Web-based application.

<b>Foodborne Disease Active Surveillance Network (FoodNet)</b>	<b>Type of system:</b> Surveillance
--	--

As part of CDC's Emerging Infections Program, FoodNet provides a network for responding to new and emerging foodborne diseases of national importance, monitoring the burden of foodborne diseases, and identifying the sources of specific foodborne diseases. It consists of active surveillance and a related epidemiological study, which helps public health officials better understand the epidemiology of foodborne diseases in the United States.

<b>External collaborating partner:</b> USDA and HHS/FDA	System is operational	Used primarily by epidemiologists and public health officials	<b>FY 2002 IT cost:</b> \$475,500	<b>Est. FY 2003 IT cost:</b> \$515,900
---	-----------------------	---	--------------------------------------	---

**Future plans:** Estimate the burden of foodborne illnesses in the United States, follow trends in the incidence of foodborne infectious disease, and attribute foodborne infections to specific food vehicles.

<b>Geographic Information Systems (GIS)</b>	<b>Type of system:</b> Supporting technology
---	---

GIS tracks the spread of environmental contamination through a community, identifies geographic areas of particular health concern, and identifies susceptible populations. Among other things, GIS can be used to help identify spatial clustering of abnormal events as the data is collected. This can assist under emergency conditions by identifying affected areas, predicting dispersion of the agent, and sharing information with personnel who are responsible for incident management.

<b>External collaborating partner:</b> None	System is operational	Used primarily by CDC officials	<b>FY 2002 IT cost:</b> \$2,105,977	<b>Est. FY 2003 IT cost:</b> \$2,091,737
---	-----------------------	---------------------------------	--	---

**Future plans:** Expansion of GIS services (e.g., for field-based use), integration with the Hazardous Substances Emergency Event System, and possible integration with CDC's NEDSS.

---

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Global Emerging Infections Sentinel Network (GeoSentinel)</b>	<b>Type of system:</b> Surveillance
--	--

GeoSentinel is a Web- and provider-based sentinel network. It consists of travel/tropical medicine clinics around the world participating in surveillance to monitor geographic and temporal trends in morbidity among travelers and other globally mobile populations. Passive surveillance and response capabilities are also extended to a broader network of GeoSentinel Network members.

<b>External collaborating partner:</b> International Society of Travel Medicine	System is operational	Used primarily by physicians in travel/tropical medicine clinics	<b>FY 2002 IT cost:</b> \$59,282	<b>Est. FY 2003 IT cost:</b> \$10,000
---	-----------------------	--	-------------------------------------	--

**Future plans:** Increasing the number and geography of involved clinics, expanding partnerships, and enhancing electronic infrastructure to include simultaneous conferencing in real time with all global sites in preparation for global disease outbreaks or bioterrorism threats.

<b>Hazardous Substances Emergency Event System (HSEES)</b>	<b>Type of system:</b> Surveillance
--	--

HSEES collects and analyzes information on events involving hazardous substances as well as threatened releases that result in a public health action. Information about the chemical, victims, and event is recorded by state health departments and transmitted to CDC in near real time for analysis and dissemination of reports. It can be easily enhanced to collect biological agents in addition to chemical agents.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state public health officials	<b>FY 2002 IT cost:</b> \$528,954	<b>Est. FY 2003 IT cost:</b> \$580,866
---	-----------------------	---	--------------------------------------	---

**Future plans:** Inclusion of additional state health departments and integration with GIS.

<b>Health Alert Network (HAN)</b>	<b>Type of system:</b> Communications
-----------------------------------	--

HAN is a nationwide system serving as a platform for the distribution of health alerts, dissemination of prevention guidelines and other information, distance learning, national disease surveillance, and electronic laboratory reporting, as well as for CDC's bioterrorism and related initiatives to strengthen preparedness at the local and state levels. Among other things, HAN is to provide early warning alerts and to ensure capacity to securely transmit surveillance, laboratory, and other sensitive data.

<b>External collaborating partner:</b> Local, state, and territorial public health agencies	System is operational	Used primarily by state public health officials	<b>FY 2002 IT cost:</b> \$624,000	<b>Est. FY 2003 IT cost:</b> \$624,000
---	-----------------------	---	--------------------------------------	---

**Future plans:** Not available.

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Influenza Sentinel Provider Surveillance System</b>	<b>Type of system:</b> Surveillance
--	--

The Influenza Sentinel Provider Surveillance System is one of four separate components that allows CDC to, among other things, detect changes in influenza and monitor influenza-like illness. It is accessible through the Internet and provides data on the circulation and impact of influenza year-round. It also provides information on new influenza strains in circulation that can be used to determine the components of the vaccine for the next influenza season and as a pandemic warning.

<b>External collaborating partner:</b> None	System is operational	Used primarily by CDC officials, physicians, state public health officials and WHO	<b>FY 2002 IT cost:</b> \$52,623	<b>Est. FY 2003 IT cost:</b> \$54,063
---	-----------------------	--	-------------------------------------	--

**Future plans:** Not available.

<b>Laboratory Information Tracking System (LITS Plus™)</b>	<b>Type of system:</b> Supporting technology
--	---

LITS Plus™ is a laboratory data management system, which is used to enter, edit, analyze, and report laboratory test results electronically. Users can examine all the data about a specimen, including data from all laboratories that performed tests on the specimen. It provides seamless integration of laboratory data, including laboratory instrument data and incorporates extensive laboratory data management functionality.

<b>External collaborating partner:</b> DOD and Global AIDS Program (Africa)	System is operational	Used primarily by public health, CDC, DOD, and Global AIDS officials	<b>FY 2002 IT cost:</b> \$1,769,098	<b>Est. FY 2003 IT cost:</b> \$1,831,522
---	-----------------------	--	--	---

**Future plans:** Develop and implement standardized modules in LITS Plus™ for all CDC Category A bioterrorism labs and to comply with CDC's Public Health Information Network.

