AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# BATTLING BIOTERRORISM: WHY TIME INFORMATION-SHARING BETWEEN LOCAL, STATE AND FEDERAL GOVERNMENTS IS THE KEY TO PROTECTING PUBLIC HEALTH

## HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

DECEMBER 14, 2001

**Serial No. 107–132**

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

82–632 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

## COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

### SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

THOMAS M. DAVIS, Virginia, *Chairman*

JO ANN DAVIS, Virginia
STEPHEN HORN, California
DOUG OSE, California
EDWARD L. SCHROCK, Virginia

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii

### EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

MELISSA WOJCIAK, *Staff Director*
HOWARD DENIS, *Professional Staff Member*
TEDDY KIDD, *Clerk*
DAVID RAPALLO, *Minority Counsel*

# CONTENTS


Page

Hearing held on December 14, 2001 ..... 1

Statement of:

Baker, Edward, M.D., M.P.H., Director of Public Health Practice Program Office, accompanied by Kevin Yeskey, M.D., Acting Director, Bioterrorism Preparedness and Response Program, National Center for Infectious Diseases ..... 8

Regan, Rock, National Association of State Chief Information Officers, chief information officer, State of Connecticut; Gianfranco Pezzino, M.D., MPH, Council for State and Territorial Epidemiologists, State epidemiologist, Kansas Department of Health and Environment; Paul Wiesner, M.D., MPH, National Association of County and City Health Officials, director, DeKalb County Board of Health; Michael H. Covert, American Hospital Association, president, Washington Hospital Center; Carol S. Sharrett, M.D., MPH, director of health, Fairfax County Department of Health; and Charles E. Saunders, M.D., president, EDS Health Care Global Industry Group ..... 36

Letters, statements, etc., submitted for the record by:

Baker, Edward, M.D., M.P.H., Director of Public Health Practice Program Office, prepared statement of ..... 11

Covert, Michael H., American Hospital Association, president, Washington Hospital Center, prepared statement of ..... 69

Pezzino, Gianfranco, M.D., MPH, Council for State and Territorial Epidemiologists, State epidemiologist, Kansas Department of Health and Environment, prepared statement of ..... 47

Regan, Rock, National Association of State Chief Information Officers, chief information officer, State of Connecticut, prepared statement of .... 39

Saunders, Charles E., M.D., president, EDS Health Care Global Industry Group, prepared statement of ..... 83

Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of ..... 5

Wiesner, Paul, M.D., MPH, National Association of County and City Health Officials, director, DeKalb County Board of Health, prepared statement of ..... 56

# BATTLING BIOTERRORISM: WHY TIME INFORMATION-SHARING BETWEEN LOCAL, STATE AND FEDERAL GOVERNMENTS IS THE KEY TO PROTECTING PUBLIC HEALTH

---

**FRIDAY, DECEMBER 14, 2001**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY,
COMMITTEE ON GOVERNMENT REFORM,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Hon. Thomas M. Davis (chairman of the subcommittee) presiding.

Present: Representatives Tom Davis of Virginia, Horn, and Turner.

Also present: Representative Shays.

Staff present: Melissa Wojciak, staff director; Amy Heerink, chief counsel; George Rogers, counsel; Howard Denis and Victoria Proctor, professional staff members; Teddy Kidd, clerk; David Rapallo, minority counsel; and Jean Gosa, minority assistant clerk.

Mr. TOM DAVIS OF VIRGINIA. Good morning. Welcome to today's hearing on the information-sharing capabilities of the Center for Disease Control and Prevention, hereinafter the CDC, for responding to a bioterrorism threat. This hearing will review the CDC's March 2001 report, "Public Health's Infrastructure: Every Health Department Fully Prepared, Every Community Better Protected."

The best initial defense against public health threats, whether naturally occurring or deliberately caused, continues to be accurate, timely recognition and reporting of problems.

To that end, one of our top priorities must be to ensure that we have a strong information-sharing network that protects privacy while seamlessly connecting local, State and Federal Governments. Moreover, timely and easy access to information is key to applying effective countermeasures.

However, the CDC report noted serious deficiencies in the timely distribution of information between Federal, State and local governments in response to critical public health threat.

The March 2001 report outlined a number of goals for improving communication and information technology capabilities at the Federal, State and local level. The hearing today will examine our progress to date in meeting the goals set forth in that report and the timeframes for reaching our, as yet, unmet goals.

Additionally, it will discuss lessons learned from the recent events related to the anthrax incidents in October and November of this year as well as existing pilot programs on the Health Alert Network and the National Electronic Disease Surveillance System.

The hearing today will also review best practices for information-sharing among Federal, State and local entities to determine our next steps for responding to future bioterrorism crisis. The recent anthrax attacks shows the need to improve information-sharing capabilities of the disparate Federal, State and local health authorities as well as private hospitals in the event of a public health emergency.

Both basic IT infrastructure and communication protocols must be clarified in order to achieve the efficient system necessary to effectively respond to an emergency.

There is borne out by CDC's estimate that currently only 68.1 percent of U.S. counties have high speed-Internet access and can receive a broadcast message. Moreover, only 13 States have high-speed Internet connections with all of their counties.

Originally, CDC's goal, as stated in their March 2001 report, was to ensure by 2010 that all health departments have continuous high-speed access to the Internet and have established standard protocols for data collection, transport, electronic reporting, and information exchange to protect privacy while seamlessly connecting, local, State and Federal data systems; to have immediate on-line access to current global health recommendations, health and medical data, treatment guidelines and information on the effectiveness of public health interventions; and to have the capacity to send and receive sensitive health information via secure electronic systems and to broadcast emergency health alerts.

In the wake of recent events, the CDC is considering ways to accelerate the timetable for implementation of the recommendations in its March report, ahead of the original 2010 target date.

In addition, CDC has developed tools for States to perform a self-assessment of information-sharing capabilities. It has begun to work to develop a grant program to implement these tools, identify gaps and develop a plan that includes a joint State-local strategy to fill these gaps.

Additionally, three ongoing CDC initiatives—the Health Alert Network, Epi-X, and the National Electronic Disease Surveillance System—are being used to achieve the recommendations listed above.

The Health Alert Network [HAN], is a nationwide program to establish the communications/information distance learning organizational infrastructure needed to respond to public health emergencies. It will link local health departments to one another and to other organizations critical for preparedness and response. Its features include providing to State and local health officials high-speed, secure Internet connections, on-line access to CDC's prevention recommendations, practice guidelines and disease data; the capacity to transmit secure surveillance, laboratory and other sensitive data and access to distance learning programs and services, and early warning and alert broadcasts.

Moving forward, it is going to be necessary to determine what current Federal telecommunications development programs can be

used in conjunction with the CDC initiatives to facilitate necessary improvement in the public health IT infrastructure nationwide.

Finally, the subcommittee will review the effect media reporting played in the public health community's response to anthrax incidents.

As public health professionals attempted to provide warnings and guidance based on traditional epidemiological methods, they often found themselves outpaced by constant media reports. Timely and accurate transmission of information to the general public will be a vital communication objective in future health emergencies.

Recent events have shown the slim margin of error in this area before public mistrust begins to take hold. Thus, future communication plans must take into account the role the media will play in shaping public reaction and ensuring the correct message emerges immediately from those responsible for making health policy decisions.

The subcommittee today is going to hear testimony from Dr. Edward Baker and Dr. Kevin Yeskey of the CDC. We will also hear from Mr. Rock Regan of the National Association of State Chief Information Officers; Dr. Gianfranco Pezzino, of the Council of State and Territorial Epidemiologists; Dr. Paul Wiesner of the National Association of County and City Health Officials; Mr. Michael Covert of the American Hospital Association; Dr. Carol Sharrett of the Fairfax County Department of Health; and Dr. Charles Saunders, EDS Health Care Global Industry Group.

I now yield to Congressman Turner for any statement that he may wish to make.

Mr. TURNER. Thank you, Mr. Chairman; and thank you for hosting the hearing today on this very critical subject. And I welcome all of our witnesses who have come to share with us the progress that we are making in this area.

There is no question, based on what the Centers for Disease Control report told us just a few months ago, that we have serious deficiencies in our public health system in our effort to deal adequately with the threat coming from biological agents.

The recent experience with anthrax, I think, underscores the need to be very aggressive with regard to this particular area. I noted in the CDC report that it concluded that public health agencies lacked basic equipment, such as computers and Internet connections, as Chairman Davis mentioned. It mentioned that many of our public health laboratories are old, outdated and unsafe. It also acknowledged that many of our physicians and other health professionals across the country are ill-equipped and untrained to deal with the new threats.

Our Nation long ago understood that we had to be ready to respond to nuclear attack, and our early warning systems, now, that have been in place for a number of years, enable us as a nation to respond almost immediately to the threat of a nuclear missile attack.

We need to have the same capability with regard to a biological attack. And much less is understood or known about those threats by the American people. And I think our purpose here today is to

explore the progress we are making, and to determine the direction that we need to go with regard to that very serious threat.

So I welcome all of our witnesses today. Thank you for coming and we look forward to hearing from you.

[The prepared statement of Hon. Jim Turner follows:]

**Opening Statement**
**Representative Jim Turner**

**Ranking Member**
**Subcommittee on Technology and Procurement Policy**

December 14, 2001

---

GOOD MORNING. LET ME WELCOME OUR WITNESSES FROM THE C.D.C., AS WELL AS OUR DISTINGUISHED WITNESSES FROM THE VARIOUS ORGANIZATIONS IN THE SECOND PANEL. I AM GLAD YOU ALL COULD BE WITH US TODAY.

EARLIER THIS YEAR, C.D.C. ISSUED A REPORT THAT RAISED CONCERNS WITH THE COMMUNICATIONS INFRASTRUCTURE WITHIN OUR HEALTHCARE SYSTEM. THE REPORT MADE THE FOLLOWING CONCLUSIONS:

> OUR LOCAL PUBLIC HEALTH AGENCIES LACK BASIC EQUIPMENT, SUCH AS COMPUTERS AND INTERNET CONNECTIONS. OUR PUBLIC HEALTH LABORATORIES ARE OLD AND UNSAFE. OUR STATE AND LOCAL HEALTH DEPARTMENTS DO NOT HAVE THE CAPACITY TO INSTITUTE PROVEN INTERVENTION STRATEGIES . . . . OUR PUBLIC HEALTH PHYSICIANS AND NURSES ARE UNTRAINED IN NEW THREATS LIKE WEST NILE VIRUS AND WEAPONIZED MICROORGANISMS.

THE C.D.C. REPORT MADE SEVERAL RECOMMENDATIONS TO IMPROVE THIS SITUATION, AND MOVING FORWARD ON THESE STEPS HAS BECOME AN URGENT TASK IN LIGHT OF THE SEPTEMBER 11 ATTACKS. C.D.C. HAS DEVELOPED TOOLS FOR STATES TO PERFORM SELF ASSESSMENTS, FOR EXAMPLE, AND THEY HAVE DEVELOPED GRANT PROGRAMS FOR STATES TO IDENTIFY AND ADDRESS DEFICIENCIES IN THEIR SYSTEMS.

IN ADDITION, I LOOK FORWARD TO A FULL UPDATE ON THE PROGRESS OF THREE OTHER C.D.C. COMMUNICATIONS INITIATIVES: THE HEALTH ALERT NETWORK, THE EPIDEMIC INFORMATION EXCHANGE, AND THE NATIONAL ELECTRONIC DISEASE SURVEILLANCE SYSTEM.

DESPITE THIS PROGRESS, HOWEVER, SOME OBSERVERS HAVE EXPRESSED DISSATISFACTION WITH THE APPROACH TO DATE.

DR. JOSEPH WAECKERLE, FOR EXAMPLE, TESTIFIED TWO WEEKS AGO ON BEHALF OF THE AMERICAN COLLEGE OF EMERGENCY PHYSICIANS. HIS COMMENTS WERE DELIVERED BEFORE ANOTHER SUBCOMMITTEE WITHIN THE GOVERNMENT REFORM COMMITTEE — THE NATIONAL SECURITY SUBCOMMITTEE. DR. WAECKERLE OFFERED THESE CONCLUSIONS:

BIOLOGIC TERRORISM, IN MY OPINION, HAS THE POTENTIAL TO BE THE DOOM OF MANKIND, NOW AND INTO THE FUTURE . . . AND I THINK THAT IT REQUIRES AN APPROPRIATE STRATEGY AND RESPONSE . . . .

THERE IS ONE MAJOR FAULT THAT I BELIEVE WE NEED TO FOCUS ON . . . . TO DATE, DESPITE NUMEROUS COMMITTEE HEARINGS AND MUCH WRITING AND RHETORIC, THE LOCAL COMMUNITY AND THOSE KEY PLAYERS HAVE NOT BEEN INTEGRATED OR COORDINATED WITH ANY NATIONAL PROGRAMS AND THEY HAVE NO INPUT. AND I WOULD HOPE THAT WHEN WE TALK ABOUT COMMUNICATION WITH THE PUBLIC AND CRISIS COMMUNICATION, WE REMEMBER THAT . . . COMMUNICATION BETWEEN THE FEDERAL FAMILY AND THE LOCAL AND STATE PARTNERS . . . HAS BEEN NEGLECTFUL AND IT NEEDS TO BE GREATLY IMPROVED.

WITH THIS IN MIND, I LOOK FORWARD TO HEARING FROM DR. BAKER ABOUT HIS REPORT, ABOUT THE RECOMMENDATIONS CONTAINED WITHIN THE REPORT, AND ABOUT THE C.D.C. RESPONSE TO OBSERVERS LIKE DR. WAECKERLE.

THANK YOU, MR. CHAIRMAN.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. We are also joined today by another subcommittee chairman on the Government Reform Committee, Mr. Horn from California. Any comments?

Mr. HORN. I listened to your eloquence and to Mr. Turner's eloquence, and I am ready to listen to the witnesses. So thanks for putting the hearing together.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

I call our first panel of witnesses to testify. As you know, it is the policy of this committee that all witnesses be sworn when you testify. Would you please rise with me and raise your right hands.

[Witnesses sworn.]

Mr. TOM DAVIS OF VIRGINIA. To afford sufficient time for questions of the witnesses, I would like you to try to stay at 5 minutes. Each of you has a green light there. When it turns yellow, you have a minute to sum up. We have your complete statement, and that is included in the record.

So we will start with Dr. Baker.

**STATEMENT OF EDWARD BAKER, M.D., M.P.H., DIRECTOR OF PUBLIC HEALTH PRACTICE PROGRAM OFFICE, ACCOMPANIED BY KEVIN YESKEY, M.D., ACTING DIRECTOR, BIOTERRORISM PREPAREDNESS AND RESPONSE PROGRAM, NATIONAL CENTER FOR INFECTIOUS DISEASES**

Dr. BAKER. Good morning, Mr. Chairman and members of the subcommittee. I am Dr. Edward Baker. I serve as Director of CDC's Public Health Practice Program Office. With me today is Dr. Kevin Yeskey, who currently serves as Director of our Bioterrorism Preparedness and Response Program. Thank you for this invitation.

And, as you know, increased vigilance and preparedness for unexplained illnesses and injuries are an essential part of the public health effort to protect our citizens against terrorism and other public health threats. The terrorist events on and since September 11th have been defining moments for all of us, and they have greatly sharpened our Nation's focus on public health.

Even before the September 11th attack, CDC was making substantial progress to define, develop, and implement nationwide a set of strategies and capacities required at the local, State and Federal level to prepare for and to respond to deliberate attacks on the health of our citizens. Since September 11th, we have worked very closely with our public health partners to accelerate these efforts, to share critical lessons learned, and to identify seven specific high-priority areas for immediate strengthening. We are committed to working with you and others to increase our efforts even further in the months ahead.

As you know, CDC serves as a trusted source of scientific information on emerging infectious diseases and many other public health threats. Since September 11th, CDC has issued 175 updates in response to the terrorist attacks and anthrax investigations through a variety of communications channels reaching an estimated 7 million health professionals in the public.

These have included our rapid communications systems, the bioterrorism Web site, which is www.bt.cdc.gov, nationwide satellite

broadcasts through our public health training network, and special telephone hot lines. This level of communication and collaboration with our partners has been crucial to the investigation and response to these events.

But improvements can be made as called for in CDC's report, which you, Mr. Chairman, referred to a moment ago, the report entitled Public Health's Infrastructure: A Status Report.

