Attachment G

United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2005

INFORMATION TECHNOLOGY

Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure

GAO-05-308

June 2005

INFORMATION TECHNOLOGY

Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-308, a report to congressional requesters

Why GAO Did This Study

The anthrax scare of October 2001 exposed serious weaknesses in the U.S. public health infrastructure. Since then, the appearance of new infectious diseases has made preparation and readiness even more critical. Information technology (IT) can be a major factor in detecting and responding to public health emergencies, including bioterrorism.

GAO was asked to review the progress of major federal IT initiatives aimed at strengthening the ability of government at all levels to respond to public health emergencies, as well as to describe key challenges facing agencies pursuing these initiatives.

What GAO Recommends

To improve the development of major public health IT initiatives, GAO recommends, among other actions, that the Secretary of Health and Human Services (1) establish clear linkage between the initiatives and the national health care strategy and federal health architecture and (2) encourage interoperability through the adoption of standards for health care data and communications.

In response to a draft of this report, HHS generally concurred with the recommendations, while DHS did not comment specifically on them. Both agencies provided additional contextual information and technical comments, which were incorporated as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-05-308.

To view the full product, 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.

What GAO Found

Although significant work remains, federal agencies have made progress on major public health IT initiatives. These initiatives include one broad initiative at the Centers for Disease Control and Prevention (CDC)—known as the Public Health Information Network (PHIN)—which is intended to provide the nation with integrated information systems, and two initiatives at the Department of Homeland Security (DHS), which are focused on biosurveillance (see table). CDC's PHIN initiative has made progress by establishing communications systems and promoting standards, but more work remains on associated surveillance systems. For example, public health officials told GAO that they did not find PHIN's BioSense application useful because of limitations in the data currently collected. DHS also has major initiatives related to public health, both of which are in development. In addition, a system associated with one of the DHS initiatives—BioWatch—has been deployed. BioWatch, an early-warning environmental monitoring system that collects air samples in order to detect trace amounts of biological materials, recently underwent modification to solve an interoperability problem: its three IT components required redundant data entry in order to communicate with each other. According to DHS, it has developed a solution to this interoperability problem and implemented it at two locations; DHS plans to install that solution in the remaining BioWatch locations.

Major Federal Public Health IT Initiatives

Initiative	Description
CDC	
Public Health Information Network	A national initiative to implement a multiorganizational business and technical architecture and associated information systems.
DHS	
Biological Warning and Incident Characterization System	An initiative to integrate data from environmental monitoring and health surveillance systems to provide warning of a biological attack and to help guide an effective response.
National Biosurveillance Integration System	An effort to combine federal medical, environmental, agricultural, and intelligence data to allow early detection of events and assist response.

Sources: CDC and DHS.

CDC and DHS face challenges in planning and implementing their major public health IT initiatives. These challenges include (1) integrating current initiatives into a national health IT strategy and federal architecture to reduce the risk of duplicative efforts, (2) developing and adopting consistent standards to encourage interoperability, (3) coordinating initiatives with states and local agencies to improve the public health infrastructure, and (4) overcoming federal IT management weaknesses to improve progress on IT initiatives. Until these challenges are addressed, progress toward building a stronger public health infrastructure will be impeded, as will the ability to share essential information concerning public health emergencies and bioterrorism.

Contents

Figures

Abbreviations

BWICS	Biological Warning and Incident Characterization System
BWSIIP	BioWatch Signal Interpretation and Integration Program
CDC	Centers for Disease Control and Prevention
DHS	Department of Homeland Security
DOD	Department of Defense
Epi-X	Epidemic Information Exchange
ESSENCE	Electronic Surveillance System for the Early Notification of Community-based Epidemics
EPA	Environmental Protection Agency
HAN	Health Alert Network
HHS	Department of Health and Human Services
IT	information technology
LRN	Laboratory Response Network
NBIS	National Biosurveillance Integration System
NEDSS	National Electronic Disease Surveillance System
NEPHTN	National Environmental Public Health Tracking Network
OMB	Office of Management and Budget
PHIN	Public Health Information Network
RODS	Real-time Outbreak and Disease Surveillance
S&T	Science and Technology (Directorate of DHS)
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

June 10, 2005

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

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

The Honorable Adam H. Putnam
House of Representatives

The Honorable Richard Burr
Chairman, Subcommittee on Bioterrorism and Public Health Preparedness
Committee on Health, Education, Labor, and Pensions
United States Senate

It has been almost 4 years since the anthrax events of October 2001 highlighted the weaknesses in our nation's public health infrastructure.[1] Since that time, emerging infectious diseases have appeared—such as Severe Acute Respiratory Syndrome and human monkeypox—that have made our readiness for public health emergencies even more critical. Information technology (IT) is central to strengthening the public health infrastructure through the implementation of systems to aid in the detection, preparation for, and response to bioterrorism and other public health emergencies.

You asked us to review the current status of major federal IT initiatives aimed at strengthening the ability of government at all levels to respond to public health emergencies. Specifically, our objectives were to

[1]The public health infrastructure is the foundation that supports the planning, delivery, and evaluation of public health activities; it comprises 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.

- assess the progress of major federal IT initiatives designed to strengthen the effectiveness of the public health infrastructure and
- describe the key IT challenges facing federal agencies responsible for improving the public health infrastructure.

We selected specific IT initiatives to review from systems we identified in previous work,[2] focusing on major public health IT initiatives in surveillance and communication systems.[3] These initiatives were one broad initiative at the Department of Health and Human Services' (HHS) Centers for Disease Control and Prevention (CDC) and five initiatives at the Department of Homeland Security's (DHS) Science and Technology (S&T) Directorate. We also conducted limited work at the Department of Defense (DOD) because it provides technical support to one of the DHS initiatives. We also assessed the use of federal public health IT applications at six state and six local public health agencies. Further details of our objectives, scope, and methodology are provided in appendix I. Our work was performed from July 2004 through April 2005, in accordance with generally accepted government auditing standards.

Results in Brief

Federal agencies have made progress on major public health IT initiatives, although significant work remains to be done. These initiatives include one broad initiative at CDC—the Public Health Information Network (PHIN) initiative—which is intended to provide the nation with integrated public health information systems to counter national civilian public health threats, and two major initiatives at DHS, which are primarily focused on biosurveillance.[4] CDC's broad PHIN initiative encompasses a number of applications and initiatives, which show varied progress. Currently, PHIN's basic communications systems are in place, but it is unclear when its

[2]GAO, *Bioterrorism: Information Technology Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, GAO-03-139 (Washington, D.C.: May 30, 2003).

[3]We excluded food safety systems and Department of Defense disease surveillance systems that did not include civilian populations.

[4]There is no generally accepted definition of biosurveillance; it generally refers to the automated monitoring of information sources of potential value in detecting an emerging epidemic, whether naturally occurring or the result of bioterrorism. Information sources may include data from environmental monitoring systems, the purchases of over-the-counter medication, and medical symptoms reported during ambulatory care.

surveillance systems and data exchange applications will become fully deployed. Further, the overall implementation of PHIN does not yet provide the desired functionality, and so some applications are not widely used by state and local public health officials. For example, CDC's BioSense application, which is aimed at detecting early signs of disease outbreaks, is available to state and local public health agencies, but according to the state and local officials with whom we spoke, it is not widely used, primarily because of limitations in the data it currently collects. DHS is also pursuing two major public health IT initiatives—the National Biosurveillance Integration System and the Biological Warning and Incident Characterization System (BWICS). Both of these initiatives are still in development. The BWICS initiative, in addition, is associated with three other programs, one of which—BioWatch—is operational. This early-warning environmental monitoring system was developed for detecting trace amounts of biological materials and has been deployed in over 30 locations across the United States. Until recently, its three IT components were not interoperable and required redundant data entry in order to communicate with each other.

As federal agencies work with state and local public health agencies to improve the public health infrastructure, they face several challenges. First, the national health IT strategy and federal health architecture are still being developed;[5] CDC and DHS will face challenges in integrating their public health IT initiatives into these ongoing efforts. Second, although federal efforts continue to promote the adoption of data standards, developing such standards and then implementing them are challenges for the health care community. Third, these initiatives involve the need to coordinate among federal, state, and local public health agencies, but establishing effective coordination among the large number of disparate agencies is a major undertaking. Finally, CDC and DHS face challenges in addressing specific weaknesses in IT planning and management that may hinder progress in developing and deploying public health IT initiatives. Until all these challenges are addressed, progress toward building a stronger public health infrastructure will be impeded, as will the ability to share essential information concerning public health emergencies and bioterrorism.

[5]The strategy is being developed on the basis of a framework that HHS published in July 2004.

We are making recommendations to the Secretary of Health and Human Services to coordinate with state and local public health agencies, align federal public health IT initiatives with the national health IT strategy and federal health architecture, and continue federal actions to encourage the development and adoption of data standards. We are also making recommendations to the Secretary of Homeland Security to assess the department's alignment of its initiatives with those of other federal activities.

We received written comments on a draft of this report from HHS and DHS. HHS generally concurred with our recommendations, while DHS did not comment specifically on the recommendations. Both agencies provided additional contextual information and technical comments, which we have incorporated in this report as appropriate. We provided DOD officials with the opportunity to comment on a draft of this report, which they declined.

Background

On June 12, 2002, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002,[6] which 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; and improving state, local, and hospital preparedness and response. The Secretary of HHS is required to provide for the establishment of an integrated system or systems of public health alert communications and surveillance networks among (1) federal, state, and local public health officials; (2) public and private health-related laboratories, hospitals, and other health care facilities; and (3) any other entities that the Secretary determines are appropriate. These networks are to allow for secure and timely sharing and discussion of essential information concerning bioterrorism and other public health emergencies, as well as recommended methods for responding to such an attack or emergency. In addition, no later than 1 year after the enactment of the law, the Secretary, in cooperation with health care providers and state and local public health officials, was to establish any additional technical and reporting standards, including those for network interoperability.

[6]Public Law 107-188 (June 12, 2002).

Since fiscal year 2002, HHS has funded over $2.7 billion for public health preparedness efforts through grants administered by CDC and just over $1 billion for hospital preparedness grants administered by the Health Resources and Services Administration. To encourage the integration of health care system response plans with public health department plans, HHS has incorporated both public health preparedness and hospital performance goals into the agreements that the department uses to fund state and local public health preparedness improvements. The funding guidance provided by HHS to state and local governments calls for improvements in seven key areas:

- preparedness planning and readiness assessment,
- surveillance and epidemiology capacity,
- laboratory capacity for handling biological agents,
- laboratory capacity for handling chemical agents,
- health alert network/communication and IT,
- risk communication and health information dissemination, and
- education and training.

Over the past year, federal actions to encourage the use of IT for health care delivery and public health have been accelerated. In April 2004, the President established the goal that health records for most Americans should be electronic within 10 years and issued an executive order to "provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care." As part of this effort, the President tasked the Secretary of HHS to appoint a National Coordinator for Health Information Technology—which he subsequently did 1 week later. The President's executive order called for the Coordinator to develop a strategic plan to guide the implementation of interoperable health IT in the public and private health care sectors. In July 2004, HHS issued a

framework for strategic action that includes four broad goals; goal four of that framework is directed at improvements in public health.[7]

Further, DHS released the National Response Plan[8] this past January, under which HHS is to continue to lead the federal government in providing public health and medical services during major disasters and emergencies. In this role, HHS is to coordinate all federal resources related to public health and medical services that are made available to assist state, local, and tribal officials during a major disaster or emergency.

Role of IT in Public Health Preparedness and Response

As we reported in May 2003, IT can play an essential role in supporting federal, state, local, and tribal governments in public health preparedness and response.[9] Development of IT can build upon the existing systems capabilities of state and local public health agencies, not only to provide routine public health functions, but also to support public health emergencies, including bioterrorism. In addition, according to the Institute of Medicine, the rapid development of new IT offers the potential for greatly improved surveillance capacity.[10] Finally, for public health emergencies in particular, the ability to quickly exchange data between providers and public health agencies—or among providers—is crucial in detecting and responding to naturally occurring or intentional disease outbreaks.

Because of the dynamic and unpredictable nature of public health emergencies, various types of IT systems may be used during the course of an event. These include

[7]Department of Health and Human Services, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care* (Washington, D.C.: July 21, 2004).

[8]The National Response Plan is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of federal support to state, local, and tribal incident managers and for exercising direct federal authorities and responsibilities.

[9]GAO-03-139.

[10]Institute of Medicine of the National Academies, *The Future of the Public's Health in the 21st Century* (Washington, D.C.: November 2002).

- surveillance systems, which facilitate the performance of ongoing collection, analysis, and interpretation of disease-related and environmental data so that responders and decision makers can plan, implement, and evaluate public health actions (these systems include devices to collect and identify biological agents from environmental samples, and they make use of IT to record and transmit data); and

- communications systems, which facilitate the secure and timely exchange of information to the relevant responders and decision makers so that appropriate action can be taken.

Other types of IT may also be used, such as diagnostic systems, which identify particular pathogens and those that include data from food, water, and animal testing, but such systems are not among the major federal public health IT initiatives.