<b>Laboratory Response Network (LRN)</b>	<b>Type of system:</b> Communications
--	--

LRN is an integrated network of public health and clinical laboratories that provide laboratory diagnostics and disseminated testing capacity for public health preparedness and response. It ensures that all member laboratories collectively maintain state-of-the-art biodetection and diagnostic capabilities as well as surge capacity for all biological and chemical agents likely to be used by terrorists. LRN is based on the use of standard protocols and reagents, integrated data management, and secure communications.

<b>External collaborating partner:</b> DOD, FDA, FBI, and Association of Public Health Labs	System is operational	Used primarily by state and local public health officials	<b>FY 2002 IT cost:</b> \$385,000	<b>Est. FY 2003 IT cost:</b> \$502,500
---	-----------------------	---	--------------------------------------	---

**Future plans:** Update and revise laboratory protocols for biological and chemical agents on the LRN Web site; develop new screening assays for biological agents and obtain FDA approval for in vitro diagnostic use of new rapid screening assays; link to NEDSS; expand domestic partnership; and upgrade restricted Web site for interoperability and data exchange with key clinical entities.

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>National Botulism Surveillance</b>		<b>Type of system:</b> Surveillance
The National Botulism Surveillance system compiles information on cases of foodborne and wound botulism. CDC provides clinical, epidemiological, and laboratory consultation for suspected botulism cases 24 hours a day and is the only source for antitoxin in the United States. Also, CDC conducts a yearly survey of state and territorial epidemiologists and of state public health laboratory directors to identify additional cases that have not been previously reported.		
<b>External collaborating partner:</b> None	System is operational	Used primarily by clinicians, laboratory professionals, and epidemiologists
		<b>FY 2002 IT cost:</b> \$2,000
		<b>Est. FY 2003 IT cost:</b> \$2,000
<b>Future plans:</b> Use electronic near real-time reporting of botulism testing results, which will be integrated with reports of clinical consultations and antitoxin releases for suspect cases and for rapid case updates.		
<b>National Electronic Disease Surveillance System (NEDSS) Base System</b>		<b>Type of system:</b> Surveillance
The NEDSS base system is a component of CDC's overall NEDSS initiative. It will provide a NEDSS architecture-compliant option for states to use as a platform for disease surveillance. The NEDSS base system is a CDC-developed system that provides a platform upon which many public health surveillance systems, processes, and data can be integrated in a secure environment. It will provide the foundation for state and program area needs, data collection, and processing, including the development of modules that can be used for data entry and for management of core demographic and notifiable disease data via a Web browser. The first release supports the electronic processes involved in notifiable disease surveillance and analysis, replacing the functionality currently supported by the NETSS system. States also have the option to develop systems or elements on their own through the use of grants provided for this purpose rather than using the NEDSS base system.		
<b>External collaborating partner:</b> State, local, and territorial public health agencies, and various public health-related professional associations <sup>a</sup>	System is currently being piloted	Used primarily by state and local public health officials and CDC officials
		<b>FY 2002 IT cost:</b> Not available
		<b>Est. FY 2003 IT cost:</b> \$27,609,000
<b>Future plans:</b> Additional functionality to support other programs, such as chronic disease and environmental health programs, for use by epidemiologists, laboratory personnel, and data managers from various program areas.		

---

<sup>a</sup>Professional associations' involvement includes the Association of State and Territorial Health Officials (ASTHO), the Association of Public Health Laboratories (APHL), the Council of State and Territorial Epidemiologists (CSTE), the National Association of Health Data Organizations (NAHDO), the National Association of County and City Health Officials (NACCHO), and the National Association for Public Health Statistics and Information Systems (NAPHSIS).

**Appendix VII: Department of Health and Human Services' Systems Inventory**

<b>National Electronic Telecommunications Systems for Surveillance (NETSS)</b>	<b>Type of system:</b> Surveillance
NETSS provides weekly data regarding cases of nationally notifiable diseases. It serves a supportive role for bioterrorism-related surveillance allowing the transmission of limited epidemiological information describing cases of infectious disease that may or may not be related to bioterrorism. As needed, local and state health departments can use well-established, routine NETSS information exchange protocols to augment more focused or specific bioterrorism surveillance data exchange.	
<b>External collaborating partner:</b> State, local, and territorial public health agencies, and various public health-related professional associations <sup>a</sup>	System is operational  Used primarily by state public health officials, CDC officials, and health care providers
<b>FY 2002 IT cost:</b> \$586,301 (includes the cost for the National Notifiable Disease Surveillance System)	
<b>Est. FY 2003 IT cost:</b> \$620,929 (includes the estimated cost for the National Notifiable Disease Surveillance System)	
<b>Future plans:</b> NETSS will be phased out as NEDSS is deployed and implemented.	
<b>National Molecular Subtyping Network for Foodborne Disease Surveillance (PulseNet)</b>	<b>Type of system:</b> Supporting technology
PulseNet is an early warning system for outbreaks of foodborne diseases. It is a national network of public health laboratories that perform DNA "fingerprinting" on foodborne bacteria. It permits rapid comparisons of these fingerprint patterns through an electronic database and provides critical data for the early recognition and timely investigation of outbreaks.	
<b>External collaborating partner:</b> USDA/FSIS, HHS/FDA, Health Canada	System is operational  Used primarily by public health officials and food regulatory agency officials
<b>FY 2002 IT cost:</b> \$221,400	
<b>Est. FY 2003 IT cost:</b> \$235,000	
<b>Future plans:</b> Expansion to include additional pathogens (including those that may be used by bioterrorists) and to facilitate the establishment of compatible networks in Europe, the Pacific Rim region, and Latin America.	
<b>National Respiratory and Enteric Virus Surveillance System (NREVSS)</b>	<b>Type of system:</b> Surveillance/Communications
NREVSS is a laboratory-based system that monitors temporal and geographic patterns associated with the detection of respiratory syncytial viruses (RSV), human parainfluenza viruses (HPIV), respiratory and enteric adenoviruses, and rotaviruses. Influenza specimen information, also reported to NREVSS, is integrated with CDC influenza surveillance. While these agents are not on the CDC list, they could be potentially used for bioterrorism. NREVSS is a Web-based and telephone dial-in system.	
<b>External collaborating partner:</b> None	System is operational  Used primarily by state public health officials and professionals
<b>FY 2002 IT cost:</b> \$61,835	
<b>Est. FY 2003 IT cost:</b> \$2,685	
<b>Future plans:</b> Replace the telephone dial-in functionality to be Web-based once all users have access capabilities.	