The specific recommendations regarding information systems are being achieved through three major initiatives that you referred to a moment ago—the Health Alert Network, the National Electronic Disease Surveillance System and Epidemiologic Information Exchange, or as we call it Epi-X. I would like to describe each of these briefly.

The Health Alert Network, as you mentioned earlier, is designed to be the Nation's rapid on-line system for health communications information and training. When fully deployed, the Health Alert Network will link all local, State, and Federal public health agencies to each other and to their community partners, private health care providers, and will serve as an electronic platform for the applications that I have mentioned.

On the morning of September 11th, the Health Alert Network was fully activated within 4 hours of the attack on the World Trade Center. We issued an alert to top public health officials across the country, and in the ensuing 12 weeks, some 60 alerts, advisories and updates have been distributed through the network.

To date, as you mentioned a moment ago, 13 States have directly connected all of their counties electronically to the Health Alert Network via high-speed, continuous Internet communications; and 68 percent of all U.S. counties are now connected.

The Epidemiologic Information Exchange, or Epi-X, is CDC's secure, Web-based communications system, which serves as a portal for private electronic exchange of epidemiologic information. In response to the attacks of September 11th and subsequent events, the Epi-X system has immediately provided secure communications among State and large city epidemiologists and CDC programs, including our Epidemiologic Intelligence Service.

The National Electronic Disease Surveillance System is a visionary system which will be built on the platform of the Health Alert Network. It is targeted toward electronic, real-time reporting of information for public health action. It is designed to provide an integrated, coherent national system for public health surveillance that will have the flexibility and capacity to support a wide range of public health efforts, including our emergency response.

So what have we learned from these recent events? We have learned many lessons. First of all, that these unprecedented events have given us a chance to work and prepare for the next challenge with a deeper understanding of bioterrorism and how we share information.

We have learned that linkages that we have forged between clinical and public health communities are strong, and that these linkages have saved lives by detecting disease early.

We have learned how to shorten the time lag between acquiring new knowledge, communication and action; and we have confirmed

that close collaboration between local, State and Federal officials builds confidence in our local response.

And finally we have learned more about what information is valuable to the public and to our partners, and that will help us craft messages and materials in the future.

In conclusion, we have made substantial progress to date in enhancing the Nation's capability to prepare for and to respond to a bioterrorist event, but there is much more to be done. The best public health strategy to protect citizens against terrorism is the development, organization, enhancement of public health prevention systems and tools, including enhanced communications systems and messages.

Not only will this approach ensure that we are better prepared for a bioterrorism event, but it will also enable us to do our jobs better every day. A strong and flexible public health infrastructure is the best defense against any disease threat.

Thank you very much for your attention and for your leadership in bringing this issue to national attention.

Dr. Yeskey and I are happy to address any of your questions. Thank you.

[The prepared statement of Dr. Baker follows:]

**Testimony**
**Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform**
**United States House of Representatives**

# Bioterrorism Preparedness: CDC Efforts to Improve Public Health Information at Federal, State, and Local Levels

*Statement of*
**Edward L. Baker, M.D., M.P.H.**
*Director, Public Health Practice Program*
*Office Centers for Disease Control and Prevention*
*Department of Health and Human Services*

**For Release on Delivery**
**Expected at 10:00 am**
**on Friday, December 14, 2001**

Good morning Mr. Chairman and Members of the Subcommittee. I am Dr. Edward L. Baker, Director of the Public Health Practice Program Office at the Centers for Disease Control and Prevention (CDC). With me today is Dr. Kevin Yeskey, Acting Director of the Bioterrorism Preparedness and Response Program, National Center for Infectious Diseases, CDC. Thank you for the invitation to discuss CDC's public health response to the threat of bioterrorism, specifically our role in building a strong public health infrastructure to improve public health information at the local, state, and Federal levels.

As has been highlighted recently, increased vigilance and preparedness for unexplained illnesses and injuries are an essential part of the public health effort to protect our citizens against bioterrorism and other health threats. The terrorist events on and since September 11th have been defining moments for all of us – and they have greatly sharpened the Nation's focus on public health. Even before the September 11th attack on the United States, CDC was making substantial progress to define, develop, and implement nationwide a set of public health capacities required at all levels–local, state, and Federal–to prepare for and respond to deliberate attacks on the health of our citizens. Since September 11th we have worked very closely with our public health partners to accelerate our efforts, share critical lessons learned, and identify seven high priority areas for immediate strengthening. We are committed to increasing our efforts ever further in the coming months to ensure that every health department is fully prepared and every community better protected against such threats.

**Public Health Leadership**

The Department of Health and Human Services' (DHHS) antiterrorism efforts are focused on five key strategies: (1) improving the nation's public health surveillance and electronic communications systems to quickly detect and identify the biological or chemical agents that have been released; to track and map the spread of disease; and to report and disseminate information as rapidly as possible; (2) strengthening the capacities for medical and public health response at both the state and local level; (3) expanding the stockpile of pharmaceuticals for use when needed; (4) regulating the shipment of hazardous biological agents or toxins; and (5) expanding research on disease agents that might be released, including rapid methods for identifying biological and chemical agents, and improved treatments and vaccines.

As the nation's disease prevention and control agency, it is CDC's responsibility, on behalf of DHHS, to provide national leadership in the public health and medical communities in a concerted effort to detect, diagnose, respond to, and prevent illness and injury, whether occurring naturally or as a result of a deliberate act. This task is an integral part of CDC's overall mission to monitor and protect the health of the U.S. population and has been described in detail in such reports as CDC's 1998 plan, *Preventing Emerging Infectious Diseases: A Strategy for the 21st Century*. This plan, developed with input from state and local health departments, disease experts, and partner organizations such as the American Society for Microbiology, the Association of Public Health Laboratories, the Council of State and Territorial Epidemiologists, and the Infectious Disease Society of America, emphasizes the need to be prepared for the unexpected – whether it is a naturally occurring influenza pandemic or the deliberate release of smallpox by a terrorist.

Fundamental to this plan–and to all preparedness efforts–is a strong national public health infrastructure. Like our military system, our public health system must be at a constant state of "battle readiness," with a skilled professional workforce, robust information and communication systems, and a strong network of local, state, and Federal agencies and laboratories, effectively linked and working together.

Recognizing the importance of the nation's public health infrastructure as our first line of defense, Congress requested in FY2000 that CDC assess the current state of the infrastructure and make recommendations on possible actions that could be taken to strengthen key components. In response, in March 2001, CDC released the report *Public Health's Infrastructure: A Status Report,* developed in collaboration with national and international public health associations and officials at the local, state, and Federal levels. This report outlined 10 key recommendations for improving the public health infrastructure, building on the goals previously identified in *Healthy People 2010.* As the Committee requested, I will describe CDC's approach and strategies for achieving these goals with our public health partners, with a special emphasis on improved information and communication systems.

One of the anchors of our defense against bioterrorism continues to be accurate information regarding how to recognize a potential threat and knowledge of appropriate actions. CDC serves as a trusted source of scientific information on emerging infectious diseases and other public health threats and works with our private and public partners to communicate disease prevention information to state and local health departments, health professionals, and the public. Since September 11th, CDC has issued more than 175 updates on the response to the

terrorist attacks and the anthrax investigations through a variety of communication channels, reaching an estimated 7 million health professionals and the public.

This level of communication and collaboration with our public health partners has been crucial to the investigation and response to these events, but improvements can still be made to the nation's information and communication systems, as called for in the *Infrastructure Report.* To maximize the effectiveness of the public health response, key communications recommendations must include:

1) *All health departments* should have continuous, high-speed access to the Internet and standard protocols for data exchange. Integral to this recommendation is the ability to detect cases and track and map disease occurrence in order to manage the public health response to an outbreak;

2) *All health departments* should have immediate, online access to current health information, such as public health interventions and treatment guidelines;

3) *All health departments* should have the capacity to send and receive sensitive health information via secure electronic systems and to broadcast emergency health alerts among hospitals, medical centers, and other community partners.

These recommendations are being achieved by a State and Federal partnership through three major initiatives, which form the core of a comprehensive, nationwide health information system. These three initiatives are the Health Alert Network (HAN), the National Electronic

Disease Surveillance System (NEDSS), and the Epidemic Information Exchange, or *Epi-X*. As the events of September 11th highlighted so dramatically, these three initiatives are critical to our nation's emergency response now–and for the future–and must be fully implemented as quickly as possible by States with Federal assistance. They must be fully implemented as quickly as possible, in a seamlessly integrated system that supports rapid and effective public health action. I will describe each briefly.

**Health Alert Network**

The Health Alert Network, or HAN, is designed to be the nation's rapid online system for health communication, information, and training. When fully deployed, the Health Alert Network will link local, state, and Federal agencies with their community partners, private health care providers, and others, and will serve as the electronic platform for NEDSS, Epi-X, and other applications. The Health Alert Network is being developed in three Phases, incorporating the three key recommendations of the *Infrastructure Report*. The three phases are:

***Phase I:*** Ensure that each county health department has 1) continuous, high-speed Internet access, 2) the capacity to receive emergency broadcast health alert messages, and 3) online access to Satellite and Web-Based distance-learning programs for just-in-time training and health updates.

***Phase II:*** Extend HAN to the full range of community partners; enhance information security and redundancy at each node in the network; ensure 24/7 operation and reach through expanded HAN Operations Centers at state and large city headquarters; and

deploy mobile phones, pagers, and new communications devices to state and local health officials.

*Phase III:* Provide time-saving and innovative information tools and resources for public health practice in the field, including model emergency plans and protocols; pictures, maps, and diagnostic reference images; health communication and media materials; and lessons learned from peer communities. Many of these resources are under development in three City-County Health Departments–Dekalb County, GA, Rochester/Monroe County, NY, and Denver City/County, CO–which serve as HAN Exemplar Sites and laboratories of innovation.

On the morning of September 11th, the Health Alert Network was fully activated for only the second time since its inception. Within four hours after the attack on the World Trade Center the Health Alert Network was in put into full operation at one of CDC's offsite facilities and began transmitting health messages to the top 250 public health officials in the 50 states, Guam, and 7 large cities. Over the course of the ensuing 12 weeks, some 60 health alerts, advisories, and updates have been transmitted directly from CDC, and the Network has been extended to potentially reach an estimated 1 million recipients in the first wave, including 1,500 local and county health officers and a wide range of frontline public and private practice physicians, nurses, laboratorians, environmental specialists, health communicators, and other professionals.

In addition to this first "tier" of communication transmitted directly from CDC, states with CDC funding and guidance have established their own statewide Health Alert Networks for

retransmitting and augmenting CDC information. Through August 2001, 40 states and cities had received Health Alert Network awards. In September the remaining states, the District of Columbia, and Guam received small planning grants to get started. To date:

- Thirteen states have directly connected 100% of their counties (924) to the Health Alert Network via high-speed continuous Internet access; the remaining 37 states have reached an additional 1,217 counties, for a total of 2,142 counties, or two-thirds (68.1% ) of all U.S. counties.

- Forty-two states are extending the Health Alert Network to reach private providers; these currently include approximately 2500 hospitals and 6,000 physician offices.

- All 50 states are developing full-function distance-learning systems for access to CDC training courses and broadcasts; since September 11th, CDC has reached 1.1 million public and private health professionals through a series of 12 Satellite and Web Broadcasts.
- All 50 states are developing Health Alert Network Web Sites; many of these are fully operational and have been used since September 11th to communicate with health professionals, the media, and the public, and to link directly to CDC's Web Site for Public Health Emergency Preparedness and Response.

**The Epidemic Information Exchange *(Epi-X)***

The Epidemic Information Exchange (Epi-X), is CDC's secure web-based communications system that provides intelligence sharing capabilities for CDC, state and local health officials, and select military health personnel regarding newly identified disease outbreaks and health events, particularly those suggestive of bioterrorism. Epi-X is intended to provide secure, moderated communication to help public health officials prepare for, and respond to, epidemics and other emerging health events, including bioterrorism. Epi-X serves as an important portal for private, electronic exchange of epidemiologic information, including early notification of suspected cases of disease, online discussions of presumptive diagnoses and laboratory reports, and rapid requests for onsite epidemic assistance. Epi-X also facilitates the rapid submission, review, and publication of timely updates for CDC's premier weekly health bulletin, the *Morbidity and Mortality Weekly Report* (MMWR), which provides definitive and citable articles for the scientific literature.

In response to the attacks on September 11th, Epi-X immediately provided secure communications among state and large city epidemiologists and CDC programs, including the Epidemic Intelligence Service. Since the identification of the first anthrax case in Florida, CDC and state and local health authorities have posted over 80 Epi-X reports on bioterrorism-related threats, investigations, and responses. Epi-X has also been used to notify health authorities by telephone and/or pager about urgent information on the anthrax investigations and to initiate telephone and on-line conferences to coordinate the ongoing public health response. In operation since December 2000, medical personnel review all content before distribution on Epi-X and they monitor the site on a 24/7 basis. Currently, 731 health officials at the local, state and

Federal level have access to Epi-X. To improve intelligence gathering and sharing across agencies, CDC plans to gather information from additional sources such as international health agencies, and to include additional Federal agencies, military installations and local public health and safety authorities in Epi-X. CDC will also assist other organizations in using standard reporting tools, developing editorial policies, and training users in online features. These expansions will further enable state and local health departments to identify and report public health threats, including those suggestive of bioterrorism. Epi-X represents an important, specialized application built upon the platform of the Health Alert Network.

**National Electronic Disease Surveillance System (NEDSS)**

Public health surveillance is a crucial monitoring function for CDC and its partners. It is these ongoing data collection activities that help us detect threats to the health of the public. Without our public health surveillance systems, we might not identify outbreaks or other important problems in time to prevent the further spread of disease. We cannot investigate problems, identify their causes, and implement control measures if we have not detected them. Surveillance systems also let local health departments map the location of cases, track whether cases are increasing or decreasing over time, and link laboratory data with case reports, to either confirm them as cases, or provide prompt reassurance if tests are negative. These surveillance data are critical to target resources appropriately for public health response. Recent events have underscored this essential role of public health surveillance.

The traditional operation of our surveillance systems generally consists of paper or facsimile reporting by providers to health departments. If a case of illness is particularly unusual

or severe (such as a case of anthrax or rabies), the provider will call the local health department immediately. CDC and its partners have recognized the need to build more timely, comprehensive surveillance information systems that are less burdensome to data providers. Several years ago, we initiated the development of the National Electronic Disease Surveillance System (NEDSS). The ultimate goal of NEDSS is the electronic, real-time reporting of information for public health action. NEDSS includes direct electronic linkages with the health care system; for example, medical information about important diagnostic tests can be shared electronically with public health officials as soon as a clinical laboratory receives a specimen, or makes a diagnosis.

NEDSS is designed to facilitate the development of an integrated, coherent, national system for public health surveillance that will have the flexibility and capacity to support emergency response, as well as handle ongoing public health surveillance needs. NEDSS standards provide an "architecture" which can support a wide range of surveillance activities. Ultimately, NEDSS will support the automated collection, transmission, and monitoring of disease data from multiple sources (clinicians' offices, laboratories, etc.) to local and state health departments and to the CDC. NEDSS will replace current systems used by public health agencies for collecting disease surveillance data, which rely on multiple, disparate, independently designed and supported systems. All 50 states, 6 cities and 1 territory have received funding for NEDSS; 21 jurisdictions have received funds for assessment and planning. Thirty-six state and metropolitan health jurisdictions are receiving funds for NEDSS compatible systems development, including 20 jurisdictions receiving support to deploy in 2002 the NEDSS Base System, a NEDSS-compatible system developed for state use.

**State and Local Efforts**

CDC has been working to ensure that all levels of the public health community – local, state, and Federal – are prepared to work in coordination with the medical and emergency response communities to address the public health consequences of biological and chemical terrorism.

State and local health departments are able to respond in part because of CDC's support of their bioterrorism preparedness. We have seen the results of these investments in the rapid public health responses to anthrax in Florida, New York, New Jersey, Washington, DC, and Connecticut. CDC has made awards to all states and three large cities--plus Washington, DC and Guam--which are now better prepared not only to identify and respond to bioterrorist acts, but also to provide enhanced communications with Federal, state, and local public health agencies. CDC will continue and expand support to states, as well as enhance CDC's own preparedness for future attacks.