State and Local Roles in Surveillance and Communications

Although state health departments have primary responsibility for disease surveillance in the United States, total responsibility for surveillance is shared among health care providers: more than 3,000 local county, city, and tribal health departments; 59 state and territorial health departments; more than 180,000 public and private laboratories; and public health officials from multiple federal agencies. In addition, the United States is a member of the World Health Organization, which is responsible for coordinating international disease surveillance and response actions.

While health care providers are responsible for the medical diagnosis and treatment of their individual patients, they also have a responsibility to protect public health—a responsibility that includes helping to identify and prevent the spread of infectious diseases. Because health care providers are typically the first health officials to encounter cases of infectious diseases—and have the opportunity to diagnose them—these professionals play an important role in disease surveillance. Generally, state laws or regulations require health care providers to report confirmed or suspected cases of notifiable diseases[11] to their state or local health department. States publish lists of the diseases they consider notifiable and therefore subject to reporting requirements. According to the Institute of Medicine,

[11]A notifiable disease is an infectious disease for which regular, frequent, and timely information on individual cases is considered necessary for the prevention and control of the disease.

most states also require health care providers to report any unusual illnesses or deaths, especially those for which a cause cannot be readily established. However, according to CDC, despite state laws requiring the reporting of notifiable diseases, a significant proportion of these cases are not reported, which is a major challenge in public health surveillance.

Health care providers rely on a variety of public and private laboratories to help them diagnose cases of notifiable diseases. In some cases, only laboratory results can definitively identify pathogens.[12] Every state has at least one public health laboratory to support its infectious diseases surveillance activities and other public health programs. State laboratories conduct testing for routine surveillance or as part of clinical or epidemiologic studies. For rare or unusual pathogens, these laboratories provide diagnostic tests that are not always available in commercial laboratories. State public health laboratories also provide specialized testing for low-incidence but high-risk diseases such as tuberculosis and botulism. Results from state public health laboratories are used by epidemiologists to document trends and identify events that may indicate an emerging problem. Upon diagnosing a case involving a notifiable disease, local health care providers are required to send the reports to state health departments through state and local disease-reporting systems, which range from paper-based reporting to secure, Internet-based systems.[13]

States, through their state and local health departments, have principal responsibility for protecting the public's health and therefore take the lead in conducting disease surveillance and supporting response efforts. Generally, local health departments are responsible for conducting initial investigations into reports of infectious diseases, employing epidemiologists, physicians, nurses, and other professionals. Local health departments are also responsible for sharing information that they obtain from providers or other sources with the state department of health. State health departments are responsible for collecting surveillance information statewide, coordinating investigations and response activities, and

[12]Pathogens are bacteria, viruses, parasites, or fungi that have the capability to cause disease in humans.

[13]In some cases, depending on state law, providers and others report first to local health departments, which report the disease information to the state health department. Local health departments may also conduct their own follow-up investigations into reports of notifiable diseases.

voluntarily sharing surveillance data with CDC and others. States vary in their requirements governing who should report notifiable diseases; in addition, the deadlines for reporting these diseases after they have been diagnosed vary by disease. State health officials conduct their own analyses of disease data to verify cases, monitor the incidence of diseases, and identify possible outbreaks.

In reporting their notifiable disease data to CDC, states use multiple and sometimes duplicative systems. States are not legally required to report information on notifiable diseases to CDC, but CDC officials explained that the agency makes such reporting from the states a prerequisite for receiving certain types of CDC funding.

Federal Role in Surveillance and Communications

Generally, the federal government's role in disease surveillance is to collect and analyze national disease surveillance data and maintain disease surveillance systems. Federal agencies investigate the causes of infectious diseases and maintain their own laboratory facilities. They also use communications systems to share disease surveillance information. In addition, federal agencies provide funding and technical expertise to support disease surveillance at the state, local, and international levels.

Federal agencies such as CDC, the Food and Drug Administration, and DOD conduct disease surveillance using systems that gather data from various locations throughout the country to monitor the incidence of infectious diseases. In addition to using surveillance systems to collect and analyze notifiable disease data reported by states, federal agencies use other surveillance systems to collect data on different diseases or from other sources (e.g., international sources). These systems supplement the state data on notifiable diseases by monitoring surveillance information that states do not collect.

In general, surveillance systems are distinguished from one another by the types of infectious diseases or syndromes they monitor and the sources from which they collect data. Some disease surveillance systems rely on groups of selected health care providers who have agreed to routinely supply information from clinical settings on targeted diseases. A relatively new type of surveillance system, known as a syndromic surveillance system, monitors the frequency and distribution of health-related symptoms—or syndromes—among people within a specific geographic area. These syndromic surveillance systems are designed to detect anomalous increases in certain syndromes, such as skin rashes, that may

indicate the beginning of an infectious disease outbreak. Some monitor data from hospital and emergency room admissions or data from over-the-counter drug sales. Other data sources may include poison control centers, health plan medical records, first-aid stations, emergency medical service data, insurer claims, and discharge diagnosis information. For syndromic data to be analyzed effectively, information must be timely, and the analysis must take into account the context of the locality from which the data were generated.

Because syndromic surveillance systems monitor symptoms and other signs of disease outbreaks instead of waiting for clinically confirmed reports or diagnoses of a disease, some experts believe that syndromic surveillance systems could help public health officials increase the speed with which they may identify outbreaks. However, as we reported last September, syndromic surveillance systems are relatively costly to maintain compared with other types of disease surveillance and are still largely untested.[14]

Major CDC and DHS Public Health IT Initiatives

Two federal agencies are involved in major public health IT initiatives that focus on disease surveillance and communications.

- CDC, one of HHS's divisions, has primary responsibility for conducting national disease surveillance[15] and developing epidemiological and laboratory tools to enhance surveillance of disease, including public health emergencies. It also provides an array of technical and financial support for state infectious disease surveillance.

- DHS's mission involves, among other things, protecting the United States against terrorist attacks, including bioterrorism. Its Science and Technology (S&T) Directorate serves as the department's primary research and development arm. Its focus is on catastrophic terrorism—threats to the security of the United States that could result in large-scale loss of life and major economic impact. S&T's work is designed to

[14]GAO, *Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts*, GAO-04-877 (Washington, D.C.: Sept. 30, 2004).

[15]CDC's responsibilities for surveillance are not limited to diseases, but also include chemical, injury, and health conditions, among others.

counter those threats, both by improvements to current technological capabilities and development of new ones.

(Other federal agencies' roles in public health are described in app. II.)

CDC's major IT initiative, known as PHIN, is a national initiative to implement a multiorganizational business and technical architecture for public health information systems. After the 2001 anthrax incidents, CDC was mandated to increase national preparedness and capabilities to respond to naturally occurring diseases and conditions and the deliberate use of all threats, including biological, chemical, and radiological agents. CDC sees PHIN as an essential part of its strategy to achieve this mandate.

According to CDC, the PHIN architecture

- defines and documents the systems needed to support public health professionals;
- identifies the industry standards that are necessary to make these systems work together;
- develops the specifications necessary to make these standards do the work of public health;
- defines integration points for systems to work together to meet the broad functional needs;
- establishes tools and components that support standards-based systems; and
- supports the certification process necessary to establish interoperability.

To help achieve its goals, PHIN is also intended to integrate and coordinate existing systems, and CDC makes PHIN software available for optional use by state and local public health agencies.

PHIN has substantial size and scope, because it is intended to serve as a comprehensive architecture, information exchange network, and set of services that will integrate existing capabilities and advance the ways in which IT can support public health. It is intended to improve public health systems and networks and to provide a means for exchanging data with

other federal agencies, state and local government agencies, the private health care sector, and others.

As part of PHIN, CDC has established the PHIN Preparedness initiative, which it describes as striving to accelerate the pace at which jurisdictions acquire or acquire access to public health preparedness systems. This initiative focuses on the near-term aspects of PHIN. According to CDC, the agency and its public health partners have identified a set of functional requirements defining the core capabilities for preparedness systems; these are categorized into six broad functional areas:

- Early event detection: The early identification of bioterrorism and naturally occurring health events in communities.
- Outbreak management: The capture and management of information associated with the investigation and containment of a disease outbreak or public health emergency.
- Connection of laboratory systems: The development and adoption of common specifications and processes to enable public health laboratories to electronically exchange information with public health agencies.
- Countermeasure and response administration: The management and tracking of measures taken to contain an outbreak or event and to provide protection against a possible outbreak or event.
- Partner communications and alerting: The development of a nationwide network of integrated communications systems capable of rapid distribution of health alerts and secure communications among public health professionals involved in an outbreak or event.
- Cross-functional components: Technical capabilities, or components, common across functional areas that are necessary to fully support PHIN Preparedness requirements.

CDC officials stated that by September 2005, the agency will expect states to meet PHIN Preparedness requirements in these areas as a condition for receiving public health preparedness funding; CDC expects that this condition on funding will promote a wider adoption of PHIN standards.

Table 1 presents communications and surveillance applications that are part of the PHIN initiative (some of which are significant system development efforts in themselves), along with the PHIN Preparedness functional areas that they support.

Table 1: PHIN Applications Reviewed

Application[a]	PHIN Preparedness functional area	Description
Communications		
Epidemic Information Exchange (Epi-X)	Partner communications and alerting	A secure, Web-based communications system through which public health professionals share information relevant to public health emergencies.
Health Alerting	Partner communications and alerting	A service that broadcasts e-mails of emergency notifications from CDC to state health officers, epidemiologists, lab directors, etc.
Surveillance		
BioSense	Early event detection	A Web-based application that provides access to health-related data to enhance early event detection of naturally occurring events and possible bioterrorist attacks. It is intended to enhance early detection by including syndromic surveillance and diagnostic data.
National Electronic Disease Surveillance System (NEDSS) Base System	Early event detection	A surveillance system that supports the electronic processes involved in notifiable disease surveillance and analysis, replacing the functionality supported by the current legacy system (National Electronic Telecommunications System for Surveillance). It is expected to provide the platform upon which state and program area needs, data collection, and processing can be built, including the development of modules that can be used for data entry and management of disease surveillance data.
National Environmental Public Health Tracking Network (NEPHTN)	—	An interoperable standards-based network planned to integrate three components: hazard monitoring, exposure surveillance, and health effects surveillance. This system is being designed to identify potential relationships between exposure and health conditions that either indicate the need for additional research or require intervention to prevent disease, disability, and injury. Data from NEPHTN will be available for public health policy analysis.
Other		
LRN Results Messaging	Connection of laboratory systems	An application supporting the exchange of laboratory test results from the Laboratory Response Network (LRN) laboratories to public health departments and to CDC, with current use in support of the BioWatch program of air sampling in many U.S. metropolitan areas.

(Continued From Previous Page)

Application[a]	PHIN Preparedness functional area	Description
Outbreak Management System	Outbreak management	An application that runs on a laptop, a local area network, and in synchrony with a central repository for the collection, management, and analysis of data during investigations of disease outbreaks. It provides response teams with a standardized data management tool.
PHIN Messaging System[b]	Cross-functional components	A generic, standards-based message transport system that is platform-independent and uses the Electronic Business Extensible Markup Language (ebXML) infrastructure to securely transmit public health information over the Internet.

Source: CDC.

[a]PHIN also includes other components that we did not review, such as PHIN Directory and PHIN Vocabulary Services, because our review was focused on communications and surveillance systems.

[b]Although the PHIN Messaging System is not an application per se, it is an important data exchange component for PHIN applications.

Many of these applications are associated with larger initiatives that predated PHIN (see table 2), which are now incorporated under the PHIN umbrella. For example, the origins of NEDSS date to 1995, when CDC co-authored a report that documented the problems of fragmentation and incompatibility in the nation's disease surveillance systems.[16] The recommendations in this report led CDC to develop the NEDSS initiative, which was begun in October 1999 and incorporated into PHIN in 2002.

[16]CDC and Agency for Toxic Substances and Disease Registry, *Integrating Public Health Information and Surveillance Systems* (Atlanta, Ga.: Spring 1995).

Table 2: Initiatives under PHIN

Initiative	PHIN Preparedness functional area	Description
BioSense	Early event detection	An initiative supporting early event detection that uses an approach to public health surveillance based on the secondary use of health care and health-related data.
Health Alert Network (HAN)	Partner communications and alerting	An initiative to ensure that state and local health departments have rapid and timely access to emerging health information through providing grants to develop connectivity and alerting capabilities.
National Electronic Disease Surveillance System (NEDSS)	Early event detection	An initiative to implement a national surveillance architecture using data and information system standards. This architecture is to advance the development of efficient, integrated, and interoperable surveillance systems at federal, state, and local levels.
National Environmental Public Health Tracking Network (NEPHTN)	—	A collaborative effort between CDC and the Environmental Protection Agency to develop a national environmental public health tracking network that will allow direct electronic data reporting of health effects, exposure, and hazard data.

Source: CDC.

As part of its mission to protect the nation against terrorist attacks (including possible bioterrorism), DHS is also pursuing major public health IT initiatives. These initiatives and associated programs, which are primarily focused on signal interpretation and biosurveillance, are described in table 3.