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Plague</b>	<b>Type of system:</b> Surveillance
---------------	--

The plague surveillance system is comprised of clinical, epidemiological, and ecologic information on presumptive and confirmed cases reported by state public health departments. Basic descriptive statistical analyses are performed on these data, such as regional- and county-specific incidence rates. Plague is also one of three internationally quarantinable diseases, and, according to the International Health Regulations, all cases must be investigated and reported to the World Health Organization in Geneva.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state and local public health officials and Indian Health Services' officials	<b>FY 2002 IT cost:</b> \$2,350	<b>Est. FY 2003 IT cost:</b> \$2,350
---	-----------------------	---	------------------------------------	---

**Future plans:** Integrate with CDC's bioterrorism preparedness programs.

<b>Public Health Laboratory Information System (PHLIS)</b>	<b>Type of system:</b> Surveillance
--	--

PHLIS is designed for use in public health laboratories for the reporting and analysis of a variety of conditions of public health importance, which have a significant laboratory-testing component, e.g., salmonella. PHLIS reports standard demographic data that are associated with a laboratory isolate as well as laboratory test results, information about laboratory procedures, and outbreak-related information.

<b>External collaborating partner:</b> None	System is operational	Used primarily by state public health officials	<b>FY 2002 IT cost:</b> \$149,091	<b>Est. FY 2003 IT cost:</b> \$154,160
---	-----------------------	---	--------------------------------------	---

**Future plans:** Not available.

<b>Statistical Outbreak Detection Algorithm (SODA)</b>	<b>Type of system:</b> Surveillance
--	--

SODA processes pathogen information (i.e., salmonella, shigella, and e. coli) on a daily basis to detect anomalies or unusual clusters in the reported versus expected counts at the state, regional, and national levels. Its main goal is to provide users with an interface to view reports, generate graphs and produce maps from the state, regional, and national perspectives. SODA utilizes a cumulative sums algorithm commonly used in the manufacturing industry. The output is a statistical measure that is flagged for review by CDC's foodborne staff. SODA uses general information from lab specimen data, such as date and location.

<b>External collaborating partner:</b> None	System is operational	Used primarily by epidemiologists	<b>FY 2002 IT cost:</b> \$112,350	<b>Est. FY 2003 IT cost:</b> \$116,169
---	-----------------------	-----------------------------------	--------------------------------------	---

**Future plans:** Addition of other pathogens for monitoring.

---

**Appendix VII: Department of Health and Human Services' Systems Inventory**

---

<b>Unexplained Deaths and Critical Illnesses Surveillance System</b>	<b>Type of system:</b> Surveillance
--	--

As part of CDC's Emerging Infections Program, the Unexplained Deaths and Critical Illnesses Surveillance System is expected to contain limited epidemiological and clinical information on previously healthy persons aged 1 to 49 years who have illnesses with possible infectious causes. It is also expected to provide active population-based surveillance through coroners and medical examiners at limited sites. National and international surveillance will be passive for clusters of unexplained deaths and illnesses.

<b>External collaborating partner:</b> None	System is in development	Used primarily by epidemiologists	<b>FY 2002 IT cost:</b> \$28,980	<b>Est. FY 2003 IT cost:</b> \$37,290
---	--------------------------	-----------------------------------	-------------------------------------	--

**Future plans:** Further development of an integrated data management system for clinical, epidemiological, specimen tracking, and test results data, including novel diagnostics and pathogen discovery.

---

**Food and Drug Administration**

---

<b>Electronic Laboratory Exchange Network (eLEXNET)</b>	<b>Type of system:</b> Surveillance
---	--

eLEXNET provides a Web-based system for real-time sharing of food safety laboratory data among federal, state, and local agencies. It is seamless and secure, allowing public health officials at multiple government agencies engaged in food safety activities to compare and coordinate laboratory analysis findings. It captures food safety sample and test result data from participating laboratories and uses them for risk assessment and decision-support purposes, improving early detection of problem products and enabling active food safety surveillance and evaluation of potential threats to the American food supply.

<b>External collaborating partner:</b> USDA; DOD	System is operational	Used primarily by public health and agricultural food safety officials	<b>FY 2002 IT cost:</b> \$5,096,000	<b>Est. FY 2003 IT cost:</b> \$3,750,000
--	-----------------------	--	--	---

**Future plans:** Expanding participating food safety laboratory partnerships and developing an integrated short- and long-term strategic plan and communications planning approach.

---

Source: GAO analysis of HHS data.

# Appendix VIII: Department of Veterans Affairs' Systems Inventory

VA manages one of the nation's largest health care systems and is the nation's largest drug purchaser. The department purchases pharmaceuticals and medical supplies for the Strategic National Stockpile Program and the National Medical Response Team stockpiles.

VA identified one information system.

## Department of Veterans Affairs

<b>Emerging Pathogens Initiative (EPI)</b>	<b>Type of system:</b> Surveillance			
EPI identifies antibiotic-resistant and otherwise problematic pathogens within the Veterans Health Administration facilities. This information is used to help formulate plans on a national level for intervention strategies and resource needs. Results of aggregate data may also be shared with appropriate public health authorities for planning on the national level for the non-VA and private health care sectors. EPI provides general surveillance on specific pathogens and diseases.				
<b>External collaborating partner:</b> None	System is operational	Used primarily by VA medical staff	<b>FY 2002 IT cost:</b> Not available	<b>Est FY 2003 IT Cost</b> Not available

**Future plans:** Addition of new diseases or organisms as they are identified.

Source: GAO analysis of VA data.