**Public Health Infrastructure Development**

In addition to these efforts, CDC has also worked with ASTHO, NACCHO, and other public health partners to implement the new law enacted last November, the *Public Health Threats and Emergencies Act of 2000.* This landmark legislation calls for three important milestones to strengthen the nation's public health infrastructure:

- Development of a set of consensus public health infrastructure capacities required for national, state, and local public health systems and their workforces;

- Assessment of the current state of the nation's public health systems using these capacities to identify critical gaps in the infrastructure; and

- Technical assistance and funding to state and local health agencies to fill those gaps, beginning with the highest priority areas.

To date, CDC, HRSA, ASTHO, NACCHO, and state and local public health officials have jointly developed the set of public health infrastructure capacities and have identified seven priority areas for immediate strengthening. These seven areas build on the findings and recommendations of the *Infrastructure Report:*

- **System Readiness:** Public health systems with the ability and surge capacity to effectively respond to public health threats and emergencies.

- **Information Systems:** Secure, accessible information systems for rapid communication, acquisition, analysis and interpretation of health data, and public access to health information.

- **Communication**: Swift, secure, two-way communication mechanisms to distribute scientific and health information to communities and policymakers; provide timely, accurate public information and advice to policymakers during emergency events; and coordinate logistical communication within the response community.

- **Epidemiology and Surveillance**: Public health systems with the capacity to monitor health events, to identify patterns or aberrations, to track and respond to outbreaks, and to investigate underlying causes.

- **Laboratory**: Public health laboratories with the ability to produce timely and accurate laboratory results for diagnostic and investigative purposes.

- **Workforce**: A public health workforce capable of delivering the Essential Public Health Services during routine and emergency operation.

- **Policy, Laws, & Evaluation**: Utilization of community assessment findings to establish priorities, ensure proper legal authorities, and improve the effectiveness of programs and policy decisions.

The President's budget for FY2002 recommended funding to get this important work started. The Administration's emergency request after September 11th included funding to make further progress on these and other priorities.

**Lessons Learned**

The events of this fall are unprecedented. Like every organization and every individual, CDC has learned many lessons. As we work through the current anthrax threats and prepare for the next challenge, whatever it may be, we take forward a deeper understanding of bioterrorism and of how we share information.

We learned that the linkages we have helped forge between clinical and public health communities are strong and that these linkages saved lives by detecting illness early. We learned how to shorten the time lag between acquiring new knowledge, communication and action. We confirmed that close collaboration of local, state, and Federal public health personnel builds confidence in local response. We are newly aware of the challenge that changing science presents to clear communication. As we learned about the health risks of this outbreak, we had to modify recommendations, refocus investigations, and change our message. We put new scientific information into action with great speed. We also learned more about what information is valuable to the public and our partners, which will help us craft messages and materials in the future.

**Conclusion**

In conclusion, CDC is committed to working with other Federal agencies and partners as well as state and local public health departments to ensure the health and medical care of our citizens. We have made substantial progress to date in enhancing the nation's capability to prepare for and respond to a bioterrorist event, but there is much more to be done. The best public health strategy to protect the health of civilians against biological terrorism is the development, organization, and enhancement of public health prevention systems and tools, including enhanced communications mechanisms and messages. Other priorities include strengthened public health laboratory capacity, increased surveillance and outbreak investigation capacity, and education and training at the local, state, and Federal levels. Not only will this approach ensure that we are better prepared for deliberate bioterrorist threats, but it will also enable us to recognize and control naturally occurring new or re-emerging infectious diseases. A strong and flexible public health infrastructure is the best defense against any disease outbreak.

Thank you very much for your attention. I will be happy to answer any questions you may have.

Mr. TOM DAVIS OF VIRGINIA. Dr. Yeskey, you are just here to help answer questions; is that right?

Mr. YESKEY. That is right.

Mr. TOM DAVIS OF VIRGINIA. Before I go to Mr. Horn, Steve, I will start with you. But I want to ask one question.

A specific concern raised by local health departments was, it was unclear exactly who was in charge at the Federal level.

Before we embark on an in-depth examination of information-sharing capabilities, has CDC moved to address this fundamental point: Who is in charge?

Dr. BAKER. This is a challenging issue, as you know. And what we do at CDC is to work with our local and State partners in any investigation of a disease outbreak. And so we work to defer to the local authorities as they relate to the media and relate to their communities to provide information.

As far as within the Federal system, CDC is designated as the lead public health agency in events of this type.

Mr. TOM DAVIS OF VIRGINIA. Getting the word out is very, very important. We will hear some of the later testimony in terms of some of the confusion.

I am going to recognize the gentleman from California.

Mr. HORN. Thank you, Mr. Chairman. I have got one interest, and that is the laboratory interest.

Are they spread accurately across the counties that you mentioned, that had this network in computing?

One of our problems in the last 30 years has been where doctors had their own laboratory that was separated because it was felt they would—to get just their labs, and they were told to go get separate labs. And hospitals have certain labs.

So if you have some of this type of either flu that—some biological or chemical, how do we deal with that and get that done in a very rapid time so people aren't panicking? What is your feeling on that? And what should we do to link all of those labs up?

Dr. BAKER. Two thoughts, Congressman. One is that there is an activity under way called the Laboratory Response Network. This was created under the bioterrorism program, and this network has been used extensively throughout the anthrax situation to handle samples. It was used extensively in Florida to process materials there. And expansion and strengthening of that network is one specific way to address part of what you are asking about.

A second major initiative is one that we refer to as the National Laboratory System. You mentioned private hospitals. We believe there needs to be a concerted national effort to link the public health laboratories, that are typically run by governmental agencies, and private hospital laboratories in a much more seamless way to move information back and forth between them, to share information, to have standard protocols, standard ways of transmitting samples back and forth so we can track them more efficiently.

So those are the two initiatives that are under way to address the laboratory issue.

Mr. HORN. What about the smallest towns? Do we separate them at certain things and get a different chain or what?

Dr. BAKER. Within the Laboratory Response Network, there are levels of activity. And the smallest level, the lowest level, has the

least complexity. A small local hospital laboratory, for example, would have that capacity in most situations. As you move up the level of complexity, there are more centralized laboratories that address this.

Our commitment is that every community, regardless of how remote or how rural, have access to those laboratory services.

Mr. HORN. Thank you.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

With regard to increased coordination, tell us a little bit about the degree of coordination between our Federal agencies. In particular, I have on my mind, as many of us do, the recent reports about the Department of the Army's research on anthrax and the fact that, apparently, that may not have been known by other agencies of government.

Is that a problem? And should there be greater coordination and knowledge exchanged there?

Dr. BAKER. I am going to defer to Dr. Yeskey a bit on the specifics. He is more directly involved with the anthrax activities than I am. But just a general thought on that.

There have been very close collaborations with various parts of the Army, USAMRIID, the laboratory that does the work, as you know, on infectious disease research and has worked very closely with CDC throughout the course of the anthrax situation.

Again, it is always good to have more collaboration and more communication. We never can do that too much. But I would like Dr. Yeskey to elaborate a bit on your question.

Dr. YESKEY. I would agree with Dr. Baker that increased and improved coordination and integration is a desired goal. CDC worked hard, and continues to work hard, to integrate our activities with other Federal agencies, both within DHHS, such as the FDA or the Office of Emergency Preparedness, as well as outside the Department, with the Department of Justice, with the Environmental Protection Agency and others.

We try and coordinate—during the anthrax incident, we had close collaborations with all of those organizations, had a full-time liaison established at the FBI headquarters. I had a full-time liaison at the U.S. Postal Service office to help coordinate our activities with theirs.

So we attempted to make our best efforts at coordinating our activities both within DHHS, as well as outside the Department.

Mr. TURNER. Is there full disclosure between those agencies and those laboratories; or does each of them just sort of go their own way, share what they want to when they want to?

Dr. YESKEY. I can speak for CDC's laboratories. We tried to coordinate and had daily telephone conferences with both the FBI laboratory personnel, as well as Department of Defense personnel, to help coordinate lab result reporting during the anthrax incident.

Mr. TURNER. What kind of tracking is there of dangerous biological agents when they are transferred from one lab to another? And are those protocols common throughout government agencies, or do they vary from one to the other?

Dr. YESKEY. The transport of hazardous agents falls under the Select Agent Rule where organizations or institutions that manage or that are involved in the interstate transport of hazardous biological agents must register and then coordinate those transfers with the CDC and the Federal Government.

Mr. TURNER. By what method are those agents transmitted? Is it by ordinary private carrier? U.S. mail? How do those things travel?

Dr. YESKEY. There are established protocols for the transport of those materials to ensure that the integrity of the packages remains during the transfer of those. CDC has written protocols that govern that.

Mr. TURNER. And what method of transport is used for those kind of materials?

Dr. YESKEY. Depending on distance, it can be air courier, it can be ground transportation; but it is usually regular courier, private service.

Mr. TURNER. So the private service transmitting the package would know it is dangerous, but may not know exactly what they are transmitting from one locale to the other?

Dr. YESKEY. That is correct.

Mr. TURNER. Is that an appropriate way to handle this type of material, or should it be handled by the agencies and its employees by personal delivery rather than by using private carriers?

Dr. YESKEY. I will have to provide that information for the record at a later time.

Mr. TURNER. Does that answer mean you don't have an opinion or you are not familiar enough with the process to have an opinion?

Dr. YESKEY. My opinion is that it is appropriate, it is an appropriate mechanism for the transport of the materials.

Mr. TURNER. If we were going to suggest improvement in the handling of that material, what kinds of things would you suggest that we look at?

Dr. YESKEY. I think we need to examine to see if there are methodologies to improve the packaging, integrity, the notification of how the material is sent from one organization to the other, receipt times, anticipated delivery times, things like that, ensuring the security of that package as it goes through the transport system.

Mr. TURNER. Should we be reevaluating who we share this material with? In other words, I understand that some private labs can have access to some materials. I believe that is correct; isn't it, Dr. Baker?

Dr. BAKER. What we might want to do, just on this line of questioning, if this would be responsive, Congressman, is—if I understand your question, you are asking us about the transport of hazardous materials for which CDC does have responsibility under the Select Agent Rules, as Dr. Yeskey mentioned.

Each of us does not deal directly with that particular area of activity. Inevitably, in light of recent events, we are rethinking a lot of things we are doing, and this may be one of them; I can't tell you that today.

We would be happy to provide to you and work with you on specific areas that may need improvement, including how these get

transported and some of the issues that you are raising for us today, if that would be helpful to you.

Mr. TURNER. It would be helpful.

As I understood your answer there, you are already beginning to look at those protocols?

Dr. BAKER. What I said was that in light of recent events, we in public health are rethinking a lot of things. This has been an extraordinary experience for all of us, and CDC has been having a number of expert meetings over the last several weeks, bringing in experts from around the country to reflect on what has been happening and to then learn from each of these groups of people that come in.

And we can share with you both that sort of thing and on the specific issue that you raised in terms of the transport of hazardous materials. We are undoubtedly rethinking that. But neither of us is directly involved in those discussions. So we would be happy to share that with you.

Mr. TURNER. Thank you.

Mr. TOM DAVIS OF VIRGINIA. Thank you. I have a few questions.

Today, on the second panel, Dr. Sherratt, who is from my home county of Fairfax, is going to testify that the lack of CDC guidelines on anthrax initially created both anxiety and inconsistency in patient care. We also know the example of the post office reacting differently to this, looking at what I think might have been best-available-information differently than Congress did, as the information became available.

I guess my question is, how would you characterize CDC's actions in this? And what are we doing to ensure that we get a better response in the future?

I recognize we are on new ground. This came out of nowhere. So we are just looking back here, not looking for people to jump on, but to understand what happened and how we can better it the next time.

Dr. BAKER. The first thing I was going to say, Congressman Davis, was exactly what you just said. This is clearly an unprecedented event, and we all recognize that. And the response, both at CDC and at the State and local levels, has been unprecedented. We have had folks flying into various parts of the country, we have been issuing alert notices over the Internet, we have been doing nationwide satellite broadcasts. All of those are unprecedented responses.

We have learned from each of those particular activities. And, again, it is important we think to go back and look at what did happen, as you are doing here today, and learn from those lessons and, therefore, do better next time.

This was a bit of a shakedown cruise for all of us in terms of the whole public health system, and our information systems in particular. We are very proud of the way in which CDC and our partners were able to get information out through these mechanisms that we have talked with you about today.

As I mentioned, we issued an alert 4 hours after the World Trade Center event, around 1:30 on that afternoon. And issued alerts that went out now to as many as a million people on various aspects of the anthrax investigation. We have done a series of nationwide

teleconferences. We did one just yesterday on smallpox. That whole series has reached over a million people. This is the Distance Learning Network that we utilize to educate our public health work force around the country.

Unquestionably, we will be better off next time. Why will we be better off? First of all, the networks are in place and they are working and they are being expanded. So through all of this, through that experience, we have improved our relationships, we know better how to work the system.

Second, we have developed a very large amount of question-and-answer, very specific information, on a lot of aspects here that come up in the course of this investigation.

Mr. TOM DAVIS OF VIRGINIA. Let me ask you this. Does your distance learning reach the private health providers as well?

Dr. BAKER. Yes, sir. We have done programs in cooperation with the American Medical Association, the American Hospital Association, National Medical Association, a range of partners, public health, private. And again, as I said, these broadcasts—the first one we did on anthrax, I think reached about 500,000 people. It is on the Internet. You can go there and pick it up later on. It is actually being picked up overseas, as well, we are told, on the Internet.

Mr. TOM DAVIS OF VIRGINIA. OK. Another panelist in the next panel notes in his prepared statement that the NEDSS, HAN and the Epi-X projects are not always as well coordinated, and sometimes appear to have a little competition between them. Do you think that is accurate? And competition is not always bad, but in terms of when you want to disseminate information, you just have to take a team approach to get it out there and not try to play territorial. Do you feel that there is some of that? Are we still trying to get bugs out of that system? These are three new systems.

Dr. BAKER. Several thoughts. These are three new systems. That is the first and most important point. This is an ambitious enterprise overall to create an integrated public health information and communications system.

It is best to think of these three elements as three initiatives that ultimately flow together into an integrated approach to improving the way in which we share information. The Epi-X program is a confidential private way in which epidemiologists are sharing information back and forth. So the members of this network, there are over 700 participants now, can log onto a secure Web site and can talk back and forth about epidemiologic issues.

The NEDSS program, or the National Electronic Disease Surveillance System, is quite complex and quite challenging. Ultimately when it is in place, it will be a marvelous tool for public health, but it is the one that is really the least far along in terms of its actual implementation, and the reason for that has to do with the complexity.

The basic answer to your question is that these are three complementary approaches. The Health Alert Network provides the platform, it connects everyone to the Internet. The Epi-X program and the National Electronic Disease Surveillance Systems are supported by that platform.

Mr. TOM DAVIS OF VIRGINIA. OK. What steps are you taking to help ensure uniformity in control system architecture once systems

like the NEDSS are implemented by individual States? Is there or will there be an oversight or central control board to regulate how the systems are used or modified?

Dr. BAKER. First of all, for the Health Alert Network system, we have technological standards that were put in place a couple of years ago, and we are just in the process of updating them. So there will be then, from CDC, a set of technology standards that grantees under that grant program are provided with so that, therefore, they can buy the right kind of computers. They will have the right way to connect to the Internet and those kinds of things.

As far as the National Electronic Disease Surveillance System, there are a very extensive and complex set of standards that NEDSS participants will be asked to adhere to. So its a standards-based approach. Again, ultimately you won't be able to participate in these systems if you do not adhere to the standards.

Mr. TOM DAVIS OF VIRGINIA. OK. Can HAN be expanded to include private health care providers?

Dr. BAKER. We are expanding it now to include private health care providers. Since September 11th we have increased the distribution. We worked, as I mentioned earlier, with the American Medical Association, American Hospital Association. The way this works is that we send a Health Alert Network notice to professional organizations like the ones I mentioned, and they send it out to their members.

Mr. TOM DAVIS OF VIRGINIA. One of the problems with anthrax, and you can take a look at it, whether it is smallpox, or plague or whatever, is insufficient vaccines on hand, available, and ready to go.

Obviously we were caught off guard. This is the first time we have faced this. How are we preparing in the future on this? Do you have guidelines? We are looking ahead now to possibly expanded germ warfare, biological warfare?