Table 3: DHS Biosurveillance IT Initiatives

Initiative	Description
Biological Warning and Incident Characterization System (BWICS)	A system that is expected to integrate data from environmental monitoring and health surveillance systems with incident characterization tools[a] in order to provide timely warning of a biological attack and to help guide an effective response. BWICS is also expected to provide secure distribution of information to different types of users.
BioNet	A cooperative program between DHS's S&T Directorate and DOD (established as a demonstration project in May 2004) that is expected to integrate civilian and military capabilities at the local level for detecting and responding to the use of biological agents. The BioNet initiative is being developed in one city. It includes the use of a syndromic surveillance system known as the Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE).[b] DHS plans now call for BioNet to be terminated in fiscal year 2005 with lessons learned, tools, and capabilities transferred to the BWICS initiative.
BioWatch	An early-warning environmental monitoring system that collects air samples from high-threat cities in order to detect trace amounts of biological materials. BioWatch consists of three IT components: a sample management tracking system, a lab analysis tracking system, and an electronic reporting system. BioWatch labs use the reporting system to send data to CDC, who then sends a monthly report of negative results to DHS.
BioWatch Signal Interpretation and Integration Program (BWSIIP)	A surveillance program pilot that is intended to evaluate public data feeds for their usefulness in biomonitoring signal interpretation to provide BioWatch metropolitan areas, in the event of a signal detection, with the ongoing collection and analysis of appropriate medical information (with personally identifying information removed) that would support rapid interpretation of the signal and integration into consequence management operations. Once BWSIIP is deployed as part of BWICS, plans call for local public health agencies to use locally existing or publicly available biosurveillance tools provided by DHS, such as ESSENCE, or the Real-time Outbreak and Disease Surveillance (RODS) software.[c]
National Biosurveillance Integration System	An effort at the federal level to combine multiple data streams from sector-specific agencies—those with medical, environmental, agricultural, and intelligence data—to give DHS situational awareness that is expected to allow earlier detection of events and to assist in response actions.

Source: DHS.

[a]Incident characterization tools are designed to integrate information from surveillance, environmental monitoring, plume hazard predictions, epidemiological forecasts, and population and critical infrastructure databases.

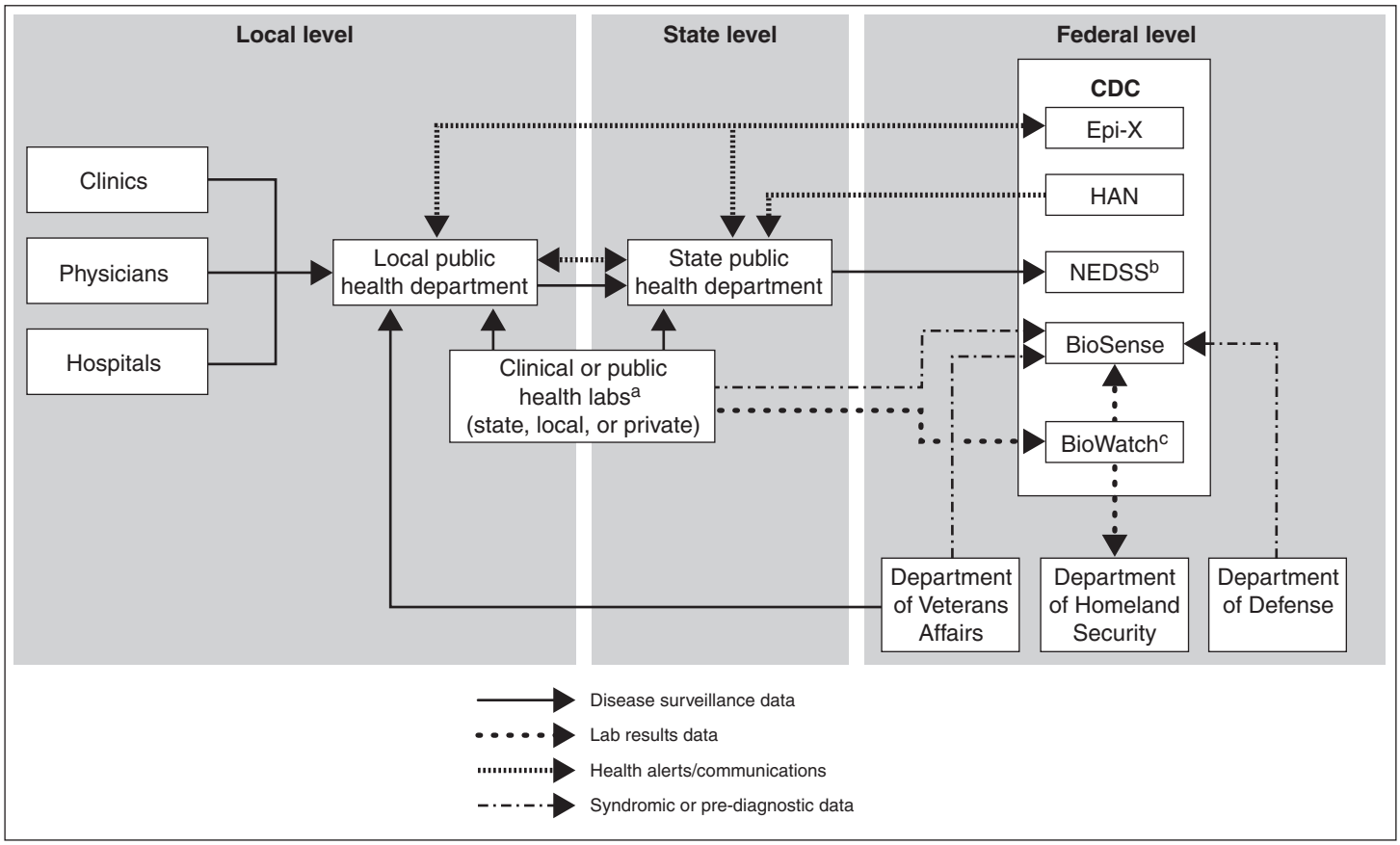
[b]ESSENCE is a syndromic surveillance software package available through free licensing agreements with the Johns Hopkins University Applied Physics Lab. The software is available to federal, state, and local health organizations that wish to deploy a Web-based syndromic surveillance system using their own data. DOD uses the system worldwide. The Department of Veterans Affairs and about 26 states and localities are implementing ESSENCE.

[c]RODS, developed by the University of Pittsburgh, is a syndromic surveillance system used by several states that collects data from hospital emergency room visits. This system identifies patients' chief medical complaints, classifies the complaints according to syndrome, and aggregates those data in order to look for anomalous increases in certain syndromes that may reveal an infectious disease outbreak.

Figure 1 illustrates a simplified flow of existing surveillance information and health alerts among local, state, and federal agencies. This diagram does not show all flows of information that would occur in the case of an

outbreak. For example, local health agencies may send alerts to health care providers.

Figure 1: Simplified Information Flow among Local, State, and Federal Agencies for Surveillance Data and Health Alerts/Communications



Source: GAO.

Note: The CDC systems listed provide information to health professionals and others by various means, such as the Internet for BioSense and Epi-X.

[a]Only selected labs participate in the BioWatch program or provide data to BioSense.

[b]Currently, state and local health departments submit information on nationally notifiable diseases to CDC using multiple systems. Once fully implemented, NEDSS will replace some of those reporting systems. Note that NEDSS or other disease-reporting systems are also implemented at the state level.

[c] Although BioWatch is a DHS initiative, CDC receives the lab results data. Positive results are sent to the DHS Homeland Security Operations Center, as well as to the Joint Terrorism Task Force and Federal Bureau of Investigation.

According to CDC, costs for its PHIN initiatives and applications for fiscal years 2002 through 2005, totaling almost $362 million, are summarized in table 4. Most of these costs support local, state, and federal public health activities.

Table 4: Reported Costs for PHIN-Related Initiatives and Applications for Fiscal Years 2002–2005

Dollars in millions

Initiatives and applications	FY 2002 actual	FY 2003 actual	FY 2004 actual	FY 2005 budget	Total
Communications					
Epi-X application	$2.1	$1.4	$0.9	$0.9	**$5.3**
Health Alert Network initiative	21.0	21.0	23.0	23.0	**88.0**
Health Alerting application	0.5	0.5	0.5	0.5	**2.0**
Grants for state and local agencies	20.5	20.5	22.5	22.5	**86.0**
Surveillance					
BioSense initiative	0	6.0	17.8	50.8	**74.6**
BioSense application	0	6.0	5.3	3.0	**14.3**
Other BioSense costs[a]	0	0	12.5	47.8	**60.3**
NEDSS initiative	27.0	27.1	24.7	24.7	**103.5**
NEDSS Base System[b]	14.0	15.2	13.8	15.0	**58.0**
Grants for state and local agencies	13.0	11.9	10.9	9.7	**45.5**
National Environmental Public Health Tracking Network (NEPHTN) initiative	0	20.5	19.9	19.2	**59.6**
NEPHTN application	0	2.0	2.2	3.0	**7.2**
Grants for state and local agencies	0	18.5	17.7	16.2	**52.4**
Other					
PHIN supporting costs[c]	0	0	9.1	8.9	**18.0**
LRN Results Messenger application	0	0	0.7	0.7	**1.4**
Outbreak Management System	0	3.1	3.1	3.2	**9.4**
PHIN Messaging System	0	in NEDSS	0.9	1.1	**2.0**
Subtotal for PHIN applications	**16.6**	**28.2**	**27.4**	**27.4**	**99.6**
Total PHIN-related initiatives and applications	**$50.1**	**$79.1**	**$100.1**	**$132.5**	**$361.8**

Source: CDC.

[a]Consist of remaining BioSense costs, including data acquisition, algorithm development, biointelligence center, etc.

[b] Includes development cost for the program area modules.

[c]Among other things, includes the development of requirements, standards, and specifications, as well as the certification and communications programs.

According to DHS, IT costs for its biosurveillance initiatives for fiscal years 2003 through 2005 total about $45 million; these are summarized in table 5. This table does not reflect the total costs for the programs supporting these IT initiatives.

Table 5: Reported IT Costs for DHS Biosurveillance IT Initiatives, Fiscal Year 2003–2005

Dollars in millions

IT initiatives	FY 2003 actual	FY 2004 actual	FY 2005 budget	Total
Biological Warning and Incident Characterization System	$0	$3.5	$10.0	**$13.5**
BioNet[a]	5.6	0	0	**5.6**
BioWatch	1.0	.5	3.8	**5.3**
BioWatch Signal Interpretation and Integration Program	0	7.3	0	**7.3**
National Biosurveillance Integration System	0	2.0	11.0	**13.0**
Total	**$6.6**	**$13.3**	**$24.8**	**$44.7**

Source: DHS.

[a]Although DHS funds BioNet, the Department of Defense's Defense Threat Reduction Agency is the project lead and responsible for managing the day-to-day operations of the project. This fiscal year, BioNet lessons learned, tools, and capabilities are to be incorporated into the BWICS initiative, after which DHS funding for BioNet is not expected to continue.

Progress Made in Federal Public Health IT Applications, But More Work Remains

CDC and DHS have made progress on federal public health IT initiatives, including CDC's PHIN initiative, which is intended to provide the nation with integrated public health information systems to counter national civilian public health threats, and two major initiatives at DHS—primarily focused on signal interpretation and biosurveillance—one of which is associated with three other programs. However, while progress has been made, more work remains, particularly in surveillance and data exchange. PHIN communications systems are being used, and improvements to surveillance systems (disease, syndromic, and environmental monitoring) are still being developed. Other PHIN applications are available for optional use by state and local public health officials, but they are not widely used because of system limitations. DHS's two major biosurveillance IT initiatives are still in the development stage, and one of the associated programs—BioWatch—is operational. However, as initially deployed, BioWatch required modification, because its three IT components did not communicate with each other, requiring redundant data entry. According to DHS, it has developed a solution to this

interoperability problem and implemented it at two locations; DHS plans to install that solution in the remaining BioWatch locations.

Projects under CDC's Public Health Information Network Are in Various Stages of Implementation

Table 6 briefly describes the status of CDC's PHIN applications, including operational status, number of installations or users, and future plans. Of the various PHIN applications, one is still in the planning process, two are partially operational, and five are operational.

Table 6: Status of Selected CDC PHIN Applications as of March 1, 2005

Applications	Status	Users[a]	Future plans
Communications			
Epidemic Information Exchange	Operational	3,260 state, local, federal, and international health officials	Upgrade for PHIN compliance Improve usability per user requests
Health Alerting	Operational	66 states, metro areas, territories	Maintain application as is
Surveillance			
BioSense	Operational	50 states, 30 metro areas	Continue to expand current functionality Add new algorithms and data sources
NEDSS Base System	Partially operational[b]	10 states	Continue to expand current functionality Improve usability per user requests Upgrade operating environment Continue development of program area modules
National Environmental Public Health Tracking Network	Planning	Not applicable	Continue state pilot projects Plan for network development based on pilots
Other			
LRN Results Messenger	Partially operational	95% of BioWatch labs	Continue to expand current functionality Improve usability per user requests Support proficiency testing Expand usage to all CDC-funded LRN laboratories
Outbreak Management System	Operational	CDC[c]	Continue to expand current functionality Improve usability per user requests Add capacity for importing data
PHIN Messaging System	Operational	51 locations[d]	Continue to expand current functionality Respond to stakeholder requests to improve usability

Source: GAO analysis of CDC data.