# Appendix IX: Environmental Protection Agency's Systems Inventory

EPA has responsibilities to prepare for and respond to emergencies, including those related to biological materials. EPA can be involved in detection of agents by environmental monitoring and sampling. EPA is responsible for protecting the nation's water supply from terrorist attack and for prevention and control of indoor air pollution. EPA's National Homeland Security Research Center is in the process of preparing an on-line virtual library of homeland security-related documents and tools intended to assist decision making during emergency situations. Data in the library will include exposure guidelines, databases, publications, and Web sites applicable to biological, chemical, and radiological threats.

EPA identified five supporting technologies.

## Environmental Protection Agency

### Indoor Air Quality and Inhalation Exposure (IAQX)

Type of system:  
Supporting technology

IAQX is an indoor air quality simulation package that consists of a general-purpose simulation program and a series of stand-alone, special purpose programs. Relatively simple mass transfer models are provided by the general-purpose simulation program, and more complex models are implemented by the stand-alone, special purpose simulation programs. In addition to performing conventional indoor air quality simulations, which calculate the pollutant concentration and personal exposure as a function of time, IAQX can estimate the adequate ventilation rate when certain air quality criteria need to be satisfied. This feature is useful for product stewardship and risk management.

External collaborating partner: None	System is operational	Used primarily by advanced users—EPA officials and the public	FY 2002 IT cost: Not available	Est. FY 2003 IT cost: Not available
--------------------------------------	-----------------------	---	--------------------------------	-------------------------------------

**Future plans:** Addition of more special purpose programs, such as models for indoor air chemistry and indoor application of pesticides.

---

**Appendix IX: Environmental Protection  
Agency's Systems Inventory**

---

<b>EPANET</b>	<b>Type of system:</b> Supporting technology
---------------	---

EPANET was developed to help water utilities maintain and improve the quality of water delivered to consumers through their distribution systems. It is a computer modeling software package that can be used to simulate drinking water distribution systems and to simulate water flow patterns in those systems. The model is also used to simulate contaminant dispersion patterns if chemical or biological contaminants are introduced into a water system. It can be used to inform water utilities where critical points (valves, pumps, etc.) are located in the system and what the impact of the system would be if those points were attacked.

<b>External collaborating partner:</b> None	System is operational	Used by EPA officials and the public	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not available
---	-----------------------	--------------------------------------	--	---

**Future plans:** Not available.

<b>RISK</b>	<b>Type of system:</b> Supporting technology
-------------	---

RISK is an indoor air quality model developed by the Indoor Environment Management Branch of EPA's National Risk Management Research Laboratory. It was developed as a tool to carry out the mission of the engineering portion of the EPA's indoor air research program to provide tools necessary to reduce individual exposure to and risk from indoor air pollutants. RISK uses the concepts of buildings and scenarios, including fixed information about a building (the number of rooms, the room dimensions, and the arrangement of the rooms) and changing information sources (sinks, air exchange, room-to-room flows, etc.). The model provides risk, exposure, and concentration information. RISK allows analysis of the impact of multiple pollutants on the indoor environment.

<b>External collaborating partner:</b> None	System is operational	Used primarily by EPA officials and the general public	<b>FY 2002 IT cost:</b> Not available	<b>Est. FY 2003 IT cost:</b> Not Available
---	-----------------------	--	--	---

**Future plans:** Addition of more risk calculations and of models and suggested values for indoor particulate.

<b>Safe Drinking Water Accession and Review System (SDWARS)</b>	<b>Type of system:</b> Supporting technology
---	---

SDWARS tracks monitoring results for specific lists of unregulated chemical contaminants to indicate occurrences in public drinking water systems. Public water systems submit Unregulated Contaminant Monitoring Rule (UMCR) data elements through SDWARS for inclusion in the National Drinking Water Contaminant Occurrence Database. SDWARS is a one-entry approach to the electronic reporting process to improve reporting quality, reduce reporting errors, and reduce the time involved in investigating and correcting errors at all levels (e.g., laboratories, states, and EPA).

<b>External collaborating partner:</b> None	System is operational	Used primarily by EPA officials and the general public	<b>FY 2002 IT cost:</b> \$350,000	<b>Est. FY 2003 IT cost:</b> \$300,000
---	-----------------------	--	--------------------------------------	---

**Future plans:** Accommodate additional contaminants, including microbial contaminants.

---

**Appendix IX: Environmental Protection  
Agency's Systems Inventory**

---

<b>Safe Drinking Water Information System Federal (SDWIS/FED)</b>	<b>Type of system:</b> Supporting technology
---	---

SDWIS/FED is a database designed and implemented by EPA to meet its needs in the oversight and management of the Safe Drinking Water Act. It contains public water system inventory information and summary violation data submitted by states and EPA regions in conformance with reporting requirements established by statute, regulation, and guidance.

<b>External collaborating partner:</b> None	System is operational	Used primarily by EPA officials	<b>FY 2002 IT cost:</b> \$2,100,000	<b>Est. FY 2003 IT cost:</b> \$1,700,000
---	-----------------------	---------------------------------	--	---

**Future plans:** Replace with a new drinking water data warehouse.

---

Source: GAO analysis of EPA data.

# Appendix X: Federal Agencies' Information Technology Initiatives

In addition to the agencies' individual systems that they identified, there are several other IT initiatives in process or being planned to better support agencies' abilities to prepare for, respond to, and communicate during public health emergency events. These projects are intended to provide integration and interoperability among systems, improve communications, and better support the public health infrastructure.