Dr. BAKER. I would like to begin the answer, but ask Dr. Yeskey to elaborate.

On the smallpox issue, Congressman, we did a nationwide satellite teleconference just yesterday to inform the public and private health care communities about smallpox. It included experts from around the country. Secretary Thompson kicked that program off. Dr. Koplan, who is our Director at CDC, participated. Dr. Henderson, who is now working in the Department, was also part of that program.

It was designed to educate people about smallpox and familiarize them with a major new plan that has just been sent out to our partners to look at as far as smallpox is concerned. As you know, the Department and CDC are committed to getting increased amounts of smallpox vaccine so that those will be available to people if the need should arise.

Dr. YESKEY. I would agree. Our contingency planning and our preparations for additional agents that might be used as a biological weapon continue. We recently released a smallpox emergency response plan to State health officers. We continue to look at other agents and preparing response plans for those particular agents and ways of enhancing the public health infrastructure so we can

respond more appropriately for another event with a different agent.

Mr. TOM DAVIS OF VIRGINIA. Let me ask another question. This really goes throughout information, expanding to all of us, whether it is congressional briefings on what is happening in Afghanistan or whatever. I learn more from television than I get from all of the darn briefings. I don't know how my colleagues feel about it, but I sometimes get more than that. Same here in your case.

It seems that CDC might be able to communicate to the general public. I am not talking about other health officials and providers, but directly to the public using the news media. Are there any plans to aggressively make use of the media in future events so that the CDC message, not the message of endless consultants hired by the media, can get out to the public? Because at the end of the day, you, the umpire, are calling the balls and strikes on some of this, and are closest to the problem and have, I think for the most part, the most up-to-date research and information. I think that is fair.

Dr. BAKER. I have a couple of thoughts on that. First of all, I personally think many of us at CDC were very proud of the role that our Director Dr. Koplan played in communicating through the media directly to the public and did exactly what you are talking about, Congressman, of trying to work with the media to get the message out. And other experts at CDC were involved in doing this as well. There was a daily briefing of our Public Affairs Office with the media folks to give them the information that they need to do their job. And so working closely in partnership with the media is a very important part of this.

Also, some of the things that we do directly, like the teleconference series that I mentioned, actually are picked up by the media and are utilized in various ways. And, again, we have learned a lot. I think one of the areas that we will now do better on is this whole area of working with the media in a complementary, coordinated way and do a better job next time.

Again, we are proud of what we have done, but we have always—we always have opportunities to learn from this experience.

Mr. TOM DAVIS OF VIRGINIA. OK. Finally, in the testimony of the next panel, we are going to hear concerns that certain aspects of the privacy provisions in HIPAA will hinder efforts to improve surveillance. Have you considered these concerns, and do you think it might be necessary to revise the privacy regulations, and are you comfortable? It is always a tough balance over what should be private and what should be public in those issues.

Dr. BAKER. This is an area which I believe we would best be advised to give you an answer back. HIPAA is a very complex area. Others at CDC work on that, and perhaps we would be best advised just to answer that one for the record.

I would like, if I could, to just mention one final point since I believe we are drawing to a close here. We particularly appreciate the support of the Congress in passing legislation, the Public Health Threats and Emergencies Act, last year. The act was, as you know, initiated in the Senate, and the House activities are very important.

And this provides us with an unprecedented opportunity to strengthen the public health infrastructure through a new grant program that we will be developing with our partners. So, again, we appreciate the leadership here in the House and the Senate on that legislation. And we are committed to working as quickly as we can to get those resources out and to implement that piece of legislation.

Mr. TOM DAVIS OF VIRGINIA. Thank you.

I am going to recognize Mr. Turner.

Mr. TURNER. Dr. Baker, is there a national registry of all dangerous biological agents identifying their location and who is responsible for those agents?

Dr. BAKER. I understand your question. I will begin an answer, and I think probably best to elaborate for the record.

Dr. Yeskey mentioned earlier, and, Kevin, you may want to say more about this, the select agent rule is part of what we are talking about. There is a list of specific agents that are listed there. These are biological agents. There are also chemical agents where inventories are done. I am not sure if your question really related specifically to biological or more broadly than that.

There are also ways in which these are inventoried, and where people understand, for example, where a particular chemical is located in terms of the plant and how it is handled, that sort of thing.

Mr. TURNER. With regard to biological agents, is there a master list kept somewhere that would tell us where all of the dangerous biological agents would be in this country and who is responsible for them at those locations?

Dr. BAKER. We are not aware of that. I understand the nature of your question, and what we will do is come up with our best answer to that in terms of what is actually done in terms of tracking these hazardous agents. I think that is what you are asking about.

Mr. TURNER. Is there even a list of what we would call dangerous biological agents? Is there an agreed list?

Dr. BAKER. There is an agreed list of what we consider the important agents as far as terrorism is concerned. Those have been identified. And then there are the select agents which are comparable to those. We can provide that list to the committee.

Mr. TURNER. Would it not be appropriate, if we have not already done so, to have a law that requires a national registry so that we would know where all of those dangerous biological agents are at any given moment in this country; who has possession of them and who is responsible for them at those locations?

Dr. BAKER. I understand your question. I understand the logic of your suggestion. I am not in a position to say yes or no to your question today, but we will be happy to do so for the record. I understand your question.

Mr. TURNER. Dr. Yeskey, do you have an opinion on that?

Dr. YESKEY. Again, I agree with Dr. Baker. We will be happy to provide a list of the agents and how they are managed.

Mr. TURNER. It seems to me in this age of biological terrorist threats that it would be wise if we at least had some requirement that dangerous agents and their locations be known, perhaps even to go so far as to have some notification system in place for the

transfer of those agents. I assume by your answers to the previous questions there must be no control whatsoever on the import or export of dangerous biological agents into this country?

Dr. BAKER. I would go so far as to say I don't believe that is true. Again, I am sorry that we don't have the information at our fingertips to answer your question, as far as the importation piece is concerned.

Mr. TURNER. I would appreciate if you could give us some response to that, because I would like to know if there is a list somewhere of all of those agents, where they are, who is responsible for them, and if there is any control whatsoever on the transport of those, any notification requirements when they are transported within our country, or when they are imported or exported. Thank you very much.

Dr. BAKER. I would be happy to work with you on that.

Mr. TOM DAVIS OF VIRGINIA. Mr. Horn, any other questions?

Mr. HORN. Fine.

Mr. TOM DAVIS OF VIRGINIA. All right. Well, I thank you very much. And what I think we will do, you will have 10 days to supplement any remarks that you would like to make.

We will take a 3-minute break as we change panels and allow the next panel to come forward. We appreciate very much your being here today.

[Recess.]

Mr. TOM DAVIS OF VIRGINIA. As you know, it is the policy of the committee to swear in witnesses. If you would rise with me and raise your right hands.

[Witnesses sworn.]

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. Please be seated.

You see that we have our indicator box in the front. It will turn green. What we would like you to try to do is stay within 5 minutes, because your total testimony is part of the official record. We will start with Rock Regan over here.

Rock, we are going to start with you. Gregory; is that your actual name?

Mr. REGAN. Greg.

Mr. TOM DAVIS OF VIRGINIA. I remember that.

But we appreciate all of your being here, and we will start with the Rock over here and move straight down. Try to keep it within 5 minutes, then we will go with questions. Again, we appreciate everyone being here.

**STATEMENTS OF ROCK REGAN, NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS, CHIEF INFORMATION OFFICER, STATE OF CONNECTICUT; GIANFRANCO PEZZINO, M.D., MPH, COUNCIL FOR STATE AND TERRITORIAL EPIDEMIOLOGISTS, STATE EPIDEMIOLOGIST, KANSAS DEPARTMENT OF HEALTH AND ENVIRONMENT; PAUL WIESNER, M.D., MPH, NATIONAL ASSOCIATION OF COUNTY AND CITY HEALTH OFFICIALS, DIRECTOR, DEKALB COUNTY BOARD OF HEALTH; MICHAEL H. COVERT, AMERICAN HOSPITAL ASSOCIATION, PRESIDENT, WASHINGTON HOSPITAL CENTER; CAROL S. SHARRETT, M.D., MPH, DIRECTOR OF HEALTH, FAIRFAX COUNTY DEPARTMENT OF HEALTH; AND CHARLES E. SAUNDERS, M.D., PRESIDENT, EDS HEALTH CARE GLOBAL INDUSTRY GROUP**

Mr. REGAN. Good morning, Mr. Chairman and members of the committee. My name is Rock Regan. I am the chief information officer with the State of Connecticut, and the president of the National Association of State Chief Information Officers. Again, it is a pleasure to be here to talk about such an important issue.

The events of the last 3 months have galvanized government at all levels to increase our emergency preparedness capabilities for a range of threats. The threat of bioterrorism is among one of the most challenging and terrifying among them.

The current anthrax crisis which has hit so close to home in Connecticut, the U.S. Capitol, as well as recent outbreaks of Ebola virus in Africa illustrate just how important our bioemergency preparedness is. It has been observed by many that our first line of defense in preparing for bioterror is our ability to communicate and coordinate.

Our information and communications systems lie at the very heart of our response. The State chief information officers sit at the nexus of these communication and coordination systems, and we appreciate again you calling this hearing on these important issues of today.

I think, as mentioned earlier, the March 2000 report by the CDC outlined a couple of specific goals: the skilled work force, robust information and data systems, effective health departments and laboratories. Certainly our focus is on the second one, robust information and data systems.

NASCIO agrees with the CDC's March assessment in terms of the HAN initiative as well as the National Electronic Disease Surveillance System. HAN and NEDSS is a great first start.

In Connecticut, if I can personalize this, the National Electronic Disease Surveillance System will replace 18 stove-pipe systems with an integrated data repository for the sharing of this information. So I think, as Dr. Baker said, it is a very complex process to put that together, but I think the benefit will be great.

These goals which again are critically important for all health departments in the Nation to have continuous high-speed access to the Internet is going to require substantial investment for States and local governments, which, again, they cannot bear alone. I think, you know, as we go forward and look at the deployment of those systems, the one fact that has to be considered is the current networks that are available in the State and local governments.

Beyond HAN, really the way to do that is a coordinated integrated State information architecture, and if I could talk specifically about a couple of issues that NASCIO is involved with, there is currently one with the criminal justice community, a global justice initiative, to create a national natural integrated architecture for justice systems. It doesn't appear, by my knowledge, those of the CIOs that I have talked to, that this effort is under way for the public health infrastructure.

While the initiatives going forward, again, are very critical, it is unclear, I think, from many of our perspectives of how they plug into the overall architecture. Standards are great, but certainly local governments and State governments would like to have a say in how those standards are put together and how they fit onto the overall overriding architecture.

The justice integration architecture to me would be a blueprint to follow for the public health systems. Again, as we look at those initiatives such as anthrax, the ability to cross-communicate information in a very timely basis across multi jurisdictions, not just health agencies, public safety, Governors, other departmental agencies within States and local governments, particularly first responders, the State CIOs and Federal homeland defense officials in conjunction with Justice and CDC again may do well in considering using the justice integrated architectural process here for creating a public health information architecture that, again, fits in with an overall State architecture and a homeland defense scenario. This integration will allow for access as appropriate to vital alert and response information by all affected State agencies.

Again, getting back to Connecticut, Connecticut, we had an anthrax issue, a 94-year-old woman who passed away as a result of the anthrax. We had a very excellent response by CDC, over 20 people responded; FBI, over 20 people responded. To think in context of what advantage to the 1 event, 10 events, 1,000 events across the country, our ability to communicate was not in place.

And I think that the infrastructure and architecture that we are talking about in these networks will be the vehicle to do it. We are just not going to have enough trained people to respond to these situations. So the communication infrastructures will be vital in any response, particularly if it is a national response.

State CIOs again want to be involved in the planning process. And to sum up, I think, as we talk about communicating, it is not just one way from the Federal Government down to the State and local jurisdictions, it is multiway processing, down from the Fed, up from the local, State to the Feds, again the sharing of information.

And summarizing, I have been asked by my Governor to ensure an effective information communications infrastructure for responding to the bioterror threat. As the Nation's governments gear up to prepare for the threat of bioterrorism, NASCIO believes the path to efficient implementation of preparedness initiatives lies with open coordination between all levels of government and views toward information systems that emphasize open architectures rather than closed, stove-pipe systems. To this end NASCIO has opened up communications with Director Ridge's Office of Homeland Security and would be pleased to coordinate and initiate co-

ordinating relationships with CDC and others to more effectively implement our public health infrastructure improvements effort.

These efforts, we believe, are necessary to safeguard the American public in every part of the Nation, in every State and every county, and in every city.

Again, I appreciate the opportunity to speak before you today.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much, Mr. Regan.

[The prepared statement of Mr. Regan follows:]

**STATEMENT OF ROCK REGAN**
**PRESIDENT**
**NATIONAL ASSOCIATION OF CHIEF INFORMATION OFFICERS OF THE STATES**
**CIO, STATE OF CONNECTICUT**

**BEFORE THE**
**COMMITTEE ON GOVERNMENT REFORM -**
**SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY**
**UNITED STATES HOUSE OF REPRESENTATIVES**

**DECEMBER 14, 2001**

Mr. Chairman, and Members of the Committee:

The events of the last three months have galvanized government at all levels to increase our emergency preparedness capabilities for a range of threats, and the threat of bioterrorism is among the most challenging and terrifying among them. The current anthrax crisis, which has hit so close to home here in the U.S. Capitol complex, as well as the very recent outbreak of the Ebola virus in Africa illustrate so clearly how important our bio-emergency response preparedness is. As has been observed many times, our first line of defense in preparing for bioterror is our ability to communicate and coordinate - our information and communication systems lie at the heart of our response. The state chief information officers sit at the nexus of these communication and coordination systems, and we appreciate your calling this hearing to examine these issues today.

The question that government at all levels is faced with is "Are we prepared for the threat of bioterrorism?" The March 2001 report by the Centers for Disease Control, *"Public Health's Infrastructure: A Status Report,"* reported that although we have made important advances in our capability to identify and respond to such incidents, the answer is clearly that we are not. The CDC goes on to recommend some specific goals in the three areas of: 1) Skilled Public Workforce, 2) Robust Information and Data Systems, and 3) Effective Health Departments and Laboratories. For our purposes here, I will focus on the second element of the CDC's recommendations, the importance of Robust Information and Data Systems, and give you some perspective from the officials responsible for information systems at the state level.

**The CDC's HAN & NEDSS: A Good Start**

NASCIO agrees with the CDC's March assessment that while recent congressional funding for such initiatives as the Health Alert Network has provided much needed support to strengthen electronic communications in selected communities, a more comprehensive, sustainable effort from Federal, State and Local government is critical. The HAN initiative, with 40 sites in 37 states funded to begin basic implementation of internet connectivity, broadcast communications, and distance-learning capacity at the local level, is a good start. In the State of Georgia, for example, the process by which the state public health department would alert physicians and hospitals of outbreaks and potential threats was, up until a short time ago, largely phone, fax and letter based. Within the last three months, however, they have seen the dramatic increases in response times by being able to send alerts to their network of physicians, hospitals and labs out over e-mail. Georgia was able to do this with a combination of funding from the CDC HAN program and other sources, and is a strong example of the good start that the Health Alert Network program represents. This being said, this start needs to be dramatically expanded before we can speak of a nationwide biological incident alert network.

The National Electronic Disease Surveillance System (NEDSS) has also provided an excellent first step in providing support to 46 states for national standards, specifications and prototypes so that critical information collected at the local level, plugged into the Health Alert Network, can be used to detect and manage outbreaks that affect more than one state or community. Having provided a start, there remain many CDC surveillance tracking systems that remain stovepiped, single purpose systems that are not integrated. The NEDSS too, needs to be dramatically expanded before we can even begin to speak of a truly integrated national bio-emergency response capability.

In Connecticut, we are in the planning stages of implementing the Health Alert Network, and as part of the effort, we are integrating 18 different disease surveillance systems into one "Integrated Data Repository".

NASCIO is also supportive of the specific goals the CDC sets for creating robust information and data systems nationwide, including the goal of:

> "Each health department will be able to electronically access and distribute up to date public health information and emergency health alerts, monitor the health of communities, and assist in the detection of emerging public health problems."