[a]Users include either the number of individuals with access to the system or the number of locations that have installed the software; while there are federal users, not all are listed in this table.

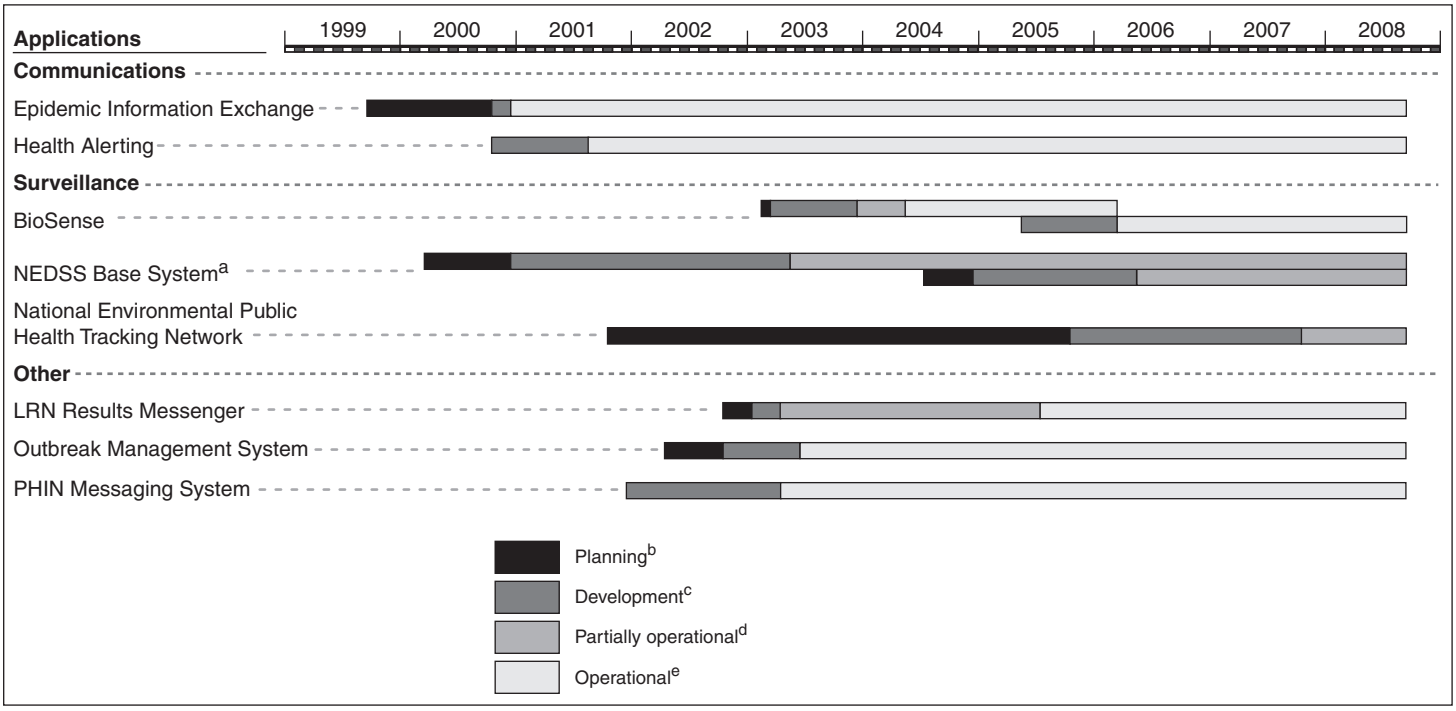
[b]Partially operational means that the system is functional and being used but not deployed to all installation sites.

[c]Not used by users outside CDC, although once used externally for a small, disease-specific outbreak at a state prison.

[d]Includes usage for 10 NEDSS Base System states, many labs in the Laboratory Response Network, 5 hospitals in the National Healthcare Safety Network, 3 state health departments for intrastate messaging, 9 hospitals and labs for lab messaging, and 2 BioSense data providers.

Figure 2 shows the time frames for the planning, development, and implementation of the PHIN applications; these applications vary considerably both in complexity and in time needed to complete implementation.

Figure 2: Estimated Time Lines of PHIN Applications



Source: GAO analysis of CDC data.

[a]The NEDSS Base System includes the development of program area modules.

[b]Planning means preparing to design the system or application.

[c]Development means the acquisition or enhancement of the system or application.

[d]Partially operational means that the system is functional and being used but not deployed to all installation sites.

[e]Operational means that the system is fully deployed.

Two PHIN Communications Systems Are Fully Implemented and in Use

Health Alerting. The Health Alerting application, which is used to broadcast e-mail alerts to state and local public health officials about disease outbreaks, became operational in October 2000. This application provides full-time (24 hours a day, 7 days a week) Internet access and broadcast e-mail and fax capabilities.

The Health Alerting application is part of the Health Alert Network initiative, which provides grant funding to states and local public health agencies for enhancement of their IT infrastructures. Using these funds, states and localities have either built their own Health Alert Networks or acquired commercial systems for alerting state and local officials. Some state Health Alert Networks use more sophisticated applications than the CDC Health Alerting application, providing various kinds of alerts based on user profiles and allowing document sharing.

Epi-X. Epi-X, which is designed to be a secure, Web-based communications system through which public health professionals share information on public health emergencies, was implemented in December 2000 and is being used by state and local public health officials. Epi-X includes multiple mechanisms for alerting; secure, moderated communications and discussion about disease outbreaks and other acute health events as they evolve; and a searchable report database. Most of the state and local health officials with whom we spoke were satisfied with the system. However, some officials questioned the need for both Health Alerting and Epi-X, since both applications have similar functionality and are used by some of the same public health officials. According to CDC, it is planning to create a common platform for use by both applications.

Two of Three PHIN Surveillance Systems Are Not Yet Fully Operational

The National Electronic Disease Surveillance System (NEDSS). The NEDSS initiative promotes the use of data and information systems standards for the development of interoperable surveillance systems at federal, state, and local levels. It is intended to minimize the problems of fragmented, disease-specific surveillance systems; however, this goal is still years away from being achieved.

A primary goal of NEDSS is the ongoing, automatic capture and analysis of data that are already available electronically. Its system architecture is designed to integrate and replace several current CDC surveillance systems, including the National Electronic Telecommunications System for Surveillance, the HIV/AIDS reporting system, and the systems for vaccine preventable diseases, tuberculosis, and other infectious diseases. In previous fiscal years, CDC funded 50 states and 7 localities. These states

and localities can use CDC's NEDSS Base System or build systems compatible with NEDSS/PHIN standards. The initiative includes an architecture to guide states and CDC as they build NEDSS-compatible systems, which can be either commercial or custom developed. The initiative is also intended to promote the use of data standards to advance the development of interoperable disease surveillance systems at federal, state, and local levels.

Besides providing a secure, accurate, and efficient way to collect, process, and transmit data to CDC, the NEDSS Base System is intended to provide a platform upon which program area modules can be built to meet state and program area data needs. (Programs may be focused on specific diseases, populations, or other areas—such as smoking or obesity.) Program area modules are critical to eventually reducing the many program-specific surveillance systems that CDC currently maintains by consolidating the data collection of the various programmatic disease surveillance activities that are currently in place.

Although CDC has been developing the NEDSS Base System since 2000, it is still only partially deployed. There are no clear milestones and plans for when the Base System will become fully deployed, although multiple versions of the Base System have been developed and deployed in several states. According to CDC, the NEDSS Base System has been deployed in 5 states since December 2004, and it expects implementation to continue with the 11 remaining states that are planning to use the Base System, but the implementation time frames will depend on when these states are ready to accept the system. Table 7 summarizes the status of NEDSS system implementation across the nation, which shows that about half of the states and localities have operational NEDSS systems.

Table 7: Number of States and Localities with NEDSS Systems

Status	NEDSS Base System	NEDSS-compatible system	Total
Planning or development	11	16	**27**
Operational	10	20	**30**
Total	**21**	**36**	**57**

Source: GAO analysis of CDC data.

Note: Total includes 50 states and 7 localities.

In addition, four NEDSS program area modules are being used, and six are in the process of being developed. Additional program area modules will be developed for other disease-specific areas in the coming years.

BioSense. CDC's BioSense, which the agency describes as an early event detection system, is designed to provide near real-time event detection by using data (without patient names or medical numbers) from existing health-related databases. Although CDC began using BioSense data in late 2003, the BioSense application was implemented for state and local use in May 2004. BioSense is continuously being updated, and current plans for phase two of BioSense development call for enhancements to begin in May 2005.

BioSense is a Web-based application that currently provides CDC and state and local users with the ability to view syndromic and prediagnostic data: specifically, Defense and Veterans Affairs ambulatory care data, BioWatch laboratory results, and national clinical labs data. Initially, CDC also provided data on sales of over-the-counter medication, but these were later discontinued. BioSense data are provided in the form of data reports displayed in various ways, rather than as raw data that can be input to analytical systems.

Although CDC uses BioSense for a number of federal bioterrorism preparedness activities, BioSense is not extensively used by the state and local public health officials with whom we spoke, primarily because of limitations in the data and its presentation. These officials stated that the DOD and VA data were not useful to them,[17] either because they were in locations without large military or veteran populations, or because they could get similar data elsewhere. For instance, many of these officials have access to local syndromic surveillance systems, which better fit their needs because the systems have better capabilities or because they provide data that are more timely than BioSense data. Some of these officials stated that they would prefer CDC to provide data for them to conduct their own analyses, especially data from national sources such as clinical laboratories, rather than displaying the data on the BioSense Web site. According to CDC officials, they will provide raw data to public health agencies upon request, have increased the number of data sets available, and have expanded the scope of user support by (1) increasing

[17]Some state and local officials said that they had found over-the-counter sales data the most useful, but these reports were discontinued.

communications with state and local public health departments in the use of and response to daily surveillance data patterns, (2) monitoring data during special events (e.g., a presidential inauguration and sporting events) at state and local request, and (3) contracting with John Hopkins University for development of a standard operating procedure for monitoring and using early event detection.

National Environmental Public Health Tracking Network (NEPHTN). Initiated in 2001, NEPHTN is still in the planning stage. CDC is planning to begin development of the network in 2006 and implementation of phase one in 2008. This initiative involves intra- and interagency collaboration among CDC and other federal agencies. CDC established a memorandum of understanding in 2003 with the Environmental Protection Agency (EPA) to coordinate activities relating to EPA's National Environmental Information Exchange Network and CDC's National Environmental Public Health Tracking Network. To date, three collaborative projects have been initiated: (1) a demonstration project in the Atlanta metropolitan area to test data linkage methods and utility of linked data; (2) a project to evaluate how different types of air quality characterization data can be used to link environmental and public health data; and (3) a project in New York to examine specific technical interoperability issues that would affect data exchange between EPA's and CDC's networks.

As envisioned, NEPHTN will be a distributed, secure, Web-based network that will provide access to environmental and health data that are collected by a wide variety of agencies, such as individual state networks. Once established, it should also provide access to environmental, health, and linked environmental-health data from both centralized and decentralized data stores and repositories, implementing a common data vocabulary to support electronic data exchanges within states, and across state, regions, and nationally.

Two Other PHIN Applications Are Not Widely Used, and One Is in Use but Considered Burdensome

Outbreak Management System. The Outbreak Management System is an application designed for case tracking during the investigation of disease outbreaks. Initially developed for use by CDC, the system is now available for use by state and local public health agencies. The project began as the Bioterrorism Field Response Application and was scoped to include only requirements related to bioterrorism response by CDC-deployed field teams. Since its inception in 2002, the scope has been broadened to include any epidemiologic investigation where standard data collection and data sharing would be advantageous. However, although the system is in use at CDC, none of the state and local public health officials with whom we

spoke use the system—either because it cannot exchange data with other software applications, or because these agencies have their own capability for tracing cases of infectious diseases. According to CDC officials, the use of the Outbreak Management System is provided as an option for state and local public health agencies. Although only CDC and one state agency have used the application in support of outbreaks, four state agencies and one federal entity have evaluated the software for potential use and may implement it in the future.

LRN Results Messenger. CDC's LRN Results Messenger utility is used by DHS's BioWatch initiative for transmitting data to CDC; however, it is burdensome to use, according to the BioWatch cities included in our review (BioWatch is discussed in more detail in the next section of this report). According to CDC, it anticipates releasing the next version of the LRN Results Messenger in September 2005, which should address the usability issues.

PHIN Messaging System. The PHIN Messaging System is available for use, but only CDC and a few states and local public health agencies use it. As of March 1, 2005, 51 organizations used it, according to CDC.[18] As yet, only BioWatch, the NEDSS Base System, and the Laboratory Response Network use PHIN Messaging; according to CDC, these are the major systems that support preparedness needs, and it is focusing on these systems first.