Information technology initiatives	Lead agency	Collaborating agencies	Status of development
<b>Public Health Information Network (PHIN)</b>	HHS/CDC	State, territorial, and local public health agencies and various public health-related professional associations <sup>a</sup>	Planning

The PHIN is an effort initiated by the CDC to provide interoperability across public health functions and organizations, such as state and federal agencies, local health departments, public health labs, vaccine clinics, clinical care, and first responders. It is intended to, among other things, (1) deliver industry standard data to public health, (2) investigate bioterrorism detection, (3) provide disease tracking analysis and response, and (4) support local, state, and national data needs. It builds on existing CDC investments from HAN, NEDSS, EPI-X, LRN, and the CDC Web. The PHIN will not replace any of these systems but will provide an "umbrella" to support the interoperability of existing CDC surveillance, communications, and reporting systems.

<b>National Electronic Disease Surveillance System (NEDSS) Architecture</b>	HHS/CDC	State, territorial, and local public health agencies and various public health-related professional associations <sup>a</sup>	Development
---	---------	---	-------------

In fiscal year 2001, CDC implemented the NEDSS architecture project to replace or enhance the interoperability of its numerous existing surveillance systems. NEDSS promotes the use of data and information standards to advance the development of efficient, integrated, and interoperable surveillance systems at the federal, state, and local levels. When completed, NEDSS will electronically integrate a wide variety of surveillance activities and will facilitate more accurate and timely reporting of disease information to CDC and state and local health departments. NEDSS is also designed to reduce provider burden in the provision of information and enhance both the timeliness and quality of information provided. The NEDSS architecture will include (1) data standards, (2) an Internet-based communications infrastructure built on industry standards, and (3) policy-level agreements on data access, sharing, burden reduction, and protection of confidentiality.

<sup>a</sup>Professional associations' involvement includes the Association of State and Territorial Health Officials (ASTHO), the Association of Public Health Laboratories (APHL), the Council of State and Territorial Epidemiologists (CSTE), the National Association of Health Data Organizations (NAHDO), the National Association of County and City Health Officials (NACCHO), and the National Association for Public Health Statistics and Information Systems (NAPHSIS).

---

**Appendix X: Federal Agencies' Information  
Technology Initiatives**

<b>Information technology initiatives</b>	<b>Lead agency</b>	<b>Collaborating agencies</b>	<b>Status of development</b>
<b>National Environmental Public Health Tracking Network (NEPHTN)</b>	HHS/CDC	EPA	Planning

The NEPHTN is a collaborative effort between CDC and EPA to develop a national environmental tracking network that will (1) be standards-based; (2) allow direct electronic data reporting and linkage within and across health effect, exposure, and hazard data; and (3) be interoperable with other public health systems. Environmental public health tracking is the ongoing collection, integration, analysis, and interpretation of data about: environmental hazards, exposure to environmental hazards, and health effects potentially related to exposure to environmental hazards. The goal of environmental public health tracking is to protect communities by providing information to federal, state, and local agencies. These agencies then use this information to plan, apply, and evaluate public health actions to prevent and control environmentally related diseases. Currently, no systems exist at the state or national levels to track many of the exposures and health effects that may be related to environmental hazards.

<b>FSIS Automated Corporate Technology Suite (FACTS)</b>	USDA/FSIS	None	Planning
--	-----------	------	----------

The FACTS initiative establishes an agencywide, integrated information management and data-sharing resource. It is intended to replace existing stovepipe application systems with a suite of components that can interact with each other and share data. FACTS is a technology suite composed of a centralized database that will (1) unite several smaller databases and projects that are interrelated and (2) provide a central point of access that will decrease data redundancy and inaccuracy. FACTS' main purpose is to support the FSIS mission by substantially improving the ability to provide information that is accurate, complete, and timely for use by agency decision makers. Although this initiative will not consolidate all food safety information systems into one system, it will allow interoperability between systems in USDA agencies and at the U.S. Customs Service. In addition, FSIS and APHIS will take major steps toward establishing an integrated data-sharing effort that will specifically define the roles of each agency and will better safeguard the United States against foreign animal diseases and food safety hazards.

<b>Biological Defense Initiative (BDI)</b>	DOD/DTRA	DOE	Cancelled
--	----------	-----	-----------

DTRA was executing the BDI program to determine the value of integrating systems with each other. This program was intended to deliver a national model for biological incidents detection capabilities and to integrate and synthesize information from exiting detectors and surveillance systems, such as BASIS, Portal Shield, RSVP, ESSENSE, and B-Safer. The intended partners in the BDI were to be CDC, Veterans Health Administration, NIH, USDA, and Interior's Fish and Wildlife Service. However, the scope of the project was drastically narrowed as a result of funding reductions—from \$215 million dollars to \$29 million dollars. BDI has recently been cancelled.

<b>Epidemic Outbreak Surveillance (EOS)</b>	DOD/Air Force	Navy, Army, DTRA, and civilian and academic partners	Development
---	---------------	--	-------------

EOS is a DTRA-supported initiative that leverages and tests existing and emerging biodefense technologies within a real-world testbed. The objectives of the EOS project are to (1) develop a scalable biodefense system for early threat warning, rapid threat identification, focused disease treatment, and outbreak containment and (2) enable the use of emerging technologies for testing, verification, and validation in a real-world, testbed environment. EOS is currently used to identify epidemics of infectious respiratory disease among USAF basic military trainees. It is the first diagnostic platform using DNA-based microarray technologies to be tested, verified, and validated.

---

**Appendix X: Federal Agencies' Information  
Technology Initiatives**

<b>Information technology initiatives</b>	<b>Lead agency</b>	<b>Collaborating agencies</b>	<b>Status of development</b>
<b>Bio-ALIRT</b>	DOD/DARPA	Walter Reed Army Institute for Research, academic and commercial partners	Development

Bio-ALIRT is being developed by DARPA to scientifically determine the value of nontraditional data sources, such as human behavior, to enable the detection of a biological outbreak from artificial or natural causes up to two days earlier than with traditional means. The Bio-ALIRT program will continue to monitor nontraditional data sources, such as animal sentinels, behavioral indicators, and prediagnostic medical data, to determine which could effectively serve as early indicators of a biological pathogen release. Data sources and algorithms will be evaluated in testbeds. The knowledge and technology developed from the testbeds would be suitable for use in any syndromic surveillance system. Future plans for Bio-ALIRT include development of new techniques, such as advanced data fusion, detection, and privacy protection algorithms, to differentiate between naturally occurring and deliberate bio-releases.