The report recommends that this goal be met by ensuring, by 2010, that all health departments have continuous, high-speed access to the internet and standard protocols for data collection, transport, electronic reporting, and information exchange that protect privacy and seamlessly connect local, state and federal data systems.

This goal, while certainly critically important to achieve, is a truly significant task, one that requires some consideration for its regulatory and fiscal implications. For all health departments in the nation to have continuous, high speed access to the internet will require a substantial investment that the states and localities cannot bear alone, and the regulatory implications of data collection, transport, electronic reporting and information exchange that protect privacy and seamlessly connect local, state, and federal data systems are of an intimidating scope as well. When one considers the huge costs and implication of complying with the Health Insurance Portability and Accountability Act (HIPAA), and the potential impact of privacy and security regulations, and then takes the next step to examine how to seamlessly connect federal, state and local data systems together across "stovepiped" systems and jurisdictions, the scope of our needed effort becomes vast. As a result, while we fully endorse the goal of an integrated, secure and private, nationwide health alert system, we only note that it is a task that requires a sustained, long-term effort in which the memory of the terrible lessons of September 11th and the subsequent anthrax crisis cannot fade.

NASCIO has been asked to comment on what barriers might exist to the further implementation of the Health Alert Network in states. While most states have endorsed the concept of the HAN, there is some evidence that some local health departments retain a focus on a concept of public health as primarily that of providing health services to the poor, while many public health professionals view their roles increasingly transitioning to that of providing health threat information and education services to the public.

**Beyond HAN: Integrated State Information Architecture**

It is particularly important to realize that the state public health/bioterror response is part of an overall Homeland Defense picture, and needs to be integrated into state information architecture networks as such. The Office of Homeland Defense has asked states to begin threat/vulnerability assessments in three areas – Kinetic threats (bombs, hijacked vehicles, etc), cyberterror, and bio-threats/terror. One of the questions that need to be considered when implementing systems such as HAN and NEDSS is "who else needs this information?" For example, the chief of the state police, and the commander of the National Guard and their staffs are your 'first responders" to a bioterror incident – they and their information systems must have access to the information, as appropriate, on your state public health

network. These systems need to be integrated - but I want to emphasize that I am not suggesting that everyone – the state police, national guard, and state public health department all share all of their information. I am suggesting that each agency needs to have access, through the state's information architecture, to the data on each other's systems that is appropriate and consistent with their mission and responsibilities.

**An Example of Integration: Justice Architecture**

For an example of a system that is integrating across local, state and federal levels, one need only look at the Justice Architecture Integration effort currently underway across the nation. Within each state, four elements of the criminal justice system are integrating information systems between themselves and with their local and federal agency partners. Local and state police agencies, Departments of Corrections, and the judicial systems are identifying commonalities and integration points with each other, and tying into the FBI, the federal corrections, and national judicial system. To date, some 43 states are making, or have made, significant progress in this area. The justice integration program, with the National Crime Information Center at its core, may be a model for what the public health information system should move toward, and in fact, it is one of the emergency management systems that the public health network needs to be plugged into. As another example of a small step in this direction, the internal website of one state's fire safety department provides direct links to that state's public health department so that fire and public safety officials can access biothreat information as it becomes available – demonstrating the obvious need for common information between the emergency medical services that the fire safety departments encompass and the information about biological events that the public health agency is responsible for disseminating.

The state CIOs and federal Homeland Defense officials, in conjunction with Justice and CDC, may do well to consider using the Justice Integration Architecture as a launching point for integrating public health information into an overarching State Information Architecture that incorporates all aspects of Homeland Defense information systems within the overall architecture. This integration will allow for access, as appropriate, to vital alert and response information, as appropriate, by all affected state agency responders.

**Anthrax in Connecticut**

We are all saddened and concerned at the tragic death of Ottilie Lundgren, a 94 year-old resident of Seymour, Connecticut, who we believe came into contact with anthrax spores through cross-contamination with letters meant for other destinations. The way the system responded to this very specific case, so close to home for us in Connecticut, is instructive for dealing with any future incidents. The state public health department, in the absence of an integrated information system, reacted in a traditional manner, communicating and coordinating on an individual basis through phones, faxes and face-to- face meetings. The Centers for Disease Control and the Federal Bureau of Investigation both sent 15 or so personnel to Connecticut to investigate the case – consider, for a moment, how the state and these federal agencies would respond to an incident involving a hundred cases, or a thousand. There aren't enough people to go around to have phone discussions, send faxes, or travel to incident locations to conduct the necessary coordination. It is clear that effective exploitation of the state's information and communications infrastructure will be necessary in any response to a large incident, and the extent to which the state's infrastructure is integrated within the state and with the federal government will be a major factor.

**Coordinate with the State CIOs**
It is critical to have the state Chief Information Officers involved in the planning efforts for the expansion of existing public health information and data infrastructure, and for new initiatives for information flows between federal, state and local health agencies. Each state is working for the creation of an overall state information architecture, designed from a holistic perspective, to allow for greater efficiency, speed, privacy and security. In most cases, HAN and NEDSS are being implemented in accordance with state IT architecture planning, but a more formal process of coordination should be established, particularly if, as we recommend, the HAN and NEDS initiatives are expanded upon. Further, as Director Tom Ridge of the Office of Homeland Security suggested in late November, if a "National Health Data Network" that would create a permanent infrastructure to connect all 50 states and public health departments is implemented, this would require extensive coordination with state CIOs to ensure connectivity and common standards with current state IT systems.

A perfect example of the proper way to think of the role of the state CIOs in the current bioterror defense framework is contained in an anecdote from one of our states: at an early meeting to consider bioterror preparedness, officials from the state public health department, and the state public safety department sat down to consider their task. It soon became clear that someone was missing from the table – someone from the State CIO's office. The basic infrastructure that supported both of their information systems – the Health Alert Network in the case of the state public health department – were reliant on the information systems infrastructure of the state, falling under the purview of the state CIO. Further, since many state CIOs have direct responsibility for the information security/cybersecurity mission, the State CIO plays a critical role in that domestic Homeland defense sector as well.

**Information flow must be two-and three-way, not just federal dissemination of information:** Greater emphasis needs to be placed on interaction between public health officials at all levels, not just the push of information downstream. The CDC Health Alert Network is often used as an information broadcast system from the CDC out to the states and localities, while in its full iteration we hope it will be more interactive. States are repositories for vast amounts of data that can and must be tapped into for the system to function at its highest effectiveness, and the federal government can assist the states in integrating their systems to first access this data, and then "mine" it for the benefit of government at all levels.

**Funding:** Finally, officials at the state, county and city levels have all expressed their concern over increasing security costs. The National Governor's Association, the National Association of Counties, and the U.S. Conference of Mayors have all made it clear that significant federal assistance, probably in the form of block grants, will be necessary for improvements in the system to have long-term effectiveness. Some NGA estimates for the cost of bio-terror preparedness efforts and communications upgrades approach $3 billion for the first year alone. This situation will become exacerbated as the tax revenue implications for the states of the downturn in the economy become clearer. As Kentucky Governor Paul Patton has commented, "State budgets are already burdened by the recession and we have responded to the requests of various federal agencies for assistance in the wake of the September 11 terrorist attacks, and to be blunt, these services aren't cheap. We need funds that will afford us the flexibility necessary to deal with the broad range of security responsibilities that now confront every governor."

The recent security challenges have caught most states in between funding cycles, and as a result, funding is being pulled together from wherever possible to implement public safety measures. At least one state is in the process of calling up National Guardsmen from their civilian responsibilities to assist that state in developing their information security vulnerability/threat assessment because of a lack of either funding or state personnel available to perform such duties. NASCIO is encouraged by the consideration in the coming days in both the House and the Senate of legislation that would provide funding for state and local preparedness.

An element of the funding question that must not be ignored here is that of basic infrastructure. An illustration of what this means and how important it can be is found in a real-life situation where a state's Health Alert Network system had to be shut down because the air conditioning systems that cooled the state's servers broke down – in the middle of a recent bio-hazard emergency. Basic infrastructure issues such as these require funding considerations in addition to those related to the implementation of information systems.

**Conclusion**

I have been tasked by my Governor to ensure an effective information and communications infrastructure for responding to bioterror incidents, an information infrastructure that he sees as the core of our response. As the nation's governments gear up to prepare for the threat of bioterrorism, NASCIO believes the path to efficient implementation of preparedness initiatives lies with open coordination between all levels of government, and a view towards information systems that emphasizes open architectures rather than closed, stovepiped systems. To this end, NASCIO has opened communications with Director Ridge's Office of Homeland Security, and would be pleased to initiate coordinating relationships with the CDC, ASTHO and others to more effectively implement our public health infrastructure improvement efforts. These efforts, we believe, are necessary to safeguard the American people in every part of the nation, in every state, in every county, and in every city. I appreciate the opportunity to appear before you.

Mr. TOM DAVIS OF VIRGINIA. Dr. Pezzino.

Dr. PEZZINO. Mr. Chairman, members of the subcommittee, I am Dr. Gianfranco Pezzino, State epidemiologist with the Kansas Department of Health and Environment. I am very pleased to be here today in my capacity as president-elect of the Council of State and Territorial Epidemiologists [CSTE].

I was asked to address questions today revolving around how the use of appropriate information technologies has helped public health officials in the management of the anthrax crisis of the past months. For more than a decade CSTE has urged CDC to move away from a model of separated, self-contained surveillance systems and to work toward the flexible integrated solution.

Three initiatives have been developed in the past few years by the CDC with substantial input from local and State public health partners. These initiatives are NEDSS, the Health Network, and Epi-X. NEDSS is an important effort. One important function of NEDSS is the establishments of standard architecture based on current industry standards for public health electronic information systems. The use of those standards will allow agencies to achieve a more effective use of information technology and to share data.

The second initiative is the Health Alert Network. This is primarily an infrastructure project to improve the information technology infrastructure in local and State health departments by helping public health agencies to obtain Internet and e-mail access.

And the third project, Epi-X, is an Internet application developed by the CDC. Through its secure Web site, Epi-X allows public health officials to exchange communication about outbreaks and other emergency health events. This electronic forum has been extensively used during the anthrax-related emergency to share information, experience and intervention protocols. Another unique feature of Epi-X is emergency notification by telephone or pager to defined groups of public health officials.

So how do these projects interact with each other? Epi-X uses the standards defined by NEDSS and exploits the network built through the Health Alert Network. All these three projects provided some essential functions during the response to the anthrax threat of the past month.

The pager that I am carrying here today is a Health Alert Network pager. This pager received multiple messages from the Epi-X project in the past few months and mailed these messages directing me to go to the Epi-X secure Web site that was set up using NEDSS standards.

So, in summary, each project gains strength from the presence of the others, and none of them can be successful alone. While these are positive developments, much work remains to believe done. We have identified three priority areas that need immediate attention.

First, the process of integration envisioned by NEDSS is far from being completed. Even the three projects that I mentioned, NEDSS, Health Alert and Epi-X, have not always built on each others' strengths. And at times they have appeared to compete for the same scare resources or to attempt to establish one project as the only one worth expansion. Funding for all of these three projects

must be assured. The three projects must work together to achieve their common goals.

The second area of priority is the link between public health departments and private health care providers. Virtually all public health emergencies will be detected through information available from some private providers. Currently the most common communications methods between private providers and public health departments remain mail, fax or telephone. It takes about 3 days for my office to prepare mailing labels, duplicate a letter, and put it in the mail so that we can reach our thousands of providers throughout the State with some public health notification.

Private health care providers also play a key role in the response to public health emergencies. And the Health Alert Network needs to expand to include private providers so that they can be quickly notified of the existence of public health threats and how to contain them.

And finally, it should never be forgotten that the functioning of even the best computer network remains based on the presence of trained, skilled, qualified public health workers. The most timely alert will be of little use when it reaches a health department running 3 half days a week and staffed with one part-time nurse, as it happens in some rural areas of my State and other parts of the country.

Funding for the support of a basic public health infrastructure must increase dramatically, and it must represent a sustained effort over time.

In conclusion, CSTE supports and appreciates the efforts made by the CDC in the past few years to improve and integrate public health information systems, but many barriers remain. Nevertheless, projects such as NEDSS, Health Alert and Epi-X have contributed enormously toward achieving better integration of information, more timely detection of public health emergencies, and more prompt and effective dissemination of health alert messages.

These initiatives are all complementary to each other, and funding and support for all of them must grow considerably so that the expected results can be achieved in a short time as possible. We cannot afford to wait.

I want to thank you, Mr. Chairman, for the opportunity to testify here this morning on this important topic.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Dr. Pezzino follows:]

# Council of State and Territorial Epidemiologists

Executive Committee:

President:
Matthew L. Cartter, MD, MPH
Epidemiology Program Coordinator
Connecticut

Vice President:
James J. Gibson, MD, MPH
State Epidemiologist
South Carolina

President-Elect:
Gianfranco Pezzino, MD, MPH
State Epidemiologist
Kansas

Secretary – Treasurer:
John P. Middaugh, MD
State Epidemiologist
Alaska

Members-at-Large:
Ursula Bauer, PhD
Chronic Disease Epidemiologist
Florida

Jesse Greenblatt, MD, MPH
State Epidemiologist
New Hampshire

Suzanne R. Jenkins, VMD, MPH
Assistant State Epidemiologist
Virginia
Infectious Disease Epidemiology

Steven C. Macdonald, PhD, MPH
Epidemiologist
Washington
Environmental Epidemiology

Bela T. Matyas, MD, MPH
Medical Director,
Epidemiology Program
Massachusetts

C. Mack Sewell, DrPH, MS
State Epidemiologist
New Mexico

Executive Director:
Donna Knutson

**TESTIMONY**

**BEFORE THE**
**SUBCOMMITTEE ON**
**TECHNOLOGY AND PROCUREMENT POLICY**
**COMMITTEE ON GOVERNMENT REFORM**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**WITNESS: GIANFRANCO PEZZINO, MD, MPH**

**DECEMBER 14, 2001**

National Headquarters: 2872 Woodcock Boulevard • Suite 303 • Atlanta, Georgia 30341-4015
phone: 770.458.3811 • fax: 770.458.8516
www.cste.org

**Mr. Chairman**, Members of the Subcommittee, I am Dr. Gianfranco Pezzino, State Epidemiologist with the Kansas Department of Health and Environment. I am very pleased to appear before the Subcommittee this morning in my capacity as president-elect of the Council of State and Territorial Epidemiologists (CSTE). CSTE (an affiliate organization of the Association of State and Territorial Health Officials) is a professional organization that includes about 400 epidemiologists engaged in the practice of public health in state and local health departments. In my testimony I will address the status of public health information systems, particularly the National Electronic Disease Surveillance System, also known as NEDSS, and the role of these systems in enhancing public health practice at the state level and facilitating the recognition of and response to bioterrorism events.

**Background - The problem**

Let me begin by providing you with some background on the events that led to the development of current initiatives that I will briefly describe in my testimony today. Over several decades, as the need of CDC and its state and local partners for surveillance for many diseases proliferated, independent, non-standardized information systems were developed by CDC's programs and centers and by state and local public health agencies to meet each separate surveillance need. This resulted in over 100 separate information systems dependent on data collected at the state and local level that are unable to communicate with one another, so that systems in one health department or one CDC program may not be able to exchange information with systems located in other agencies that monitor similar or related conditions. The presence of multiple, non-standardized, proprietary information systems in the public and in the private sectors also impaired the ability of these two sectors to exchange information.

This situation presents multiple problems. Public health surveillance is the intelligence system that we must rely on to detect any unusual health-related event, including the consequences of a bioterrorist attack. Without an integrated, comprehensive public health surveillance system, the identification of these public health emergencies or disease outbreaks with potential national impact is very problematic. In addition, the presence of multiple, non-integrated systems leads to an undesirable error rate in record-keeping, inefficient use of time and labor, potential for under or over-reporting, and a duplication of efforts. As a consequence, public health agencies have been unable to build a true national public health surveillance system that can provide a comprehensive, accurate, and timely picture of the health status of our communities.

**The response**

Many people involved in surveillance at the state and local level, as well as private sector health reporters (such as doctors and hospitals), have suffered from these inefficiencies and have called for a different approach. CSTE has recognized that CDC has a unique role and position of leadership to play in the establishment of integrated surveillance tools. For more than a decade, CSTE has urged CDC to move away from a model of separated, self-contained surveillance systems and to work toward adoption of a flexible, integrated solution. The enactment of the

Health Insurance Portability and Accountability Act (HIPAA) in 1996, with its provisions for electronic data standardization, provided further impetus to the process of building an integrated, timely, national surveillance system, while also offering unprecedented opportunities for public-private electronic interface.