Most DHS Biosurveillance IT Initiatives Are Still in Their Early Stages

DHS is also pursuing two major biosurveillance IT initiatives—the National Biosurveillance Integration System and the Biological Warning and Incident Characterization System (BWICS). The BWICS initiative, in addition, is associated with three other biosurveillance programs. Of these five, one is operational, but it has interoperability and other limitations, one is a demonstration project, and three are in development. All five were initially under the oversight of DHS's S&T Directorate; one is now the responsibility of the directorate for Information Analysis and Infrastructure Protection. Table 8 briefly describes the status and plans of DHS's biosurveillance IT initiatives for the current fiscal year.

[18]These locations are primarily public health laboratories and the 10 states that use the NEDSS Base System.

Table 8: Status of DHS Biosurveillance IT Initiatives

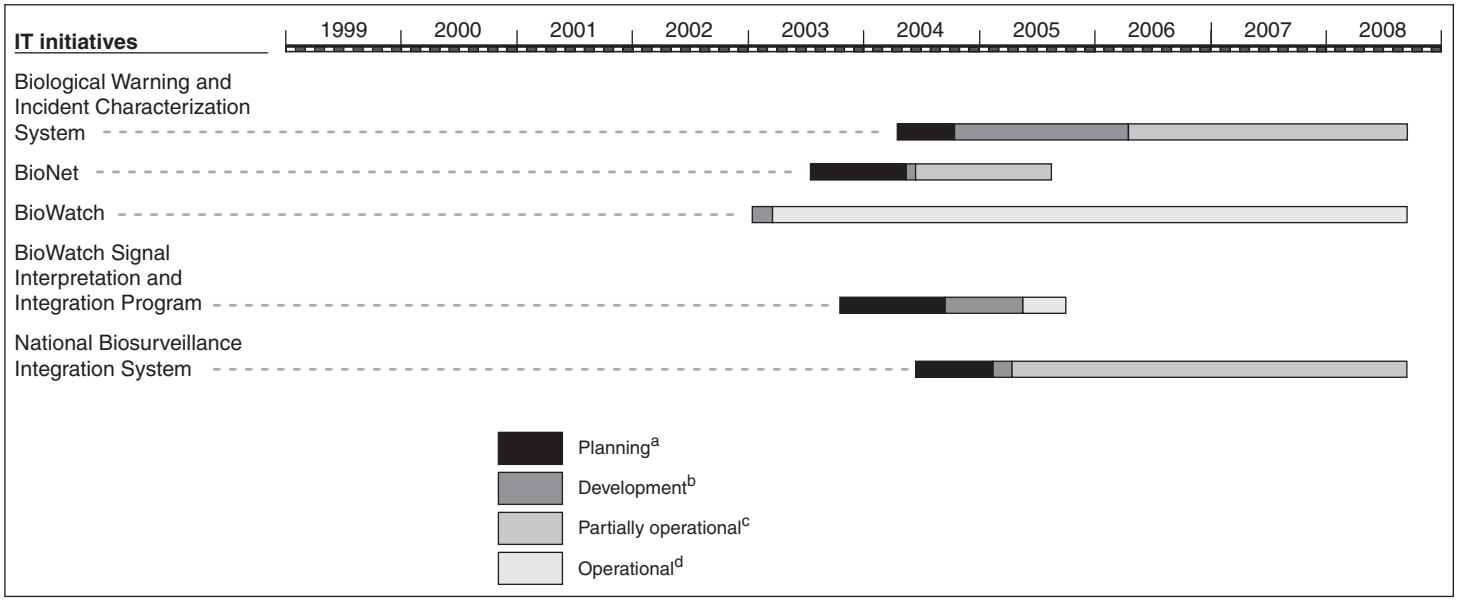
IT Initiative	Status	Users[a]	Future plans
Biological Warning and Incident Characterization System (BWICS)	Development	2 pilot sites	Deploy in phases to BioWatch cities
BioNet	Demonstration	1 pilot site	Complete pilot Transfer lessons learned, tools, templates, and capabilities to BWICS
BioWatch	Operational	Over 30 metro areas	Provide IT enhancements for top threat BioWatch jurisdictions Plan for expansion to additional BioWatch jurisdictions
BioWatch Signal Interpretation and Integration Project	Development	BioWatch locations	Complete pilot underway in one city Transition to BWICS
National Biosurveillance Integration System	Development	Not applicable	Implement systems integration

Source: DHS.

[a]Users include either the number of individuals with access to the system or the number of locations that have installed the software.

Most of DHS's biosurveillance IT initiatives are still being planned or developed. Figure 3 shows time lines for the five DHS IT initiatives.

Figure 3: Estimated Time Lines of DHS Biosurveillance IT Initiatives



Source: GAO analysis of DHS data.

[a]Planning means preparing to design the system or application.

[b]Development means the acquisition or enhancement of the system or application.

[c]Partially operational means that the system or application is functional and being used but not deployed to all installation sites.

[d]Operational means that the system or application is fully deployed.

The one DHS surveillance initiative that is operational—BioWatch—is an environmental monitoring system that was developed and implemented within a 3-month period, according to DHS officials. DHS originally intended for local public health agencies to process and analyze all BioWatch data; however, at CDC's request, DHS agreed to share data with CDC for inclusion in BioSense. BioWatch consists of three IT components:

- One component of BioWatch tracks the environmental samples as they are collected; it was developed by the Department of Energy's Los Alamos National Laboratory.

- A second component performs sample testing and reports the results; this is a commercial product.

- The third component, CDC's LRN Results Messenger, transmits the test results from the laboratory that processes the samples to CDC for analysis.

As deployed, none of these three components could exchange data electronically, so that redundant, manual data entry has been required to transfer data among the three systems. State and local public health officials in BioWatch locations told us that they were dissatisfied with the deployment of BioWatch because of this need for repetitive data entry and because they were not involved in the system's planning and implementation. DHS hired a contractor to resolve BioWatch's interoperability problem, and DHS officials now report that they have begun implementing the resulting technical improvements in BioWatch laboratories.

Additionally, EPA's Inspector General's Office recently reported that the agency did not provide adequate oversight of sampling operations for BioWatch to ensure that quality assurance guidance was adhered to, potentially affecting the quality of the samples taken; DHS officials state that this oversight issue has now been resolved.[19]

In the broader context of environmental monitoring, questions exist about detection capabilities for environmental surveillance. As we reported in May 2003, 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 infection.[20] In May 2004, the Department of Defense reported that the capability for real-time detection of biological agents is currently unavailable and is unlikely to be achieved in the near to medium term.[21]

[19]U.S. Environmental Protection Agency, *EPA Needs to Fulfill Its Designated Responsibilities to Ensure Effective BioWatch Program*, 2005-P-00012 (Washington, D.C.: Mar. 23, 2005).

[20]GAO-03-139.

[21]Department of Defense, *Department of Defense Chemical, Biological, Radiological, and Nuclear Defense Program: Annual Report to Congress* (Washington, D.C.: May 2004).

A second initiative, the BioWatch Signal Interpretation and Integration Program (BWSIIP), was established to respond to user needs regarding BioWatch. According to DHS, the initiative is intended to develop a system that will help BioWatch jurisdictions to better understand the public health or national security implications of a confirmed positive result for a biological agent from BioWatch, as well as to respond appropriately. BWSIIP is to be implemented by a consortium, initiated in 2004, that includes Carnegie Mellon University, the University of Pittsburgh, and the John Hopkins University Applied Physics Laboratory. The current BWSIIP pilot is scheduled for completion in fiscal year 2006. After DHS transitions BWSIIP to the BWICS initiative, local public health agencies will use locally available applications or tools provided by DHS for that function.

For the two remaining major biosurveillance IT initiatives, DHS is still developing requirements (lessons learned from its one demonstration project, BioNet, are being incorporated into BWICS).

- BWICS, is to integrate data from environmental monitoring and health surveillance systems, and the pilot is expected to be completed in fiscal year 2006, according to DHS officials. DHS did not complete requirements development in the two pilot cities as scheduled, and it recently changed one of the original pilot cities, requiring a new start in requirements development in the new location. After the pilot, DHS is planning to expand BWICS beyond the two pilot cities to other BioWatch locations.

- The National Biosurveillance Integration System is intended to connect the various federal surveillance systems to DHS's Homeland Security Operations Center. DHS S&T developed the system requirements and design and transferred the initiative to the Directorate for Information Analysis and Infrastructure Protection in December 2004 for implementation.

Challenges Need to Be Overcome to Strengthen the Information Technology That Supports the Public Health Infrastructure

Despite federal, state, and local government efforts to strengthen the public health infrastructure and improve the nation's ability to detect, prevent, and respond to public health emergencies, important challenges continue to constrain progress. First, the national health care IT strategy and federal health architecture are still being developed; CDC and DHS will face challenges in integrating their public health IT initiatives into these ongoing efforts. Second, although federal efforts continue to promote the adoption of data standards, developing such standards and then implementing them are challenges for the health care community. Third, these initiatives involve the need to coordinate among federal, state, and local public health agencies, but establishing effective coordination among the large number of disparate agencies is a major undertaking. Finally, CDC and DHS face challenges in addressing specific weaknesses in IT planning and management that may hinder progress in developing and deploying public health IT initiatives.

National Health IT Strategy and Architecture to Address Public Health Surveillance Are Still Being Developed

In May 2003, we recommended that the Secretary of HHS, in coordination with other key stakeholders, establish a national IT strategy for public health preparedness and response that should identify steps toward improving the nation's ability to use IT in support of the public health infrastructure. Among other things, we stated that HHS should set priorities for information systems, supporting technologies, and other IT initiatives. Since then, HHS appointed a National Coordinator for Health IT in May 2004 and issued a framework for strategic action in July 2004.[22] This framework is a first step in the development of a national health IT strategy. Goal four of the framework is directed at improvements in public health and states that these improvements require the collection of timely, accurate, and detailed clinical information to allow for the evaluation of health care delivery and the reporting of critical findings to public health officials. Two of the strategies outlined by HHS are aimed at achieving this goal: (1) unifying public health surveillance architectures to allow for the exchange of information among health care organizations, organizations they contract with, and state and federal agencies and (2) streamlining quality and health status monitoring to allow for a more complete look at quality and other issues in real time and at the point of care. The

[22]Department of Health and Human Services, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care* (Washington, D.C.: July 21, 2004).

framework for strategic action states that the key challenge in harmonizing surveillance architectures is to identify solutions that meet the reporting needs of each surveillance function, yet work in a single integrated, cost-effective architecture.

Like the national health care IT strategy, the federal health architecture[23] is still evolving, according to HHS officials in the Office of the National Coordinator for Health IT. Initially targeting standards for enabling interoperability, the federal health architecture is intended to provide a structure for bringing HHS's divisions and other federal agencies together. As part of achieving HHS's public health goal of unifying public health surveillance architectures, the federal health architecture program established a work group on public health surveillance that is responsible for recommending a target architecture related to disease surveillance to serve as the framework within the federal sector for developing and implementing public health surveillance systems. The newly formed work group, chaired by CDC and the Department of Veterans Affairs, met for the first time in December 2004. Because the new work group is so recently formed, plans are still being developed to address how CDC's PHIN initiative and DHS's IT initiatives will integrate with the national health IT strategy, such as plans to establish regional health information organizations.[24]

In the absence of a completed strategy for public health surveillance efforts, state and local public health officials have raised concerns about duplication of effort across federal agencies. Some of the surveillance initiatives in our review address similar functionality and may duplicate ongoing efforts at other federal, state, and local agencies: for example, the use and development of syndromic surveillance systems. CDC is implementing BioSense at the national level, DHS is assisting local public health agencies in implementing local syndromic surveillance systems such as ESSENCE or RODS as part of its biosurveillance initiatives, and many state and local public health agencies have their own ongoing syndromic

[23]The federal health architecture program is intended to define a framework and methodology for establishing a target architecture and standards for interoperability and communication. An architecture describes an entity in both logical terms (e.g., interrelated functions, information needs and flows, work locations, systems, and applications) and technical terms (e.g., hardware, software, data, communications, and security).

[24]HHS's goals and strategies associated with the national health IT strategy are further described in GAO, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005).

surveillance systems. As we have reported, syndromic surveillance systems are relatively costly to maintain compared with other types of disease surveillance and are still largely untested.[25] According to HHS, with regard to BioSense, the agency is taking steps to mitigate costs and risk.

State and local public health officials also expressed concern about the federal government's ability to conduct syndromic surveillance, because they see this type of surveillance as an inherently local function. Furthermore, last year the Council of State and Territorial Epidemiologists[26] reported that while state health departments are given some guidance and leeway to use federal funding to enhance and develop their own disease surveillance activities, no focused mechanism has been established for states to share ideas and experiences with each other and with CDC to determine what has or has not worked, and what efforts are feasible and worth expanding. The Council recommended that to enhance bioterrorism-related surveillance objectives, HHS and CDC form a bioterrorism surveillance initiative steering committee to review current federal surveillance initiatives affecting state and local health departments; to review state-developed surveillance systems; and to recommend surveillance priorities for continuation of funding, further development, or implementation. HHS and CDC have taken steps to respond to these recommendations, but according to the Council, it is not yet satisfied that HHS and CDC have fully addressed its concerns.