<b>Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT)</b>	DOE/SNL	None	Development
---	---------	------	-------------

PROTECT's objective is to protect people in public facilities, such as subways and airports, from chemical attacks. It is intended to address vulnerabilities of civilians that were highlighted in the 1995 chemical agent attack in the Tokyo subway system. PROTECT rapidly detects the presence of a chemical agent and transmit readings to an emergency management information system. It demonstrates the use of integrated systems for the defense of infrastructure facilities. PROTECT does not currently have a bioagent use; however, it can provide a near-term solution for 24-by-7 facility monitoring for airborne biological agent releases. PROTECT is a DOE Domestic Demonstration and Application Program (i.e., a prototype system to address specific problems in order to improve infrastructure facility protection). The program takes advantage of recent advances in technology to prepare for and respond to attacks in subways, airports, and office buildings where people are concentrated. PROTECT is jointly funded by DOE and the Department of Justice.

<b>National Food Safety Laboratory System (NFSLS)</b>	USDA/FSIS and HHS/FDA	USDA/APHIS, DOD/Army, selected state food laboratories	Development
---	-----------------------	--	-------------

The NFSLS is a newly initiated project to integrate systems for sharing information. It is currently a pilot program involving federal food laboratories at FSIS, FDA, the Army, and state food laboratories in Tennessee, Florida, New Hampshire, Massachusetts, and municipal food laboratories in Milwaukee, Wisconsin, and Cincinnati, Ohio. The program will also focus on the assurance of rapid sharing of reliable data through FDA's e-LEXNET system. USDA and HHS will collaborate with federal, state, and local agencies to: (1) provide a national seamless data exchange system for food laboratory information; (2) provide an infrastructure that is portable, intuitive, and ready to exchange data from state, local, and federal databases and varying internal network designs; (3) enhance communication and collaboration among food safety partnerships; (4) provide the ability to detect, compare, and communicate current findings in food laboratory analysis; and (5) demonstrate that multiple agencies engaged in food safety regulatory activities could leverage the resources necessary to achieve the common goal of reducing the incidence of microbial foodborne illness.

---

**Appendix X: Federal Agencies' Information  
Technology Initiatives**

<b>Information technology initiatives</b>	<b>Lead agency</b>	<b>Collaborating agencies</b>	<b>Status of development</b>
<b>National Infrastructure Project</b>	HHS/CDC	None	Development

The purpose of the National Infrastructure Project is to strengthen CDC's infrastructure and network management in order to help ensure continuity of operations for the NCEH during emergencies. Its objectives are to achieve zero latency on all network operations and to provide redundancy and higher network uptime. The center is implementing cluster technology to help achieve redundancy without latency, thus increasing the reliability of the network. Storage area networks are being used to provide logical and physical disk drives with connected servers. Other commercial tools are used to monitor the network and detect problems before they occur. NCEH is also purchasing UPS paging to allow early detection of problems within the facility. For example, pagers will go off whenever water sensors or smoke detectors are activated. NCEH has a triage plan, which includes the use of E-mails, pagers, and phone calls combined with paging systems.

<b>Forensics Internet Research Exchange (FIRE)</b>	DOE/LANL	None	Development
--	----------	------	-------------

FIRE is an initiative to develop an internet-based research exchange system for laboratories and government agencies. It is intended to allow the sharing of biothreat information over a secure VPN. It is anticipated that the system will be able to tie identified bioagent strains to particular organizations based upon previous identification of strains and their origins.

<b>Molecular Recognition-based Real Time Detection</b>	DOE/LANL	None	Planning
--	----------	------	----------

The Molecular Recognition-based Real Time Detection initiative is intended to develop new sensors for biological and chemical warfare agents. The work may provide more specific and sensitive sensors, having very low or no false positives that can be used to collect samples and provide data to information systems. Future plans include the development of single receptors for multiple bioagents or for a combination of biological and chemical agents.

---

Source: GAO analysis of agency data.

# Appendix XI: List of Selected Health Care Standards

Several organizations have defined standards for health care data and communications. Several important standards development initiatives and the vocabulary and messaging standards that they have defined are described below:

Standard	Description
Health Level Seven (HL7)	HL7 is an ANSI-accredited standards development organization that creates message format standards. Version 2.3 provides a protocol that enables the flow of data between systems. Version 3.0 is being developed through the use of a formalized methodology involving the creation of a Reference Information Model to encompass the ability, not only to move data, but to use data once it is moved.
Logical Observations Identifiers Names and Codes (LOINC)	LOINC is a set of code standards that identifies clinical questions, variables, and reports. It comprises a database of 15,000 variables with synonyms and cross-mappings; it covers a wide range of laboratory and clinical subject areas. The formal structure has six parts: component, property measured, time aspect, system, precision, and method.
Systemized Nomenclature of Medicine (SNOMED)	SNOMED is a nomenclature classification for indexing medical vocabulary, including signs, symptoms, diagnoses, and procedures; it defines code standards in a variety of clinical areas called coding axes. It can identify procedures and possible answers to clinical questions that are coded through LOINC.
Unified Medical Language System (UMLS)	The National Library of Medicine developed UMLS as a standard health vocabulary that enables cross-referencing to other terminology and classification systems and includes a metathesaurus, a semantic network, and an information sources map. Its purpose is to help health professionals and researchers retrieve and integrate electronic biomedical information from a variety of sources, irrespective of the variations in the way similar concepts are expressed in different sources and classification systems.
Common Information for Public Health Electronic Reporting (CIPHER)	CIPHER's objective is to establish standards for the data used in surveillance, to allow for a consistent definition and a consistent implementation across programs. The following objectives have been defined for CIPHER: (1) establish consistent definitions for information collected and used by surveillance systems; (2) define standards for how questions are to be formatted and information is to be collected on surveillance case report forms; (3) identify standards for the processing of data in electronic data entry systems, including value/label displays, reference table look-ups, and a minimum level of edit-checking; (4) identify storage standards; (5) provide guidance on electronic data interchange; and (6) provide guidance on coding for the display of data in statistical analyses and reports.