Three important initiatives have been launched in the last couple of years that address the limitations that hampered public health information systems. These three initiatives have been developed by the CDC with substantial input, support, and participation from local and state public health partners. These initiatives are NEDSS, the Health Alert Network, and the Epidemic Information Exchange (or Epi X).

The ***National Electronic Disease Surveillance System (NEDSS)*** is an important effort launched by CDC in FY 2000, through funding provided by Congress. One of the most important functions of NEDSS is the establishment of a standard architecture (based on current industry standards) for public health electronic information systems. This architecture, among other features, includes specifications and standards for the secure collection, transmission, and exchange of public health records for different agencies or programs. The use of these standards will allow local, state, and federal agencies to achieve a more effective use of information technology, so that we can study and understand health-related data across different programs and jurisdictions and detect potentially related cases around the country. Some of the expected advantages of implementing NEDSS are:

- Integration of information systems currently separated by differences in data formats and codes, and unable to communicate with each other. This integration will provide the ability to pull, edit, and analyze records from different databases in a combined fashion.
- Improvement of the disease reporting mechanisms, with more timely and accurate information available for decision-making and action.
- Establishment of a national electronic disease surveillance system able to identify more promptly public health threats with national implications, both natural and intentional (i.e., bioterrorism attacks).
- Interface with clinical databases (e.g., laboratories, clinics) to make medical information that is valuable for surveillance purposes available in electronic format. This will allow, for example, surveillance programs to receive electronic reports from laboratories or health care providers in a more complete and timely fashion with less burden on the health care sector.

The second initiative is the ***Health Alert Network***. This is a nationwide program that has as one of its main goals the improvement of the information technology infrastructure in local and state health departments. This network is helping public health agencies to obtain fast and secure Internet access and will facilitate linkage between local health departments and health care providers. The Health Alert Network is primarily an infrastructure project that helps health agencies assess their technology needs, acquire the appropriate equipment to meet those needs,

establish Internet connection and E-mail capability, and develop appropriate training of public health workers (particularly through the use of distant learning initiatives).

The third project, ***Epi X,*** is an Internet browser-based software application developed by the CDC. Through its secure Web site, Epi X allows public health officials at the CDC and in state and local health departments to exchange communication about outbreaks and other acute or emerging health events. In addition, Epi X contains a forum area for state epidemiologists to post information on surveillance and response activities for approximately 500 public health officials around the country. This forum area has been extensively used during the anthrax-related emergency by state and local epidemiologists to share information, experience, and intervention protocols, so that lessons learned in one part of the country can be used in other parts. Another unique feature of Epi X is emergency notification by telephone and pager to defined groups of public health officials.

**How do these projects interact with each other?**

While NEDSS, the Health Alert Network, and Epi X at first may appear like similar and perhaps overlapping or duplicative projects, a more careful examination shows that they actually address complementary needs. NEDSS fulfills the essential function of putting some order in the Tower of Babel represented by dozens of different, proprietary software applications unable to communicate with each other. The Health Alert Network helps build the technology infrastructure and networking capacity needed to link all different public health agencies to each other and to private health care providers. Epi X allows the collection and sharing of important information on public health events, facilitating the prompt recognition of disease outbreaks and possible bioterrorism attacks and the dissemination of public health alerts. To do that, Epi X uses the standards defined by NEDSS and exploits the network built through the Health Alert Network. All three projects provided some essential functions during the response to the anthrax threat of the past months, and facilitated the rapid and secure exchange of important information among the CDC and states and local public health agencies.

***In summary, each project gains strength from the presence of the others, and none of them can be successful alone.*** The critical factor is to assure that these projects can develop in harmony, avoiding duplications and gaps.

**Future challenges**

The development of these initiatives over the past few years has been a reason for satisfaction for those of us who had been frustrated by the confusion among public health information systems. While these are positive developments, much work remains to be done, and many challenges remain ahead of us. The CDC document, *Public Health's Infrastructure: Every Health Department Better Prepared; Every Community Better Protected,* laid the groundwork for a ten-year process through which our public health infrastructure can be reinforced (or, in some cases, totally rebuilt). This is an excellent document, and CSTE supports its goals. At the

same time, my organization also recognizes that the events of the past four months have changed the emphasis and importance of some of the functions outlined in that document, and our country cannot wait until the year 2010 to achieve some of the goals of the plan, especially those related to workforce development, public health surveillance, and alert and notification functions.

We have identified three priority areas that in our opinion need attention during the next months and years. First, the process of integration envisioned by NEDSS is far from being completed. Too many software applications and programs that do not comply with the NEDSS architecture still operate within CDC and in some states. As a result, the national public health surveillance system remains fragmented into pieces that cannot be combined to form a meaningful puzzle. Even within the CDC, the three projects that I have mentioned earlier, that is, NEDSS, Health Alert Network, and Epi X, have not always built on each other's strengths, and at times have appeared to compete for the same scarce resources or to attempt to establish one project as the only one worth expansion. In addition, security functions are not integrated among these and other CDC projects, and users must log on to each system using separate user names, passwords, and mechanisms. The consequences of these approaches are potentially severe, as they represent further barriers in an already complex process of integration, and increase confusion among state and local partners struggling to understand the strategic, unified vision underlying these projects. Our recommendations in this area are the following:

- Efforts for better integration among surveillance information systems must continue. The trend toward better integration must be at the base of any information technology project in the field of public health surveillance, and the CDC needs to emphasize and clarify its integration strategies both internally and externally.
- The implementation of the NEDSS project (including the deployment of the CDC-produced basic software for public health surveillance for use in states and local health departments) must be accelerated, and options should be considered to perform a formal evaluation of the compliance of CDC's and states' electronic public health information systems with the NEDSS principles and standards.
- Adequate funding for NEDSS, the Health Alert Network, and Epi X must be assured, and these three projects must work together to achieve their common goals and establish a national detection, alert, and notification system for bioterrorism events and other public health emergencies.

The second area of priority that we have identified is that the link between public health departments and private health care providers such as physicians, managed care organizations, hospitals, and laboratories needs to be strengthened. Virtually all public health emergencies, including bioterrorism attacks, will be detected through information available from some of these private providers, and they in turn must have easy access to reporting mechanisms that are fast and not burdensome. Public health surveillance must become better integrated in the daily workflow of clinics and hospitals, rather than being a separate entity requiring additional efforts and resources from the providers. Currently, the most common communication methods

between private providers and public health departments remain mail, facsimile, or telephone. In very few cases have computerized information systems linking the two sectors been put in place. Clinics and hospitals around the country often do not have computerized medical records, and when they do, the records are stored in proprietary systems marketed by multiple private vendors who do not share the same standards. The implementation of HIPAA standards may provide a boost to the adoption and expansion of standardized electronic medical records. Mechanisms must be put into place to capture relevant surveillance data directly from medical records in a timely and secure fashion. Recent contacts between the CDC, state and local health officials, and a consortium of major private vendors of health care information systems to discuss how to achieve this integration between surveillance and clinical activities are promising, and should continue. Funding for the establishment and testing of electronic data transfer applications to link emergency room, inpatient, and laboratory data with public health surveillance systems is essential. Private health care providers also play a key role not only in the detection of, but also in the response to public health emergencies. The Health Alert Network, that in most states is currently limited to public health agencies, needs to be expanded to include as many private providers as possible, so that they can be quickly notified of the existence of public health threats and how to contain them.

Finally, it should never be forgotten than the functioning of the best surveillance information system and computer network continues to rely on the presence of trained, skilled, qualified public health workers. The importance of the development and training of an adequate public health workforce cannot be overemphasized. The most timely alert will be of little or no use when it reaches a health department running three half days a week and staffed with one part time nurse, as happens in many rural areas of our country. Several CDC initiatives, such as the Epidemiology and Laboratory Capacity program (ELC), the Health alert Network, and the Emerging Infections Program (EIP), have provided limited support for the development of basic public health infrastructure and workforce training at the state and local level. However, many state applications for support sent to these programs have been accepted but not funded for lack of resources, and are currently sitting idle. Funding for the support of a basic public health infrastructure must increase dramatically and must represent a sustained effort that, over time, will yield as a dividend protection for our nation from natural or intentional public health threats.

**Conclusion**

In conclusion, the Council of State and Territorial Epidemiologists supports and appreciates the efforts made by the CDC and the Department of Health and Human Services in the past few years to improve and integrate public health information systems. Our organization, as well as other organizations representing public health workers and officials, is willing to contribute to the establishment of a national, secure, electronic surveillance system able to assure early detection of public health threats and prompt distribution of public health alerts. Many barriers remain. Some institutional memories may be hard to change. Links between the public and the private sector remain weak. Most state and local health departments are still chronically underfunded, and many of them are functioning on bare-bone budgets and resources.

Nevertheless, projects such as NEDSS, Health Alert Network, and Epi X have contributed enormously towards achieving better integration of information, more timely detection of public health emergency and bioterrorism events, and more prompt and effective dissemination of health alert messages. Programs such as the Epidemiology and Laboratory Capacity program (ELC) and the Emerging Infections Program (EIP) have helped states and local health departments begin to build the basic infrastructure and trained workforce without which advanced information systems cannot function. These initiatives are all complementary to each other, and funding and support for all of them must grow considerably so that the expected results can be achieved in as short a time as possible: we cannot afford to wait.

Finally, I want to thank you, Mr. Chairman, for the opportunity to testify this morning on this important topic. I am pleased to answer any questions the Subcommittee may have.

Mr. TOM DAVIS OF VIRGINIA. Dr. Wiesner.

Dr. WIESNER. Good morning, Mr. Chairman, and members of the subcommittee. I am Dr. Paul Wiesner. I'm the director of the Board of Health in DeKalb County, GA. I'm pleased to present testimony here today on behalf of the National Association of County and City Health Officials. That's the organization that represents the nearly 3,000 local health departments in the United States.

CDC had the foresight to establish three local Centers for Public Health Preparedness in late 1999, and we're fortunate to direct one of those centers. This morning I'm going to focus only on two of the lessons that NACCHO has learned about dissemination of information and building public health infrastructure through the Health Alert Network.

The timetable for achieving the goals stated in CDC's report that the chairman mentioned earlier must be rapidly accelerated. Early detection and a timely response to a bioterrorist attack depends upon a solid local and State public health infrastructure. This infrastructure requires a crucial array of capacities: a trained work force under top-notch organizational management; partnership building; systems readiness; epidemiological laboratory and surveillance expertise; information and communication systems; and the ability to develop local programs and local policies.

Without the fundamental capacity which we call infrastructure, the local health department is unable to address the regular community health problems that exist in the community, the threats that come from either infectious disease or environmental hazards, and certainly counter the threats from potential bioterrorism.

That same infrastructure that's used for all of the other practices of public health in our local community are the framework and foundation for preparation for bioterrorism. The local public health department in many ways is the linchpin of bioterrorism preparedness.

Now, today, the general population has an unprecedented understanding of the importance of public health but they have little grasp of the magnitude of transformation that is needed in public health practice nationwide. For all health departments in the country, capacities have not kept pace with the challenges. We must have a long-term initiative to restructure and rebuild the Nation's public health infrastructure at the State and local level as well as the Federal level, because only in that case will we have everyone in our communities protected.

Now, I'm going to talk about a second point that is a little bit more subtle and less direct than the infrastructure question, but it's no less critical. No one doubts the need for rapidly and accurately transmitting information vertically in the public health system, up and down between the Federal, State, and local public health agencies. That's absolutely vital. But what is just as important is what might be called the horizontal communication and transmission of information in all levels of government, and building those systems that communicate horizontally within our communities.

Substantial investments in technology and systems building are needed. The needs at this local level where I work, what I might call the retail level of public health, are substantial. We need real-

time surveillance systems on the ground, rapid secure and redundant communication at this level throughout the country, educational and training resources for us and our partners. And there are many within the local community beyond simply the hospital and the medical practitioner, well-trained public health investigative teams, local plans for pharmaceutical assessment and acquisition and distribution, and periodic testing of communication protocols technology in our overall local plan for bioterrorism response.

NACCHO's experience with the CDC-supported centers has demonstrated that there's one core element as far as that horizontal development, and that is partnership development. Improvements in technology must be linked to a horizontal system of solid, local relationships between public and private agencies.

Now, in conclusion, significant investments of people and money will achieve this new level of public health preparedness. Restoring the local public health infrastructure creates the sustaining foundation for preparedness. Threats to the public health do not respect jurisdictional boundaries, so if we're all going to be protected, every health department must be able to contribute to this. Sustaining this effort requires a commitment from all levels of government.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Dr. Wiesner follows:]

1100 17TH STREET, NW, 2ND FLOOR
WASHINGTON, DC 20036
(202) 783-5550
(202) 783-1583 FAX
WWW.NACCHO.ORG

NATIONAL
ASSOCIATION OF
COUNTY & CITY
HEALTH OFFICIALS

Statement of

**Paul J. Wiesner, MD**

**Director**
**DeKalb County Board of Health**
**Georgia**

on behalf of the

**NATIONAL ASSOCIATION OF COUNTY AND CITY HEALTH OFFICIALS**

before the

**Subcommittee on Technology and Procurement Policy**

**Committee on Government Reform**

**United States House of Representatives**

December 14, 2001

Good morning, Mr. Chairman and members of the subcommittee. I am Paul Wiesner, M.D. I am the director of the DeKalb County Board of Health. The Board of Health is the local public health agency serving the 665,000 people living in DeKalb County, the most densely populated and most culturally diverse county in Georgia. DeKalb County has two distinctions related to today's testimony. First, the headquarters of the U.S. Centers for Disease Control and Prevention (CDC) is located in our county. Second, under the leadership of our County CEO Vernon Jones, DeKalb County has established a local Director of Homeland Security. Along with Monroe County, New York and Denver, Colorado, our agency directs one of three local Centers for Public Health Preparedness supported by the Health Alert Network (HAN) program. This funding comes from the Public Health Practice Program Office at CDC. I am pleased to present testimony here today on behalf of the National Association of County and City Health Officials (NACCHO) – our national organization that represents the nearly 3,000 local public health departments in the United States.

CDC had the foresight to fund these three Centers for Public Health Preparedness in late 1999. That same year CDC began a study that culminated in a landmark report on the Status of Public Health's Infrastructure in the nation. How our world has changed since then!

The timetable for achieving the goals of that report must be rapidly accelerated. Our nation cannot wait until 2010 for each and every health department to have robust information and data systems. While that original timetable may have been appropriate prior to recent events, it now simply does not meet the urgency of the moment and the reasonable expectations of our communities.

Early detection and a timely response to a bioterrorist attack or any other public health emergency depends on a solid local public health infrastructure. Infrastructure means having not only sophisticated modern information technology but also a highly trained workforce under topnotch organizational leadership. Such an infrastructure will use technology effectively and form the partnerships so critical to sustaining a local system of preparedness. Specifically, that infrastructure represents the capacity of a local health department to:

- detect a bioterrorist event;
- investigate and determine the source;
- evaluate exposure;
- administer vaccines and medications; and
- communicate with the media.

Congress has an historic opportunity to redress decades of neglect of our nation's local public health systems by providing the CDC with sufficient funds for rebuilding the local public health infrastructure that is so critical to our nation's ability to respond to bioterrorism. The sooner we start the better. To accelerate the timetable requires substantial new resources and continued leadership, not only from CDC, but also from state health departments and from my colleagues in local public health.

**Lessons Learned from the Health Alert Network Program**

NACCHO and local public health agencies have learned important lessons about timely information dissemination and infrastructure building supported by the Health Alert Network (HAN).

1. Public Health Infrastructure and Public Health Preparedness. There is a very positive synergy between an investment in bioterrorism preparedness and investments in rebuilding broad local public health infrastructure. Preparing for bioterrorism also prepares us to address other public health threats. For example, handheld computers for field data collection in Denver will be used not only to respond to bioterrorism but also for daily communicable disease surveillance and in assisting outreach and routine monitoring of medication adherence for HIV care. DeKalb used the same 800 MHz radios in responding to potential anthrax incidents that it acquired and used when West Nile virus was discovered in our community. In Monroe County, a hospital status board and messaging system has multiple uses for disease surveillance and communication in addition to preparation for bioterrorism. We have demonstrated that every dollar we spend on bioterrorism preparedness pays off in many other ways.