While HHS and other key federal agencies are organizing themselves to develop a strategy for public health surveillance and interoperability, decisions regarding development and implementation are being made now without the benefit of an accepted national health IT strategy that integrates public health surveillance-related initiatives. In the case of BioSense, these decisions affect the spending of about $50 million this fiscal year and an unknown amount in future years. Until a strategy and accompanying architecture are developed, major public health IT initiatives will continue to be developed without an overall, coordinated plan and are at risk of being duplicative, lacking interoperability, and exceeding cost and schedule estimates.

[25]GAO, *Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts*, GAO-04-877 (Washington, D.C.: Sept. 30, 2004).

[26]The Council of State and Territorial Epidemiologists is a professional organization of public health epidemiologists from every U.S. state and territory, as well as Canada and Great Britain.

Development and Adoption of Standards an Ongoing Critical Challenge for Health Care

In May 2003, we recommended that the Secretary of HHS, as part of his efforts to develop a national strategy, (1) define activities for ensuring that the various standards-setting organizations coordinate their work and reach further consensus on the definition and use of standards, (2) establish milestones for defining and implementing all standards, and (3) create a mechanism to monitor the implementation of standards throughout the health care industry. 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.[27] As we testified in July 2004, HHS has made progress in identifying standards.[28] While federal action to promote the adoption of these standards continues, the identification and implementation of these standards are an ongoing process.

Despite progress in defining health care IT standards, several implementation challenges remain to be worked out, including the establishment of milestones. Currently, no formal mechanisms are in place to ensure coordination and consensus among 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. Within the federal health architecture structure, the Consolidated Health Informatics initiative is focused on the adoption of data and communication standards to be used by federal agencies to achieve interoperability of IT within health IT initiatives. In March 2003, the Consolidated Health Informatics initiative announced the adoption of 5 standards, and in May 2004, it announced the adoption of another 15 standards. Some of these standards are included as PHIN standards.[29]

[27]GAO-03-139.

[28]GAO, *Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology*, GAO-04-947T (Washington, D.C.: July 14, 2004).

[29]Those included as PHIN standards are (1) Health Level 7 (HL7) messaging, (2) Systemized Nomenclature of Medicine—Clinical Terms (SNOMED), and (3) Logical Observations Identifiers Names and Codes (LOINC). HL7 message format standards provide a protocol that enables the flow of data between systems. SNOMED–Clinical Terms is a nomenclature classification for indexing medical vocabulary, including signs, symptoms, diagnoses, and procedures. LOINC is a set of code standards that covers a wide range of laboratory and clinical subject areas and identifies clinical questions, variables, and reports.

As of March 1, 2005, CDC has adopted several industry standards and published specifications for PHIN; these standards are grouped by type in table 9.

Table 9: Industry Standards Used by the Public Health Information Network

Standard type	Standards
Messaging	Health Level 7 (versions 2, 2.3.1, 2.4, 2.5, 3)
Vocabulary	Logical Observations Identifiers Names and Codes (LOINC) Systemized Nomenclature of Medicine (SNOMED)—Clinical Terms Current Procedural Terminology Medical Subject Headings Multum Devices Multum Drugs North American Industry Classification System Unified Medical Language System International Classification of Disease, 9th edition, Clinical Modification
Data model	Health Level 7 Reference Information Model
Secure data transport	Electronic Business Extensible Markup Language Extensible Markup Language (encryption and digital signature) HyperText Transfer Protocol, secure version
Directory services	Lightweight Directory Access Protocol Directory Service Markup Language
Alerting	Common Alerting Protocol
Security	X.509 Certificates

Source: CDC.

CDC has also initiated a PHIN certification process for its partners (e.g., state and local public health agencies), which is intended to establish whether state and local systems can meet standards for the PHIN preparedness functional areas. In the future, CDC plans to require system owners to first perform self-assessment reviews to ensure that systems meet PHIN standards, followed by reviews by CDC certification teams to confirm PHIN compatibility. To be functionally compatible, systems must be capable of supporting the standards outlined for each PHIN functional area; accordingly, partners must demonstrate that their systems have this capability.

In general, state and local public health officials consider the PHIN initiative to be a good framework for organizing the necessary standards for public health interoperability. Most of the state and local officials we

spoke with agreed that CDC has done a commendable job of adopting and promoting standards for IT in selected programs. In addition, they agreed that CDC should continue to take a leadership role in pressing for industry standards and providing guidance to states and local entities. However, several officials stated that CDC should focus more of its attention on setting standards and less on developing software applications, which generally do not meet their needs and are not compatible with their specific IT environments. CDC officials say that it is important both to promote the use of industry standards and to develop software applications, especially for state and local public health agencies that have limited IT resources.

Although federal efforts to promote the adoption of these standards continue, their identification and implementation are an ongoing process. 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 will not be able to ensure that their systems can exchange data with other systems when needed.

Coordination among Federal, State, and Local Public Health Agencies Is a Major Undertaking

In defining system requirements, federal agencies are challenged by the need to involve such key stakeholders as state and local public health agencies, which are expected to use these systems for reporting data to the federal government. For example, most participating local government agencies and state public health laboratories were told to implement the BioWatch initiative in their metropolitan areas and were given the procedures and software to use for sample management and data collection. According to some public health officials, BioWatch was implemented without a plan for how states and localities would respond to a positive test result, and they were left to develop a response plan after BioWatch had been deployed. One metropolitan area did not implement BioWatch for a year after it became operational, because officials did not have a response plan in place and did not want to be responsible for responding to a potential incident without a plan for handling positive test results. According to DHS officials, since local officials had received funds for emergency preparedness, it was their understanding that BioWatch locations had response plans in place; DHS officials have since developed a methodology to target funds for specific purposes, such as response plans.

CDC has been challenged by the need to coordinate with a diverse range of state and local public health agencies. For example, CDC has found that it is difficult to implement “standard” systems that would address the full

range of different needs and levels of IT resources available at the state level. HHS officials told us that the agency strives to address this challenge by developing applications that are based on industry standards. It also provides the standards and specifications to state and local agencies so that they can build or purchase their own systems that can conform to PHIN standards. Nonetheless, there was consensus among many of the state and local officials in our review that federal agencies did not obtain adequate input from state and local officials. A few state officials with whom we spoke said that CDC does not appropriately consider their need to comply with existing state IT architectures. In addition, in an informal e-mail survey, a small group of state chief information officers agreed that federal agencies do not take into consideration state IT architectures. According to the Council of State and Territorial Epidemiologists, no mechanism has yet been established for state and federal partners to collaboratively review initiatives developed over the past 3 years and plan for the future. Instead, the approach to system design and implementation remains top-down, mainly focused on expanding federally designed syndromic surveillance for early outbreak detection without critical review of its usefulness and cost and without systematic review of state-originated systems and needs. The result is that public health responders may not buy in to and use the federally designed systems, potentially constructive state-originated ideas may not get recognition and wider application, and national bioterrorism-related surveillance will be suboptimal. According to CDC, as part of its efforts to obtain state and local input, it hosts an annual PHIN conference and holds meetings with business partner organizations, such as a recent series of meetings on PHIN preparedness requirements with selected state and local officials. In addition, under CDC's new organizational structure, the new National Center for Public Health Informatics has a division for communications and collaboration with its partners.

Further, CDC and DHS have coordinated with each other on specific projects, but that coordination has not been optimal, according to officials from both agencies. According to DHS officials, federal agencies are planning to meet within the next few months to discuss this issue. When asked about their experiences with coordination between CDC and DHS on public health IT initiatives, some of the state and local public health officials included in our review expressed concerns about coordination between the two agencies; one expressed confusion about their roles.

Until CDC and DHS establish close coordination on federal public health IT, and state and local public health agencies are more actively involved in

the definition and coordination of federal efforts, the effectiveness of the information systems intended to improve disease surveillance and communications may be inadequate.

Rigorous Planning and Management of IT Initiatives Are Important to Building a Stronger Public Health Infrastructure

A challenge that both HHS and DHS face in implementing public health IT initiatives is ensuring their effective planning and management. This requires mature, repeatable systems development and acquisition processes to increase the likelihood that projects will be delivered on time and within budget. Key elements of information and technology management include (1) IT investment management and (2) systems development and acquisition management. To help federal agencies address these key elements, we and the Office of Management and Budget have developed guidance that provides a framework on the use of rigorous and disciplined processes for planning, managing, and controlling IT resources. We have previously reported on specific weaknesses at both HHS and DHS, including the lack of robust processes for IT investment management and immature systems development and acquisition practices.[30] We made recommendations to HHS and DHS aimed at improving these practices.

HHS and CDC have recently taken steps to improve their control over IT projects, which is an important aspect of IT investment management. Because PHIN and some of its initiatives (i.e., BioSense, NEDSS, the Health Alert Network, and NEPHTN) are considered major investments for fiscal year 2006, they required review by HHS. The HHS IT Investment Review Board conducted budgetary reviews for these applications in June 2004 and recommended that the projects move forward as major IT investments; however, there is no documentation that additional HHS reviews were conducted on PHIN and its major applications until this past February, when HHS began implementing procedures for better monitoring of system development projects. In January 2004, CDC announced its intention to provide greater executive level oversight of IT investments, but it had been reorganizing and did not begin conducting control reviews for major PHIN investments until recently. In May 2004, CDC announced its new center for

[30]GAO, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004); *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, GAO-04-49 (Washington, D.C.: Jan. 12, 2004); and *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 2005).

public health informatics to better coordinate IT projects; this center was formally recognized as operational as of mid-April 2005 when Congress approved CDC's reorganization. Until CDC and HHS management provides a systematic method for IT investment reviews, they will have difficulty minimizing risks while maximizing returns on these critical public health investments.

Regarding CDC's systems development and acquisition practices, we observed weaknesses in project management that may hinder progress toward achieving PHIN objectives. For some of the projects in this review, we received limited documentation of project managers' tracking actual dates against baseline schedules, and it appeared that a number of projects had missed internal schedule dates. In November 2004, CDC started requiring project managers to provide status reports to its program management activity office on a biweekly basis. These reports are now required for five of the systems in our review. CDC officials acknowledged that project dates had to be rebaselined; after the rebaselining, CDC officials stated that their projects met official release dates.

Early last year, CDC recognized the need for more direct executive involvement in IT governance and management. This fiscal year, CDC began implementing a project management office to oversee public health informatics projects. Establishing this office and institutionalizing its processes while managing new and ongoing IT projects will be a challenge. The new office has initiated new processes to manage project interdependencies, document and track milestones for projects, and formalize project change requests. For example, the office is beginning to track projects biweekly—asking project managers to report on upcoming milestones, their confidence that those milestones will be met, issues for executive attention, staffing problems, and other potential problems. CDC is also implementing a process to standardize project management across the agency. This process is designed to incorporate, among other things, program and project management, capital planning, security certification and accreditation, and system development life-cycle processes.

DHS has been operational for just over 2 years, and the department has made progress in establishing key information and technology disciplines. However, as we have reported, these disciplines are not yet fully established and operational. For example, DHS has established an IT investment management process, but this process is still maturing. DHS has also had problems consistently employing rigorous systems development and acquisition practices. DHS did not provide

documentation of its oversight of its public health IT investments. According to DHS officials, they plan to submit a capital asset plan and business case for the BWICS initiative this year for review and approval by the DHS IT review board. However, until DHS follows through on its initial actions to address its management, programmatic, and partnering challenges, its IT investments remain at risk.

Conclusions

The federal government has made progress on major public health IT initiatives, but significant work remains to be done. CDC's PHIN initiative includes applications at various stages of implementation; as a whole, however, it remains years away from fully achieving its planned improvement to the public health IT infrastructure. In addition, DHS's initiatives are still in such early stages that it is uncertain how they will improve public health preparedness.

Federal agencies face many challenges in improving the public health infrastructure. CDC and DHS are pursuing related initiatives, but there is little integration among them, and until the national health IT strategy is completed, it is unknown how their integration will be addressed. Implementing health data standards across the health care community is still a work in progress, and until these standards are implemented, information sharing challenges will remain. In addition, state and local public health agencies report that their coordination with federal initiatives is often limited. Until state and local public health agencies are more actively involved in coordination with their federal counterparts, disease surveillance systems will remain fragmented and their effectiveness will be impeded. Finally, the development of robust practices for IT investment management and for systems development and acquisition is a continuing challenge for HHS and DHS, about which we have previously made recommendations. Until agencies address all these challenges, progress toward building a stronger public health infrastructure will be limited, as will the ability to share essential information concerning public health emergencies and bioterrorism.

Recommendations for Executive Action

In order to improve the development and implementation of major public health IT initiatives, we recommend that the Secretary of Health and Human Services take the following two actions:

- ensure that the federal initiatives are (1) aligned with the national health IT strategy, the federal health architecture, and ongoing public health IT initiatives and (2) coordinated with state and local public health initiatives and

- ensure federal actions to encourage the development, adoption, and implementation of health care data and communication standards across the health care industry to address interoperability challenges associated with the exchange of public health information.