Source: GAO.

# Appendix XII: Comments from the Department of Defense



ASSISTANT TO THE SECRETARY OF DEFENSE  
3050 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3050

MAY 19 2003

NUCLEAR AND CHEMICAL  
AND BIOLOGICAL DEFENSE  
PROGRAMS

Mr. David A. Powner  
Director (Acting)  
Information Technology Management Issues  
U.S. General Accounting Office  
Washington, D.C. 20548

Dear Mr. Powner:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, GAO-03-139, "BIOTERRORISM: Information Technology Strategy Could Strengthen Federal Agencies' Ability to Respond to Public Health Emergencies," dated April 21, 2003, (GAO Code 310432).

The DoD provides the enclosed comments for accuracy and clarification.

We appreciate the opportunity to review and respond to the subject draft audit report. Should you have any questions regarding this response, please contact COL Steve Lawrence at (703) 697-1797.

Sincerely,

Anna Johnson-Wineger, Ph.D.  
Deputy for Chemical/Biological Defense

Enclosure:  
As stated

# Appendix XIII: Comments from the Department of Energy



**Department of Energy**  
National Nuclear Security Administration  
Washington, DC 20585

May 13, 2003

Mr. David A. Powner  
Acting Director  
Information Technology Issues  
U. S. General Accounting Office  
Washington, D.C. 20548

Dear. Mr. Powner:

The National Nuclear Security Administration (NNSA) has reviewed the draft report, *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Ability to Respond to Public Health Emergencies* (GAO-03-139). While there are no recommendations to the Department of Energy or the NNSA, we offer the following comments:

- Simply inventorying the IT systems without a more detailed description of their capabilities could obscure some of the gaps or needs in the overall infrastructure. With more information, it is possible for agencies to focus scarce resources into those areas of greatest need.
- We believe that the Autonomous Pathogen Detection System (APDS), developed by the Lawrence Livermore National Laboratory, should be added to the inventory either in Appendix VI or Appendix X
- Additionally, if it is germane to the report, NNSA, and the Department as a whole, have BioWatch and BioShield involvement.

NNSA, on behalf of the Department of Energy, appreciates GAO's efforts and our opportunity to have reviewed this draft report.

Sincerely,

Michael C. Kane  
Acting Associate Administrator  
for Management and Administration



Printed with soy ink on recycled paper

# Appendix XIV: Comments from the Department of Health and Human Services

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

 DEPARTMENT OF HEALTH & HUMAN SERVICES  
Office of Inspector General  
Washington, D.C. 20201

MAY 15 2003

Mr. David A. Powner  
Director (Acting), Information Technology  
Management Issues  
United States General  
Accounting Office  
Washington, D.C. 20548

Dear Mr. Powner:

Enclosed are the department's comments on your draft report entitled, "Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies." The comments represent the tentative position of the department and are subject to reevaluation when the final version of this report is received.

The department provided several technical comments directly to your staff.

The department appreciates the opportunity to comment on this draft report before its publication.

Sincerely,

  
Dennis J. Dequette  
Acting Principal Deputy Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the department's response to this draft report in our capacity as the department's designated focal point and coordinator for General Accounting Office reports. The OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

**Comments of the Department of Health and Human Services on the General Accounting Office's Draft Report, "Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies" (GAO-03-139)**

The Department of Health and Human Services (department) appreciates the opportunity to comment on the General Accounting Office's (GAO) draft report and strongly agrees that the use of emerging information technology (IT) to support the public health infrastructure could help to improve federal agencies' abilities to prepare for and respond to public health emergencies.

**GAO Recommendation for Executive Action**

The GAO recommends that the Secretary of Health and Human Services, in coordination with the Secretary of Homeland Security, establish a national IT strategy for public health preparedness and response. This IT strategy should identify steps towards improving the nation's ability to use IT in support of the public health infrastructure. More specifically, it should:

- Identify all federal agencies' IT initiatives, using the results of our inventory as a starting point;
- Set priorities for information systems, supporting technologies, and other IT initiatives;
- Define activities for ensuring that the various standards-setting organizations coordinate their efforts and reach consensus on the definition and use of standards;
- Establish milestones for defining and implementing standards;
- Create a mechanism to monitor the implementation of standards throughout the health care industry; and
- Address existing barriers and establish mechanisms for identifying and prioritizing uses of emerging technologies that are appropriate for ensuring continued improvements to the nation's ability to prepare for and respond to public health emergencies.

**Department Response**

The department agrees that improvements in public health emergency preparedness and response capability, including bioterrorism related threats, will require progress on health information technology and standards and the National Health Information Infrastructure broadly. We offer the following general comments:

1. In general, the report would benefit from a clearer distinction between federal agency responsibilities, activities and authorities and those of the private health care sector and the public health system. The draft report and its recommendations tend to blur these activities as well as minimize the scope and complexity of the situation. Surveillance and public health in the United States are primarily state functions. Good progress is being made toward ensuring that

See comment 1.

See comment 2.

surveillance systems are compatible among the Centers for Disease Control and Prevention (CDC), local and state health departments in addition to health care providers. As a result of the Consolidated Health Informatics (CHI) initiative and several prior initiatives, agencies in the federal health care enterprise have agreed on national consensus health data standards to promote interoperability within the federal health care enterprise. Adoption of interoperability standards among federal health agencies is a major step forward and is expected to be an industry “tipping point.” However, the widespread adoption of those standards in the private sector health care and the public health system generally tends to be a much more complex and difficult goal, because the federal government has little influence in most areas.