2. Changing Organizational Cultures to Use Technology. Effective use of enhanced technology requires overcoming significant cultural challenges. These challenges include issues such as traversing the boundary between private medical care and public health agencies and addressing confidentiality and privacy concerns. Moving information across multiple private and public medical care systems will, in some of our communities, mean crossing a chasm. There is a natural tendency for the partners within a community (hospitals, doctors, and others) to be, correctly, very protective of their computer networks and wary about sharing information. Public health must provide the leadership in bridging this gap. Public health workers must be equipped not only with an understanding of communications technology, public health epidemiology, and laboratory diagnosis but, even more importantly, with high level skills in leadership, project management, negotiation, convening stakeholders and forming new and trusted relationships.

3. Sustainability. We must focus on sustainability of enhanced communication and information systems. Continuous training to achieve and maintain technical expertise and the installation of technical systems are necessary, but insufficient. Sustainability requires commitment at all levels of government, recognizing that a strong local public health system anchored by a strong health department is as essential to the protection of each community as are fire and police departments.

4. Partnerships are critical. Partnership development is often viewed as an ancillary part of planning for bioterrorism response. However, NACCHO's experience with its CDC supported centers has demonstrated that community partnership is *the core ingredient* for improving the capacity of communities to protect their residents.

   One particularly complex issue is the partnership between medical care and public health. Clinicians in community practice are traditionally oriented toward treatment and providing medical care to individuals. Public health, on the other hand, focuses on prevention and populations. Local communities can achieve true preparedness only by forming partnerships between local healthcare providers and local public health agencies. All around the nation medical care institutions and public health agencies are under stress. Declines in

reimbursement rates and increases in services to the uninsured strain financial resources that might otherwise be devoted toward fulfilling their role in local preparedness.

The events following the September 11th terrorist attacks, including the recent anthrax incidents, have reawakened both public health agencies and medical care providers to the need to work together to prepare our communities for these threats. Events that once seemed remote or inconceivable now draw together many important members of the local public health system. Many clinical providers are turning to local public health to provide leadership and guidance on these issues. Every local health department must have the capacity to provide this leadership and guidance.

5. Defining Public Health Role as First Responders. Public health agencies have not always been identified locally or nationally as first responders in disasters, and are often left out of disaster planning activities. The functions for which public health leadership, expertise and resources are necessary in identifying and responding to bioterrorism have become more clearly understood in the three preparedness center communities, as they have nationally since the anthrax outbreak. The next task is for every community nationally to define the distinct roles of first responders, the medical community, and public health professionals, and to do so before an event occurs.

6. Strengthening internal operations. In each of CDC's HAN local centers, the investment in bioterrorism preparedness has had significant positive influence on internal operations of the overall agency. An atmosphere of continuous learning has been established. In many cases, these investments have yielded not only best practices regarding bioterrorism response for peer agencies, but also exemplary practice for other units within the health department.

7 Tabletop exercises. Tabletop exercises provide invaluable opportunities to formulate and test a plan and measure preparedness capacity. Each of the centers conducted tabletop exercises and other simulation activities during their first year. These activities varied greatly between the sites depending on the purpose of the exercise. With these exercises came the development of numerous partnerships, and operational and political benefits. The Denver

Center has been recognized as a preparedness leader with their involvement in the exercise for top officials (TOPOFF). The Monroe Center has been asked to assist in developing drills for state and hospital emergency departments. As a result, the Monroe Center has now been invited to provide lectures on their tabletop exercises and exercise design using a videotape and script of a drill developed by the Monroe Center.

While the Centers have continued to conduct and host tabletop exercises, they also continued to identify areas for collaboration and measuring preparedness capacity using the findings from these tabletop exercises. In terms of operational readiness, the Denver Center identified numerous communication and surveillance gaps through involvement in the TOPOFF exercise. To address these gaps, the Denver Center attends monthly meetings with TOPOFF players to address identified problems and ultimately develop a communications plan. In helping the state hold a tabletop exercise, the Monroe Center identified numerous needs and gaps around interagency communications that are now being addressed.

Our own experience in DeKalb County over the last two years has been extremely positive. We have designed and delivered a series of "tabletop" bioterrorism educational and planning exercises to several local hospitals with extensive and enthusiastic participation on each occasion. These exercises are educational, not evaluative – they are designed to bring representatives from a variety of hospital departments in contact with local, state and federal public health, fire, emergency medical services, and law enforcement personnel, among others. We have used a series of realistic scenarios to uncover and explore key planning and response issues, each pointing the way toward future collaborative partnerships. A critical feature for us has been the creation of relationships with healthcare providers and other response sector personnel resulting in a new willingness on their part to participate in non-traditional surveillance systems involving hospital emergency rooms, EMS providers and others. New information systems that allow for the real time exchange of this disparate data are necessary to assure the early detection of a covert bioterrorist attack.

**Preparing the Local Public Health System**

An important prerequisite to achieving local public health preparedness is ensuring that local public health agencies have direct access to the information, the technology, and the resources necessary to engage other members of the local response community. A well-prepared local public health *department* is not the same thing as a prepared local public health *system*. Recent experience with anthrax incidents has not only focused attention on how different levels of government can work together more effectively, but has also awakened many agencies to the role of the local public health agency as a member of the first response community. Our own county's two-year effort to create a regional bioterrorism response plan resulted in establishing or enhancing relationships with representatives from over thirty (30) local response agencies. These agencies working together to assure the health of their community are the *local public health system.* The horizontal communication and rapid exchange of information among these agencies is a basic requirement during any emergency response.

When resources, technology and leadership are in place to support robust partnerships within local public health systems, efforts to create effective information exchange systems stand a much better chance of success. Local incompatibilities in interagency communications technologies present challenges and additional resources are necessary to resolve them.

Local public health agencies are uniquely positioned to compile, analyze and disseminate information critical to the public's health. Most hospitals, for example, are only aware of cases of communicable disease among their own population of patients. Many emergency medical services (EMS), fire and police agencies also receive information segregated by precinct or otherwise handicapped by delays in its acquisition. Clusters, trends, and patterns of significant disease events or exposure are more likely to be detected by a central entity able to view broadly the incidence of adverse health events within a community. This is a central responsibility of local public health agencies. The challenge is to establish collaborative information partnerships at the local level and bring together widely disparate information sources. This requires the development of secure information systems and highly trained staff to man them.

**Public Health and the Media**

It is not possible to overstate the value of an ongoing, positive, trusting and respectful relationship between local public health officials and the media. Even more importantly, that relationship must be in place long before an event occurs. As we have witnessed in the past three months, public health and the media are both at a disadvantage in the face of rapidly developing and unprecedented public health events. Public health's disadvantage is that, unlike the media, we have no longstanding, battle-tested system of rapid information collection, verification, and exchange. Consequently, the media suffers because, without such a system, the information they receive may be inconsistent, not current, and uncoordinated. Ultimately, it is the public that suffers.

An additional factor is the ease with which even large local public health agencies can be overwhelmed by media requests for information. As a case in point, although hundreds of miles separate my own county from the nearest recently documented human case of anthrax, our health department has faced a constant stream of local and national media inquiries on the subject. County incidents of perceived exposure to "suspicious" substances, numbering well over 50 to date, further fuel the interest of both the media and the public.

It is clear that interactions between the media and the local public health system must be accounted for in the continued development of HAN. The gaps between the media's ability to report such information and public health's ability to first acquire and process it needs to be narrowed. It is also clear that we need to do more than create systems that feed the media's desire for information. At our Center for Public Health Preparedness in DeKalb County we are exploring the development of a media educational tabletop exercise in which local members of the press receive instruction in how the local public health system will operate during threats such as bioterrorism. At the same time, public health stands to benefit from opportunities to learn more about the media's desires and methods of operation and through formation of relationships with local media representatives.

**Building on the Lessons Learned**

NACCHO, CDC and its exemplar centers all recognize that the lessons learned and the best practices developed will protect the public's health only if they are widely disseminated, incorporated into the infrastructure and daily practice of public health in every community, and continually improved.

NACCHO has been very active in disseminating information regarding local public health preparedness activities. Along with the CDC and others, NACCHO supports an annual HAN conference drawing wide participation from state and local public health workers. Additional information sharing has occurred via satellite educational broadcasts, Web-based resources and periodic national teleconference calls with leading public health authorities participating.

NACCHO and its member agencies are collaborating in a national effort with CDC to develop a set of Core Capacities for Bioterrorism Preparedness for local public health systems. Presently in draft, this document describes four key abilities that each local public health system needs to achieve as a measure of preparedness. These are: surveillance and epidemiology; laboratory; communication; and emergency preparedness and response. Also included are descriptions of how each capacity might be achieved, including training and technology considerations.

These capacities will not be achieved without significant investments of energy, money and time. Nor should they be seen as endpoints in achieving local public health preparedness. A broader nurturing and restoration of the local public health infrastructure will be necessary to sustain gains in local preparedness capacity. Finally, public health capacity must be increased at every local public health agency. As the nation's recent experience with anthrax has illustrated, threats to the public's health do not respect jurisdictional boundaries. As with bioterrorism and many other public health threats, if we are not *all* prepared then *none* of us is prepared.

Mr. Chairman, we are grateful for your interest and will be happy to provide any further information you may require.

Attachment: 11/5/01 Letter from Paul Wiesner, MD, to HHS Secretary Tommy Thompson

**Office of the Director**

DeKalb County
Board of Health
Richardson Health Center
445 Winn Way, 5th Floor
P.O. Box 987
Decatur, GA 30031

phone: 404.294.3700

fax: 404.294.3715

www.dekalbhealth.net

Paul J. Wiesner, M.D.
Director,
DeKalb County
Board of Health

November 5, 2001

The Honorable Tommy G. Thompson
U.S. Health & Human Services Secretary
U.S. Department of Health and Human Services
200 Independence Ave., SW
Washington D.C. 20201

Dear Mr. Secretary:

All of us at the DeKalb County Board of Health are very grateful that you found time in your busy schedule to visit us on Tuesday, October 30, 2001. We really appreciate the enthusiastic support you promise in rebuilding the local public health infrastructure of our nation.

I was proud to hear you say that you recognized the exemplary model we have developed here in DeKalb County. We acknowledge the support of CDC's Health Alert Network Program, the Public Health Practice Program Office at CDC, and your HHS regional office. Yours is an historic opportunity to rebuild the local public health infrastructure by replicating the best practice models developed here and at our sister exemplar sites in Rochester, NY and Denver, CO.

As you know well, the initial request from OMB for supplemental funding to address bioterrorism provides very little to strengthen local capacity to stop outbreaks of disease. Bioterrorism detection and response begins at the local level and cannot succeed without a strong local public health infrastructure. Senators Frist and Kennedy have recognized this clearly, and Congress last year passed their bill to build core public health capacities in a rational, accountable fashion. In addition to the Health Alert Network program, the White House should explicitly support a level of funding sufficient to implement Senators Frist and Kennedy's bipartisan bill fully and rapidly. Every community will then be protected from the consequences of bioterrorism by a public health system that has all necessary capacities.

A group of national public health leaders has reviewed the approach envisioned by Senators Frist and Kennedy and identified the need for $835 million initially to fund it. I support that figure as a starting point. Additionally, I shared with you the following rationale for funding needs for this initiative and the ways I would recommend directing the funding to the local health departments. The U. S. population is 422 times the size of DeKalb County's population (665,685). We invested more than $600,000 per year of CDC and HHS Regional Office dollars over the past three years to establish a good basic Center for Public Health Preparedness (CPHP). That amounts to 90 cents per person per year. Using a national population of 281.4 million, we need an investment of $253 million per year, and to sustain it for four years – a total of 1.012 billion (253X4=1.012).

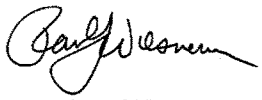
I suggest the following distribution of the $1.012 billion (federal dollars):

- Ten advanced CPHP in local health departments @ $1.5m per year = $60m over 4 years
- 130 basic CPHP in local health departments @ $.6m per year = $312m over 4 years
- Per capita investment of remaining funds = $640m over 4 years

I recommend a 2:1 match of federal funding to local/state funding, bringing the $640 million up to $960 million, and the overall investment to $1.332 billion over four years (or $333 million per year). I also strongly urge that you assure that all of the $333 million be dedicated to the local level of the national system. That is one third of the $1 billion annual investment recommended in the attached document. The enclosed document clearly outlines what our nation would receive from this investment.

On a personal note – the Wisconsin connection. I was pleased to see for myself why my brothers Tom and Frank speak so highly of you. You are not only a dedicated public servant, but an engaging and engaged leader. Neither I, nor my staff at the DeKalb County Board of Health, will forget your visit.

Sincerely,



Paul J. Wiesner, M.D.
Director

PJW/JB

Enclosure: Frist-Kennedy Public Health Infrastructure Enhancement Program: Potential Uses of Funds by State and Local Health Agencies

cc: Tom Wiesner
Frank Wiesner

Mr. TOM DAVIS OF VIRGINIA. Mr. Covert.

Mr. COVERT. Thank you, Mr. Chairman, members of the committee, staff members. I'm pleased to appear before you today. I'm Michael H. Covert, president of the Washington Hospital Center here in Washington, DC. I'm here today representing the American Hospital Association and its nearly 5,000 hospitals, health systems, networks and other providers of care.

One of our key readiness challenges is to foster stronger ties between the public health system and hospitals. Hospitals are a public safety asset. We need to better integrate hospitals into the public health and safety infrastructure to enhance our community's ability to respond to disaster. This will require a Federal recognition of the important role that hospitals and health systems need to play in coordinating community-wide efforts to deal with disasters, including potential agents of bioterrorism. And it will take a commitment of Federal resources to support efforts by hospitals and public health departments to access and distribute information and emergency alerts, monitor the health of communities, and help detect emerging health problems.

Let me share with you some of the lessons that we've learned from our experience in dealing with the recent outbreaks of anthrax in the Nation's Capital area. We learned that a lack of effective integration and communication between the Federal Government and our local health department early on stymied our ability to effectively plan the screening and monitoring of a large number of anthrax patients. By the way, we saw over 500. There was no regional tracking mechanism to capture information that could have been used for monitoring epidemiological trends. Each institution in the first days was left to its own devices to gather information on how best to treat patients and then in turn share it with the health department.

Many questions arose as to how to maintain the privacy and confidentiality of this data. These concerns will only be exacerbated by the new Health Insurance Portability and Accountability Act's medical privacy regulations.

Our experience in responding to anthrax cases also underscores the need for public health departments to be able to update hospitals continually on key developments, but the health department was often unable to do so, which affected our ability to plan for care and staffing.

Another potential problem is the jurisdictional issue. Who coordinates surveillance efforts to avoid duplication? In rural areas of the country, hospitals will need to play a larger role in performing many of the duties that a health department would normally perform. As a former health director, I know there were many communities that lacked resources and personnel to track and manage a mass casualty incident. There also needs to be better and more sophisticated gathering of data and operations of artificial intelligence capabilities to help evaluate patients who may be victims of a terrorist attack. Ideally, these systems should also tie into hospitals' electronic medical records.

Over and over again, the points of failure in a disaster response are the information and communications systems. Cell phones don't work. Land line telephone systems are overloaded. There are no

systems for tracking patient data on a regional basis. We need to invest a large amount of money to build an information and communications infrastructure that has capacity, redundancy, and robustness and includes all public safety agencies—police, fire, EMS, and hospitals.

Mr. Chairman, September 11th and the aftermath changed the way hospitals must think of disaster readiness. Hospitals must now prepare for what once was unimaginable. For example, the Washington Hospital Center will need to invest over $40 million to deal with current readiness needs today. One fourth of those dollars, between $8 and $10 million, are needed to be spent on information systems, communications, and technology. When you hear the request for significant funding by the AHA, they are very much on track, at least with what I believe what we are finding at the individual hospital level.

To strengthen community readiness, the AHA is pleased to be a part of a new coalition, the Partnership for Community Safety. The partnership includes public health officials, hospitals, fire chiefs, emergency physicians, emergency medical personnel, and nurse leaders: the heart of any community's front line emergency response efforts. I know that you recognize that.