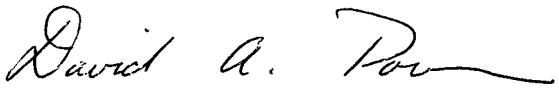
We also recommend that the Secretary of Homeland Security align existing and planned DHS IT initiatives with other ongoing public health IT initiatives at HHS, including adoption of data and communications standards.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Acting Inspector General at HHS and Director of the Departmental GAO/OIG Liaison at DHS (these comments are reproduced in app. III and IV). HHS generally concurred with our recommendations, while DHS did not comment specifically on the recommendations. Both agencies provided additional contextual information and technical comments, which we have incorporated in this report as appropriate. We provided DOD officials with the opportunity to comment on a draft of this report, which they declined.

Among its comments, HHS officials stated that this report does not adequately represent the department's accomplishments in implementing standards and specifications for health IT or the benefits of pursuing a standards-based approach. We concur with HHS on the importance of standards for health information technology and have been calling for federal leadership in expediting standards since 1993. Page 61 lists GAO reports on health IT, several of which address the benefits of standards and the need for a national health IT strategy. In response to HHS's comment that we suggest that early event detection is duplicative or irrelevant at the federal level, neither we nor the state and local public health officials suggest that early event detection at the federal level is irrelevant. Rather, we are reporting the concerns of state and local public health officials regarding the federal government's role, which merits further discussion and more involvement of state and local health officials.

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 of this letter. At that time, we will send copies of the report to other congressional committees. We will also send copies to the Secretaries of Health and Human Services, Homeland Security, Defense, and Energy. In addition, copies will be sent to the state and local public health agencies that were included in our review. Copies will also be made available at no charge on our Web site at www.gao.gov. If you have any questions on matters discussed in this report, please contact me at 202-512-9286 or by e-mail at pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.



David A. Powner
Director, Information Technology Management Issues

Objectives, Scope, and Methodology

The objectives of our review were to

- assess the progress of major federal information technology (IT) initiatives designed to strengthen the effectiveness of the public health infrastructure and
- describe the key IT challenges facing federal agencies responsible for improving the public health infrastructure.

To address these objectives, we conducted our work at Health and Human Services (HHS), Department of Homeland Security (DHS), and Department of Defense (DOD) offices in Washington, D.C., and the Centers for Disease Control and Prevention (CDC) in Atlanta. We selected specific IT initiatives to review from systems we identified in previous work,[1] focusing on major public health IT initiatives in surveillance and communication systems. We excluded food safety systems and DOD disease surveillance systems that did not include civilian populations. We discussed our selection with federal officials to help ensure that we were addressing the most relevant major initiatives. To assess the progress of major federal IT initiatives designed to strengthen the effectiveness of the public health infrastructure, we analyzed agency documents such as Office of Management and Budget's Exhibit 300s, minutes of executive council meetings, and system development documents, including project plans, functional requirements, and cost-benefit analyses. We supplemented our evaluation of agency documents with interviews of federal officials. Through interviews with these officials and with state and local public health officials, we also assessed CDC's and DHS's interaction and coordination with each other on their IT initiatives.

Because these federal initiatives affect state and local public health agencies, we supplemented our analysis of agency documentation by interviewing officials from six state and six local public health agencies on progress being achieved by CDC and DHS. We conducted our work at the San Diego County Health and Human Services Agency; the California Department of Health Services in Sacramento; the Thurston County Public Health and Social Services and the Washington State Department of Health

[1]GAO, *Bioterrorism: Information Technology Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, GAO-03-139 (Washington, D.C.: May 30, 2003).

in Olympia; the Austin/Travis County Health and Human Services Department and the Texas Department of State Health Services in Austin; the Milwaukee City Health Department; the Wisconsin Department of Health and Family Services in Madison, Wisconsin; the Boston Public Health Commission and the Commonwealth of Massachusetts Department of Public Health in Boston; the New York State Department of Health in Albany; and the New York City Department of Health and Mental Hygiene. The states and local public health agencies were selected because they were actively involved in implementing at least one of CDC's Public Health Information Network IT applications. We interviewed them on the impact of federal IT initiatives on state and local public health operations and lessons they learned from integrating federal IT initiatives into their local public health infrastructure. If they had systems similar to the federal systems in our review, we discussed how their systems compared with the federal initiatives. We also interviewed representatives of several public health professional organizations, which CDC considers its partners, such as the National Association of County and City Health Officials, the Association of State and Territorial Health Officials, the Council for State and Territorial Epidemiologists and the Association of Public Health Laboratories. We also had a discussion with the National Association of State Chief Information Officers.

To identify key IT challenges facing federal agencies responsible for improving the public health infrastructure, we analyzed published GAO reports, agency documents, and other information obtained during interviews and site visits. We summarized the results of our evaluation and identified the key challenges that CDC and DHS have consistently encountered as they implement the IT initiatives included in our review.

Our work was performed from July 2004 through April 2005 in accordance with generally accepted government auditing standards.

Federal Agencies and Their Roles in Public Health Preparedness and Response

The **Department of Health and Human Services** (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 following:

- 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. The office maintains a 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.

- The **Centers for Disease Control and Prevention** (CDC) has primary responsibility for nationwide disease surveillance for specific biological agents, developing epidemiological and laboratory tools to enhance disease surveillance, and providing an array of scientific and financial support for state infectious disease surveillance, prevention, and control. CDC has an emergency operations center to organize and manage all of its emergency operations, allowing for immediate communication with HHS, the Department of Homeland Security, 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.

- The **Food and Drug Administration** 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.

- The **Agency for Healthcare Research and Quality** 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 antibioterrorism research. It has initiated several major projects and activities designed to assess and enhance linkages between the clinical care delivery system and the public health infrastructure. 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 among 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 **National Institutes of Health** is responsible, among other things, 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.

- The **Health Resources Services Administration** 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 to state and local governments to support hospitals' efforts toward bioterrorism preparedness and response.

The **Department of Homeland Security** (DHS) is responsible for, among other things, protecting the United States against terrorist attacks. One activity undertaken by DHS is coordination of surveillance activities of federal agencies related to national security.

- The **Science and Technology Directorate** serves as the primary research and development arm of DHS, using our nation's scientific and technological resources to provide federal, state, and local officials with the technology and capabilities to protect the nation. The focus is on catastrophic terrorism—threats to the security of our homeland that could result in large-scale loss of life and major economic impact. The directorate's work is designed to counter those threats, both by

improvements to current technological capabilities and development of new, revolutionary technological capabilities.

- The **Information Analysis and Infrastructure Protection Directorate** is responsible for helping to deter, prevent, and mitigate acts of terrorism by assessing vulnerabilities in the context of continuously changing threats. It strengthens the nation's protective posture and disseminates timely and accurate information to federal, state, local, private, and international partners.

- The **Emergency Preparedness and Response Directorate** is responsible for the National Incident Management System, which establishes standardized incident management processes, protocols, and procedures that all responders—federal, state, local and tribal—will use to coordinate and conduct response actions.

The **Department of Defense**, while primarily responsible for the health and protection of its service members, contributes to global disease surveillance, training, research, and response to emerging infectious disease threats.

- The **Defense Threat Reduction Agency** provides technical expertise and capabilities in combat support, technology development, threat control and threat reduction, including chemical and biological defense.

- The **United States Army Medical Research Institute of Infectious Diseases** conducts biological research dealing with militarily relevant infectious diseases and biological agents. It also provides professional expertise on issues related to technologies and other tools to support readiness for a bioterrorist incident.

The **Department of Energy** is developing new capabilities to counter chemical and biological threats. It expects the results of its research to be public and possibly lead to the development of commercial products in the domestic market.

- The **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.

- The **national research laboratories** (e.g., Lawrence Livermore, Los Alamos, and Sandia) are developing new capabilities for countering chemical and biological threats, including biological detection, modeling, and prediction.

The **Department of Agriculture** (USDA) is responsible for protecting and improving the health and marketability of animals and animal products in the United States by preventing, controlling, and eliminating animal diseases. USDA's disease surveillance and response activities are intended to protect U.S. livestock and ensure the safety of international trade. In addition, USDA is responsible for ensuring that meat, poultry, and certain processed egg products are safe and properly labeled and packaged. USDA establishes quality standards and conducts inspections of processing facilities in order to safeguard certain animal food products against infectious diseases that pose a risk to humans.

- The **Agricultural Research Service** conducts research to improve onsite rapid detection of biological agents in animals, plants, and food and has improved its detection capability for diseases and toxins that could affect animals and humans.

- The **Food Safety Inspection Service** provides emergency preparedness for foodborne incidents, including bioterrorism.

- The **Animal and Plant Health Inspection Service** has a role in responding to biological agents that cause zoonotic diseases (i.e., diseases transmitted from animals to humans). It also has veterinary epidemiologists to trace the source of animal exposures to diseases.

The **Environmental Protection Agency** (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. It is also responsible for protecting the nation's water supply from terrorist attack and for prevention and control of indoor air pollution.

The **Department of Veterans Affairs** (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 VA Emergency Preparedness Act of 2002 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.

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

JUN 3 2005

Mr. David A. Powner
Director
Information Technology Management Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Powner:

Enclosed are the Department's comments on the U.S. Government Accountability Office's (GAO's) draft report entitled, "INFORMATION TECHNOLOGY—Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure" (GAO-05-308). 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,

Daniel R. Levinson

Daniel R. Levinson
Acting 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 U.S. Government Accountability Office reports. OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

COMMENTS OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S REPORT ENTITLED, "INFORMATION TECHNOLOGY—FEDERAL AGENCIES CHALLENGES IN IMPLEMENTING INITIATIVES TO IMPROVE PUBLIC HEALTH INFRASTRUCTURE" (GAO-O5-308)

The Department of Health and Human Services (HHS) appreciates the opportunity to review the Government Accountability Office's (GAO's) draft report.

GAO's Recommendation:

In order to improve the development and implementation of major public health IT initiatives, we recommend that the Secretary of Health and Human Services:

- ***Ensure that the Federal initiatives are: (1) aligned with the National health IT strategy, the Federal health architecture, and ongoing public health IT initiatives; and (2) coordinated with State and local public health initiatives; and***

- ***Ensure Federal actions to encourage the development, adoption, and implementation of health care data and communication standards across the health care industry to address interoperability challenges associated with the exchange of public health information.***

HHS Response:

The Department generally concurs with the two core recommendations as noted in the draft report; however, there are a number of statements and concepts that should be reviewed and adjusted to provide a more accurate representation of public health's IT infrastructure. Therefore, HHS offers the following general comments regarding the draft report.

During the anthrax events of 2001, public health entities exchanged data through faxes, e-mails, and telephone conversations, which lacked effective information technology (IT) to support preparedness and response needs. Today, through the Public Health Information Network (PHIN), public health has an interoperable, standards-based systems architecture that not only enables the secure and reliable electronic exchange of data but also provides specific systems and resources which perform preparedness and response functions for early event detection, outbreak management, the connection of laboratory systems, partner communication and alerting, and countermeasure and response administration.

The PHIN systems implement industry standards such as Health Level (HL) 7, and others, and are ready to work with standards-based electronic health records and other developing components of the nationwide health IT strategy. The draft report does not adequately represent the accomplishments in implementing technical specifications and standards for private, State, local, and HHH/CDC's systems, and the improvements and progress in public health IT since 2001. Readers may not recognize the significant amount of progress that has been made. Moreover, the draft does not reflect Secretary Leavitt's clearly stated strategic

1

commitments, in his recently adopted 500-Day Plan, to expresss a clear vision of health information technology that conveys its benefits to patients, provider and payers; and to convene a national collaboration to further develop, set and certify health information technology standards and outcomes for interoperability, privacy and data exchange. (See http://www.hhs.gov/500DayPlan).

Incorporating an interoperable, standards-based strategy and standards-based systems across a nationwide public health network introduces challenges but provides a greater long-term rate of return in terms of National cost savings and benefits as documented in a recent report on information exchange and interoperability published by the Center for Information Technology Leadership (CITL) http://www.himss.org/ASP/ContentRedirector.asp?ContentId=52848. This report found that, over a 10-year period, a health information exchange approach which is not based on standards could have a nationwide cost of over $34 billion. The CITL report also found that, while using systems which incorporate a standards-based approach, the cost savings could be over $337 billion.

See comment 1.

The GAO draft report focuses on many of the challenges such as longer deployment times associated with a standards-based approach; however, without the recognition of the activities involved in, or benefits of, pursuing a standards-based approach and standards-based systems, readers of the GAO report may not recognize the long-term benefits or even the negative impacts that alternative approaches may have. HHS requests that these benefits be incorporated into the final report to represent the strategy and value which are directly associated with these challenges.

See comment 2.