2. While we agree that more coordination across federal agencies would be helpful, the report does not adequately recognize the level of interagency coordination and success that is already underway, particularly regarding the CHI initiative and the adoption of health data interoperability standards. Instead of describing the CHI initiative as a promising model for coordination that has been successful, the report tends to minimize the CHI effort and contribution in both interagency coordination and major progress on health data interoperability standards. For example, the CDC’s National Electronic Disease Surveillance System (NEDSS) and the CDC and Health Resources and Services Administration (HRSA) cooperative agreements described above all include CHI data standards.
3. Coordinated by the Office of the Assistant Secretary for Public Health Emergency Preparedness, the FY 2003 CDC and HRSA cooperative agreements for public health and hospital preparedness for bioterrorism both place emphasis on information technology (IT) interoperability and laboratory data standards, and both incorporate the same health information technology guidance to the states.
4. Emphasizing the importance of standards for data, for security, and for electronic transport has been a main theme of the CDC NEDSS activities and, more recently, for the broader Public Health Information Network (PHIN). The report, however, does not appear to recognize CDC’s plans for PHIN.

See comment 3.

See comment 4.

See comment 5.

See comment 6.

However, what the report categorizes as IT systems includes core activities of CDC’s National Center for Infectious Disease (NCID) programs, of which IT is a part, but not the essence. The CDC made an effort to communicate this distinction to the team doing this investigation, but does not believe it is reflected in the report. For example, FoodNet is included in the analysis. A CDC-state collaborative scientific activity, FoodNet conducts surveillance for food borne diseases. It involves CDC program personnel and personnel infrastructure in 10 states. The IT is needed to exchange the data and this effort will be enhanced as implementation of NEDSS/PHIN evolves. The IT is needed to help support the FoodNet effort, but FoodNet is not an IT system. There are other examples. Failing to understand this distinction could lead to an overemphasis of the role of

---

**Appendix XIV: Comments from the  
Department of Health and Human Services**

IT in public health surveillance, create unreasonable expectations for IT improvements, and result in potentially simplistic suggestions and solutions.

The following are GAO's comments on the Department of Health and Human Service's letter dated May 15, 2003.

1. In the background section of the report, we discuss the state and local government roles in dealing with public health emergencies, using a graphic to further illustrate the different roles. In this section, we have attempted to make a clear distinction between federal responsibilities and the responsibilities of other entities involved in responding to the release of a biological agent.
2. As we stated in our report, the Consolidated Health Informatics Initiative is an interagency work group lead by HHS, which recently announced the first set of standards. While we are encouraged by the interagency coordination involved in this initiative, additional work is still needed—in defining activities for ensuring further coordination and consensus on the adoption and use of additional standards, in establishing milestones for defining and implementing all standards, and in creating a mechanism to monitor the implementation of these standards throughout the health care industry. We recognize that the adoption of standards is an issue for the entire health care industry.
3. In response to these comments, we have added information on HHS's cooperative agreements with states and local governments to the background section of the report.
4. We have included information we received about PHIN in appendix X.
5. We agree with HHS that IT is one of several components that support the core activities of public health surveillance; we discussed this in the Agency Comments and Our Evaluation section of the report.
6. While FoodNet may be a collaborative scientific activity for surveillance of foodborne diseases, it also includes an IT component for data exchange, which was reported to us by CDC officials.

# Appendix XV: Comments from the Department of Veterans Affairs



THE SECRETARY OF VETERANS AFFAIRS

WASHINGTON

May 12, 2003

Mr. David A. Powner  
Director (Acting)  
Information Technology Issues  
U.S. General Accounting Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Powner:

The Department of Veterans Affairs (VA) has reviewed your draft report, *BIOTERRORISM: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies* (GAO 03-139). VA agrees with your overall assessment that information technology can more effectively facilitate emergency response if standards are developed and implemented that allow systems to be interoperable.

VA continues to partner actively with other Federal agencies, particularly the Department of Defense (DoD) and the Centers for Disease Control and Prevention (CDC), in information technology homeland security efforts. In conjunction with those two lead agencies, VA is developing the capability to provide a computerized data stream that will be transmitted daily to DoD and the CDC for contemporaneous analysis. Although the primary emphasis of the data supply will be ICD-9-CM coding information, other demographic and patient location data will be provided, as well. The data stream, which does not include interpretable unique identifiers, will be collected and analyzed by the CDC through its BioSense program, and by the DoD through its ESSENCE program. These data could also be paired with other data streams from other sources to identify patterns in syndromes and illnesses that may not originate from natural occurrences. VA outpatient and emergency room visits will provide the source data. An operational completion date for the venture has not yet been projected.

Thank you for the opportunity to comment on your draft report.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Anthony J. Principi".

Anthony J. Principi

---

# Appendix XVI: GAO Contacts and Acknowledgments

---

## GAO Contacts

David A. Powner, (202) 512-9286, (303) 572-7316 or [pownerd@gao.gov](mailto:pownerd@gao.gov)  
M. Yvonne Sanchez, (202) 512-6274 or [sanchezm@gao.gov](mailto:sanchezm@gao.gov)

---

## Acknowledgments

In addition to those named above, Larry E. Crosland, Neil J. Doherty, Amanda C. Gill, Pamlutricia Greenleaf, Joanne Fiorino, M. Saad Khan, Teresa F. Tucker, and Caroline C. Villanueva, made key contributions to this report.

---

## GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site ([www.gao.gov](http://www.gao.gov)) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone:      Voice: (202) 512-6000  
                              TDD: (202) 512-2537  
                              Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)  
E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Public Affairs

Jeff Nelligan, Managing Director, [NelliganJ@gao.gov](mailto:NelliganJ@gao.gov) (202) 512-4800  
U.S. General Accounting Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548