In several places throughout the draft report, GAO suggests that without a completed nationwide health strategy and accompanying architecture major initiatives are at risk (page 31, paragraph 2, " Health IT Strategy and Architecture to Address Public Health Surveillance Are Still Being Developed"). For the last 4 years, public health has been preparing for and responding to threats that impact the health of U.S. citizens; among these public health threats are Severe Acute Respiratory Syndrome (SARS), West Nile Virus, monkeypox, influenza, and hurricanes. In each event, the evolving IT has provided increasing value to public health, and public health's requirements continue to evolve and inform the overall strategy and architecture.

Because of pressing preparedness needs, public health is working closely with the National Coordinator for Health IT to implement industry standards and standards-based systems that will work with emerging health IT standards. This is a necessary iterative strategy to gain immediate value and strengthen the public health infrastructure and also incorporate standards to facilitate interoperability not only among public health but other Federal and health organizations. For example:

- CDC is implementing HL7-based lab result reporting from 94 of the Laboratory Response Network public health testing labs. These results will use Logical Observation Identifier Names and Codes (LOINC) and Systemized Nomenclature of Medicine (SNOMED) coding and industry standard transport and security. Because of the use of these standards, these results can be delivered to multiple recipients supporting multiple missions.

2

- CDC is implementing HL7-based reportable condition case reports for preparedness related events nationally. CDC has developed over 40 HL7 standard implementation guides and industry standard supportive vocabulary so that suspect and confirmed disease cases can be exchanged between organizations.

  CDC's BioSense data provisioning support will emphasize the use of these industry standards for data exchange in the activities it supports and will, in many instances, take non-standard data formats and convert them to standard data and messaging formats to foster and advance the use of these industry standards in organizations receiving data.

- CDC's BioSense efforts will also foster data mobility in Regional Health Information Organizations (RHIO's) sharing the goals of having transportable electronic health records that can work with a National Health Information Network (NHIN). This point is one of many demonstrating how PHIN-related initiatives support plans to establish RHIO's (page 33).

- CDC's efforts are also supporting HL7 standards-based lab result reporting with SNOMED and LOINC coding from large private clinical laboratories such as LabCorp, Quest, Mayo, and others. These lab results in standard format can be used to support the delivery of electronic lab results to health care delivery organizations, as well as supporting public health organizations.

As supporting evidence of this challenge's impact, the GAO draft report focuses on syndromic surveillance efforts within public health. The draft accurately points out that the Federal Health Architecture's (FHA) public health surveillance working group was formed 6 months ago. However, the report does not mention that a number of FHA workgroups, such as the FHA Interoperability workgroup and Consolidated Health Informatics (CHI), have been in existence for a longer period of time. Through these workgroups, many Federal standards have been established. CDC has actively participated in the formation of these standards, and PHIN and BioSense are fully compatible with the standards of this nationwide Federal architecture. Other organizations' initiatives and software applications may not adhere to these standards but, as in the case of the Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE) and State and local public health applications, CDC is actively working to assist those initiatives in meeting these standards. This example, however, reflects a challenge associated more with adopting standards across a wide and diverse technology base than the absence of a completed strategy. HHS requests that this section of the draft report (page 32) be revised.

See comment 3.

In addition, it is essential to note that early event detection at the local, State, and Federal levels is neither duplicative nor irrelevant at a Federal level as the draft report suggests, but rather mandatory in protecting the public's health. Clearly, there are many who believe that looking at trends in one jurisdiction will not capture multi-jurisdictional events (there are many examples of outbreaks that have only been identified when multi-jurisdictional data have been examined), will not allow for the tracking of a communicable disease, such as SARS, being dispersed through travelers, such as with SARS, and will not allow for National situational

See comment 4.

3

awareness during a major event. When a major event occurs, National decision makers need to understand the size, scope, location and spread of the event. As the event progresses, they need to compare similar data from many different jurisdictions to understand the effectiveness of countermeasures and response. Therefore, HHS requests that this part of the section be deleted.

Finally, the last paragraph of this section (page 34) overstates the urgency of the health architecture challenge. BioSense, as part of the PHIN architecture, is a standards-based, interoperable application that adheres to the Federal health IT strategy, which includes the FHA and CHI standards. The current language asserts that decisions are being made without a strategy in place and that CDC and the National Coordinator are not aligned. As stated in the previous paragraphs, these assertions are not accurate from an HHS perspective. Furthermore, there is no assessment of the risk associated with waiting. Finally, fiscal year (FY) 2006 costs for BioSense are unknown at this time. Therefore, HHS requests that this paragraph be deleted from the final report.

See comment 5.

HHS agrees that it is a challenge to strengthen the National public health infrastructure as the nationwide health IT strategy continues to evolve, but potential and real threats which adversely affect the public's health continue to occur. These technology initiatives assist public health in responding to threats, and the risk of not moving forward in discrete, iterative phases significantly outweighs that of waiting for a completed strategy. HHS suggests that this section does not accurately represent today's environment. Strategic pieces of a nationwide health IT architecture are in place; PHIN preparedness standards are in place; and the two are tracking with each other. Therefore, HHS requests that this section be revised based on the preceding comments.

See comment 6.

Following are key challenges that have been identified by CDC for realizing a nationwide standards-based, interoperable public health network:

- In an emergency, State and local health departments and clinical care sites usually share most data without consistent, mandatory reporting. However:
    - There is large variability in the type and coverage of data that are accumulated at the State and local levels;
    - Baseline data against which the emergency data trends need to be compared for situational awareness are largely unavailable; and
    - The processes and technical infrastructure to exchange the emergent data versus the routine data are so different that substantial technical and data work need to occur during each emergency causing a loss of critical time.
- Public health's role in preparedness and response has been perceived as limited to data collection and communications. Public health plays a far larger role, not only in detecting the event, but in managing, containing, and mitigating the event and its impact of events on the public. This larger role includes early event detection, outbreak

4

management, countermeasure response and administration, laboratory results exchange, and partner communication and alerting.

- Some organizations do not invest in solutions that are standards-based. As a result, interoperability among different partners is significantly impeded, and information and data, two items essential to decision makers in an emergency, are often not exchanged in the most efficient and time-sensitive manner.

5

The following are GAO's comments on the Department of Health and Human Services letter dated June 3, 2005.

GAO Comments

1. We agree with HHS that the cost benefits of a standards-based approach to public health systems are potentially considerable. However, as we have reported before, the Center for Information Technology Leadership acknowledges that their cost estimates are based on a number of assumptions and inhibited by limited data that are neither complete nor precise.[1]

2. We agree with HHS that standards-based systems provide important benefits. In our May 2003 report, we made several recommendations regarding the establishment and use of standards that are highlighted in this report. We also state that 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.[2]

3. HHS states that our report does not mention a number of activities related to the Federal Health Architecture and the Consolidated Health Informatics initiative. We described the status of workgroup efforts specific to public health surveillance. In terms of the standards adopted by the Consolidated Health Informatics initiative, we presented the relevant standards in our table of industry standards used by the Public Health Information Network. We disagree with HHS that the paragraph needs to be revised. While the development of standards and policies is a key component of progress toward the implementation of a national health IT strategy, the development of a national strategy and corresponding federal architecture is equally important.

4. We disagree with HHS that we should delete our discussion of the concerns of state and local public health officials regarding duplication of effort across federal agencies. Neither we nor the state and local public health officials suggest that early event detection at the federal

[1]GAO, *Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology*, GAO-05-309R (Washington, D.C.: Feb. 17, 2005).

[2]GAO-03-139.

level is irrelevant. Rather, we are reporting the concerns of state and local public health officials regarding the federal government's role, which merits further discussion and more involvement of state and local health officials.

5. We have adjusted our report to indicate that fiscal year 2006 costs for BioSense are unknown.

6. HHS comments that not moving forward with its technology initiatives presents greater risk than waiting for a completed national health IT strategy. We are not suggesting that HHS stop its ongoing activities; we only point out the risks associated with developing and implementing major IT initiatives without a coordinated strategy in place.

Comment from the Department of Homeland Security

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

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 3, 2005

Mr. David A. Powner
Director
Information Technology Management Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Powner:

Thank you for the opportunity to comment on GAO's draft report entitled, "Information Technology: Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure," GAO-05-308. Under separate cover we have provided extensive technical comments which we trust you will incorporate in the final report for clarity and to reflect the current state of the information technology (IT) initiatives being undertaken in the Department's Science and Technology (S&T) Directorate.

The Department of Homeland Security (DHS) has just two overarching IT initiatives within the S&T Directorate. The first of these is the Biological Warning and Incident Characterization System (BWICS), which is to be the baseline BioWatch signal interpretation tool and will be deployed to all BioWatch cities. BWICS, once implemented, will link to both BioSense and the National Biosurveillance Integration System (NBIS). BioWatch (a component of BWICS) is not an IT system but rather, an environmental monitoring system for biological threat agents that uses an IT system for sample tracking, laboratory analysis, and data transmission to the Center for Disease Contol (CDC). BioWatch Signal Interpretation and Integration Program (BWSIIP) is an effort that was initiated earlier to deploy some electronic medical surveillance tools to a BioWatch city to aid in signal interpretation. Once this effort is completed this fiscal year it will transition into BWICS, providing some of the medical surveillance tools to be used in the broader portfolio of BWICS signal interpretation tools. The second of S&T's IT initiatives is NBIS, which will integrate a much larger set of biosurveillance information across the nation from sector specific agencies; not just in BioWatch cities. As noted earlier, BWICS will be one of many feeds into NBIS.

In the report, the term "biosurveillance" should be defined better because this word has different connotations. NBIS collects medical, environmental, and intelligence data, but in BWIC, it is not DHS's goal to develop medical biosurveillance systems but to use existing ones, either from locally existing systems or CDC, to provide health related syndromic data and information to assist in BioWatch signal interpretation and incident characterization. The draft report is erroneous in stating that our "…initiatives are still in such early stages that it is uncertain how they will improve public health preparedness". BioWatch, which was initially deployed in January of 2003, has been in existence for over 2 years and provides the

See comment 1.

www.dhs.gov

ability for rapid biothreat detection prior to the presentation of clinical symptoms for rapid intervention. This initiative currently provides protection for a considerable percentage of the population with the potential to significantly minimize the mortality and morbidity associated with an intentional release of a biothreat agent into the environment. However, it is important to note that BioWatch is only one of the tools decision makers will use to understand or reconstruct a bioterrorist event. Several scenario-driven system studies have reinforced the utility of coupling biomonitoring data with biosurveillance data, sampling plans and strategies, and plume modeling to provide a better understanding of the target agent that was released, the method of release, its viability and degradation rate in the environment, etc. Assembling and analyzing this information will prove to be extremely beneficial in determining the affected areas/regions and population for rapid intervention, consequence management, remediation and restoration. Furthermore, BioWatch is designed to detect medium to large-scale release/attacks; medical biosurveillance data from federal and local sources will greatly assist in BioWatch signal interpretation and in capturing or serving as indicators for smaller scale release/attacks which could be missed by the BioWatch system.

Due to the urgencies and importance of protecting the citizens of United States from a potential biological attack, DHS was requested to quickly deploy BioWatch, a research and development program at the time. Its primary goal was to provide rapid biodetection capability for rapid intervention to minimize mortality and morbidity and not interoperable IT systems due to time limitations. It is also important to note that DHS has been fully aware of the importance of an interoperable IT system to support such an extensive and complex architecture to provide nationwide biothreat coverage from the very beginning. The systematic approach taken by DHS was to initially deploy BioWatch and then follow through to address the deficiencies and to provide the appropriate tools for incident characterization and reconstruction, which currently is being addressed and accomplished through coordination and collaboration with the local BioWatch public health programs and environmental protection communities.

We thank you again for the opportunity to provide comments on this draft report and look forward to working with you on future homeland security issues.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison

The following is GAO's comment on the Department of Homeland Security's letter dated June 3, 2005.

GAO Comment

1. We disagree with DHS's statement that we erroneously categorize its initiatives as still in the early states. The initiatives that we are referring to as being in the early stages are the Biological Warning and Incident Characterization System and the National Biosurveillance Integration System, which according to DHS officials are considered their two major IT initiatives. DHS categorized them as being in development.

GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, 202-512-9286, pownerd@gao.gov

Staff Acknowledgments

In addition to those named above, Barbara S. Collier, Neil J. Doherty, Amanda C. Gill, M. Saad Khan, Gay Hee Lee, Mary Beth McClanahan, M. Yvonne Sanchez, and Morgan Walts made key contributions to this report.

Related GAO Reports on Health Information Technology

Health Information Technology: HHS Is Taking Steps to Develop a National Strategy. GAO-05-628. Washington, D.C.: May 27, 2005.

Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology. GAO-05-309R. Washington, D.C.: February 17, 2005.

HHS's Efforts to Promote Health Information Technology and Legal Barriers to its Adoption. GAO-04-991R. Washington, D.C.: August 13, 2004.

Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology. GAO-04-947T. Washington, D.C.: July 14, 2004.

Information Technology: Benefits Realized for Selected Health Care Functions. GAO-04-224. Washington, D.C.: October 31, 2003.

Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies. GAO-03-139. Washington, D.C.: May 30, 2003.

Automated Medical Records: Leadership Needed to Expedite Standards Development. GAO/IMTEC-93-17. Washington, D.C.: April 30, 1993.

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548