In conclusion, hospitals are upgrading existing disaster plans and continue to tailor their disaster plans to suit individual needs of the community in the face of new threats. America's caregivers perform heroic life-saving acts every day, and in the face of the unexpected they can be depended upon to rise to the needs of their respective communities.

I appreciate the opportunity and look forward to answering questions.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Covert follows:]

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802

(202) 638-1100 Phone
www.aha.org

**Testimony**
**of the**
**American Hospital Association**
**before the**
**Subcommittee on Technology and Procurement Policy**
**of the**
**Committee on Government Reform**
**of the**
**United States House of Representatives**
**on**

**Public health system's capacity to respond to bioterrorism**

**December 14, 2001**

Mr. Chairman, I am Michael H. Covert, president of The Washington Hospital Center, Washington, DC. I am here today representing the American Hospital Association (AHA) and it's nearly 5,000 hospitals, health systems, networks, and other providers of care. We appreciate this opportunity to present our views on our nation's health care facilities' readiness to deal with a potential terrorist attack utilizing chemical, biological or radiological (CBR) weapons.

In its March 2001 report, "Public Health's Infrastructure: A Status Report," the Centers for Disease Control and Prevention (CDC) stated that public health surveillance systems still rely heavily on a time-consuming, resource-intensive "pony express" system of paper-based and telephone reporting. The report also noted the importance of standards-based information and communication systems that monitor disease and enable effective communication among public and private-health organizations, the medical, and the public. The report contains several recommendations to improve each health department's ability to access and distribute public health information and emergency alerts; monitor the health of communities; and help detect emerging health problems.

The AHA supports the CDC's recommendations on establishing robust information and data systems for public health departments. The best defense against public health threats is accurate, timely recognition and reporting of problems. Timely and easy access to information is key to applying effective countermeasures. That's why it is important for all health departments to move as quickly as possible to have:

- Continuous high-speed access to the Internet and standard protocols for data collection, transport, electronic reporting, and information exchange that protect privacy while seamlessly connecting local, state, and federal data systems;

- Immediate, on-line access to current public health recommendations, health and medical data, treatment guidelines, and information on the effectiveness of public health interventions; and
- The capacity to send and receive sensitive health information via secure electronic systems and to broadcast emergency health alerts.

America's hospitals and health systems also must be ready to withstand the threat of bioterrorism by maintaining a skilled workforce and a robust information and data system. We also need to strengthen are communication mechanisms and protocols to share information with, and receive guidance from, federal, state, and local health agencies.

I would like to take this opportunity to share with the subcommittee the Washington Hospital Center's experience with the recent cases of anthrax in the Washington, DC area, and some lessons we've learned. A lack of effective interaction and communications between the federal government and our own health department early on stymied our ability to effectively plan for the screening and monitoring of potential patients. We did not have a tracking mechanism to capture information that could have been used for monitoring and trending purposes epidemiologically. Each institution in the first days was left to its own devices to capture information on how best to treat patients and then, in turn, share it with the health department.

Many questions arose as to how this data would be maintained in a private manner. This will only be exacerbated by the new Health Insurance Portability and Accountability Act (HIPAA). Requirements for consent forms and restrictions on sharing of data related to patients will hamper timely care giving and follow-up treatment. Also evident was the need for the local health department to have round-the-clock capability to update surrounding hospitals on key developments. But that capability was not available and affected our efforts to plan for care and staffing. There also needs to be better and more sophisticated automatic gathering of data and operation of artificial intelligence capabilities to evaluate data on patients for irregularities. Ideally, these systems should be able to tie into hospitals' electronic medical records.

Mr. Chairman, September 11 and its aftermath changed the way hospitals must think of disaster readiness. Hospitals must now prepare for what once was unimaginable. Following a disaster, a hospital will have to be prepared to sustain intense demands placed upon them for the first 24 to 48 hours before federal resources arrive to supplement their resources. This means that all hospitals must:

- be integrated in the local public health safety infrastructure with public health, police, fire, and EMS;
- increase inventories of drugs, ventilators, respirators, and antibiotics to combat the effects of chemical and biological weapons;
- increase the supplies of gloves, gowns and masks – the basic ingredients needed to treat victims of a mass disaster and to protect health care workers;
- establish better communications with public health and safety entities to coordinate care;
- improve surveillance and detection to watch for potential outbreaks;
- add backup water supplies, auxiliary power sources and increased fuel storage;
- enhance their current decontamination units; and

- provide specialized mental health services not only to patients, but also to families, first responders, hospital staff and the general public.

I will discuss these issues in more detail later in my testimony.

On the issue of community readiness, I would like to note an important development that took place earlier this week. A number of organizations representing the nation's front line of response announced the formation of a new coalition to advocate for strengthening community readiness for biological, chemical and nuclear terrorism and other disasters. The AHA is pleased to be a member of the "Partnership for Community Safety: Strengthening America's Readiness."

The partnership's current members represent public health officials, hospitals, fire chiefs, emergency physicians, emergency medical personnel, and nurse leaders – the heart of any community's front-line emergency response efforts. In addition to the AHA, it includes the American Ambulance Association, American College of Emergency Physicians, American Organization of Nurse Executives, American Public Health Association, Association of American Medical Colleges, National Association of County and City Health Offices, International Association of Fire Chiefs, and the National Association of State EMS Directors. The Partnership will advocate for communities by engaging in public education and educating our respective members about best practices, by encouraging local coordination of all those involved in emergency response and by working together as field leaders to shape good public policy. Our goal is to support the men and women who must be there to respond to every kind of emergency.

While proposals pending in Congress represent modest first steps toward supporting readiness efforts, the Partnership will advocate for a comprehensive and sustained approach to community readiness. In addition to working together to help shape national policy, the partnership will promote collaboration among its members to retool disaster plans and focus on the need to increase capacity for responders to prepare for the new challenges of terrorism. Members agree that additional resources are needed to: improve communications infrastructure, community-based planning and disease surveillance, disease reporting and field laboratory identification systems; increase the community's capacity to deal with disasters; protect responders from the effects of biologic, chemical and nuclear agents; and enhance training programs, continuing education, and community drills for mass casualty incidents.

## HOSPITAL DISASTER PLANS

Hospitals nationwide, like those that directly responded to the September 11 tragedies, have disaster plans in place that have been carefully developed and tested. The plans are multi-purpose and flexible in nature because the number of potential disaster scenarios is large. As a result, hospitals maintain "all-hazards" plans that provide the framework for managing the consequences of a range of events. Hospitals conduct at least two drills a year: one may be focused on an internal event, such as a complete power failure. Another must be focused on an external event, such as a major highway crash, a hurricane or an earthquake. A hospital near an airport, for example, might focus on responding to an airplane crash, while a hospital near a nuclear plant or an oil refinery would focus on responding to the consequences of incidents at

those sites. It is important to remember that all disasters are local, and that local agencies and organizations must work together so that response mechanisms are tailored to the needs of their community.

A good example of how hospitals worked with their communities to prepare for a wide range of possibilities was the change of the calendar to the year 2000. Throughout 1999, hospitals across the nation engaged in a major preparedness effort: Y2K readiness. While Y2K was easier to address than mass casualty readiness, because it had a known time ... midnight of December 31 ... and place ... the hospital ... the consequences were unknown. Hospitals were ready.

Mass casualty preparedness is similar, because the possibilities are many. But it is also different because of its uncertainty. No one can accurately predict when such a disaster will occur, where it will occur, or what will be its cause and consequences. That is why the all-hazards plan, tailored to suit the needs of each individual hospital and its community, has provided an excellent framework for doctors and nurses forced into action by a wide range of events. Nowhere was this better reinforced than on September 11.

## SEPTEMBER 11: HOSPITAL REACTION

When hospitals in New York received the call to expect thousands of injured patients, triage teams were immediately set up, rehabilitation centers were transformed into auxiliary emergency rooms, and hundreds of off-duty nurses and doctors swarmed the hospital to offer assistance. Hospitals in New Jersey and Connecticut were also at the ready. In Washington, readiness paid off as regional hospitals in Virginia, the District of Columbia and Maryland launched into their disaster modes. And in Pennsylvania, facilities in the southwest part of the state were ready to provide care for victims of the airplane crash there. When the emergency plan went into effect, everyone was in their place, doing their jobs. Nurses, doctors, and others, working side by side, communicating effectively, relying on teamwork and training to assist the incoming wounded.

Different cities, different hospitals, hundreds of miles away from each other, each responding efficiently to a direct hit of terrorism. Each reacted in a positive, planned manner that not only saved lives, but also proved that America's health care heroes are dedicated, caring professionals who are ready for the worst of circumstances. The health care professionals and volunteers at all the sites were prepared to treat far more patients than actually came to them. Death tolls were simply too high, and health care workers grieved that they couldn't do more.

## LEARNING TOOLS

It is important to realize each incident is used to improve our preparedness. Disaster managers use the term "after action analysis" to describe the types of activities that are conducted to study what happened, what worked and what did not. The AHA and its state, regional and metropolitan associations work with our member hospitals to share throughout the field critical information that can be derived from responses to events. The following are important facts that we already know:

- By definition, a mass casualty incident, such as a terrorist attack involving biological, chemical or nuclear agents, would overwhelm the resources of most individual hospitals. Equally important, a mass casualty incident is likely to impose a sustained demand for health care services rather than the short, intense peak customary with many smaller scale disasters. This adds a new dimension and many new issues to readiness planning for hospitals.

- Hospitals, because of their emergency services and 24-hour a day operation, will be seen by the public as a vital resource for diagnosis, treatment, and follow up for both physical and psychological care.

- In disasters, hospitals become "safe havens" for first responders, victims and their families. Therefore, hospitals must be prepared to meet the basic non-health care needs of individuals, such as food, water and child care.

- To increase readiness for mass casualties, hospitals have to expand their focus to include planning within the institution, planning with other hospitals and providers, and planning with other community agencies.

- Traditional planning has not included the scenario in which the hospital may be the victim of a disaster and may not be able to continue to provide care. Hospital planners should consider the possibility that a hospital might need to evacuate, quarantine or divert incoming patients.

- Readiness could benefit from exploring the concept of "reserve staff" that identifies physicians, nurses and hospital workers who are retired, have changed careers to work outside of health care, or now work in areas other than direct patient care (e.g., risk management, utilization review). The development of a list of candidates for a community-wide "reserve staff" will require that we regularly train and update the reserves so that they can immediately step into various roles in the hospital, thereby allowing regular hospital staff to focus on taking care of disaster casualties.

- Hospital readiness can be increased if state licensure bodies, working through the Federation of State Medical Boards, develop procedures allowing physicians licensed in one jurisdiction to practice in another under defined emergency conditions. Nursing licensure bodies could increase preparedness by adopting similar procedures or by adopting the "Nursing Compact" presently being implemented by several states.

## BIOTERRORISM

The threat of chemical, biological and radiological agents has become a focus of counterterrorism efforts because these weapons have a number of characteristics that make them attractive to terrorists. Our recent experience with anthrax-contaminated mail is a grim reminder of that fact. Specifically, biological agents pose perhaps the greatest threat. Dispersed via the air handling system of a large public building, for example, a very small quantity may produce as many casualties as a large truckful of conventional explosives, making acquisition, storage and transport of a powerful weapon much more feasible. Some CBR agents may be delivered as "invisible killers," colorless, odorless and tasteless aerosols or gases.

The distinguishing feature of some biological agents--such as plague or smallpox--is their ability to spread. The initial victims become the source of infection to additional victims. The effects of viruses, bacteria and fungi may not become apparent until days or weeks after initial exposure, so there will be no concentration of victims in time and locale to help medical personnel arrive at a diagnosis. Exposure to biological agents may cause a variety of symptoms, including high fever, skin blisters, muscle paralysis, severe pneumonia, or death, if untreated. Many of the biological agents thought to be most likely to be used by terrorists have symptoms that initially resemble the flu or other common and less life-threatening illnesses. Therefore, the role of clinicians in quickly recognizing unusual patterns of symptoms and illnesses is critical to minimizing the impact of bioterrorism.

## HOSPITAL READINESS

Because September 11 redefined the meaning of disaster, hospitals are now upgrading their existing readiness plans to meet the new needs of their communities. Since the risk of chemical and biological attacks is now an obvious concern, hospitals are reassessing their current plans and incorporating elements to prepare for these kinds of treatment. The AHA so far has sent five Disaster Readiness Advisories to all of America's hospitals with information and resources to help them in this effort. The following are among the key items that we believe need to be addressed to help hospitals as they update their disaster plans to meet the challenges of a threat that, until recently, seemed hypothetical: an attack using chemical, biological or radiological agents.

**Medical and pharmaceutical supplies -** Hospitals must be properly stocked with antibiotics, antitoxins, antidotes, ventilators, respirators, and other supplies and equipment needed to treat patients in a mass casualty event.

**Communication and notification -** There is a need for greater coordination of public health and safety and hospital communications, and improvements in the ability of different entities to communicate with each other on demand. In addition, alternative and redundant communication systems will be required in case existing systems fail in an emergency.

**Surveillance and detection -** Improving hospital disease surveillance and reporting infrastructure will be critical to determining whether a cluster of disease is related to the release of a biological or chemical agent. The ability to rapidly identify the agent involved is vital.

**Personal protection -** Hospital supplies of gloves, gowns, masks, etc. would quickly be used up during an attack, and personal protective equipment like canister masks – used by those dealing directly with potentially contaminated patients – is rarely kept in adequate numbers to meet demands of a large casualty attack.

**Hospital facility -** Among the capabilities hospitals will need in the event of an attack: lockdown ability; auxiliary power; extra security; increased fuel storage capacity; and large volume water purification equipment.

**Dedicated decontamination facilities** - Hospitals need a minimal capability for small events and the ability to ramp-up quickly for a larger event.

**Training and drills** - Staff training is needed at all levels for all types of potential disasters. Additional disaster drills beyond the two per year required by JCAHO, particularly community-wide drills, would enhance the level of hospital readiness.

**Mental health resources** - Mass casualty events trigger escalated emotional responses. Hospitals must be ready to treat not only patients exhibiting these symptoms, but others, such as family members, emergency personnel and staff.

## COMMUNICATION / TRANSPORTATION ISSUES

To truly solidify response readiness, the federal government should help establish an emergency communication and transportation strategy. During the recent attacks, street closings and clogged roads impeded EMS workers as they tried to reach the affected areas, and hindered quick access to hospitals. No-fly zones were implemented to prevent other air attacks, but those zones hindered med-evac helicopters and other air transports that shipped blood and bandages to hospitals in dire need. Hospitals need assistance from Federal Aviation Administration officials to keep the skies open to critical medical aircraft.

In addition, any biochemical attack will require the coordination of local, state and federal agencies. In response, the Centers for Disease Control and Prevention have invested in and upgraded state-of-the-art labs to identify and monitor reports of suspicious cases of illness across the country. Working in conjunction with state and local epidemiologists, they will communicate their findings to government agencies.

## READINESS RESOURCES

Realistically, America can never afford to prepare every hospital in the country for every possibility of attack. However, the federal government can provide assistance to help ensure that hospitals and their local agencies are best able to respond to potential attacks. These funds would be earmarked to meet the challenges outlined above, including inventories of the necessary drugs and equipment needed to help victims of terrorist attacks. Communities need the funding to assist their hospitals and expand their emergency relief teams, as well as to establish or implement new systems of readiness.

## HOSPITAL CHALLENGES: WORKFORCE SHORTAGES

There is no more important strategy in this domestic war on terrorism than to help our hospitals reach a state of readiness. But if America's hospitals are to enhance their readiness for a new world of possibilities, they must have in place the people they need to do the job. However, America's hospitals are experiencing a workforce shortage that will worsen as "baby boomers" retire. Currently, our health systems have 126,000 open positions for registered nurses, for example. The United States Department of Health and Human Services predicts a nationwide shortage of 400,000 nurses by 2020. There also are shortages of other key personnel, such as pharmacists. This shortage cuts to the core of America's health care system, because dedicated, caring people are the heart of health care.

Fortunately, Congress has recognized the importance of this issue. Legislation has been introduced that can help hospitals attract and maintain the health care workforce that is needed to ensure that our patients receive the right care, at the right time, in the right place. For example, the Nurse Reinvestment Act (S.706/H.R. 1436) offers the right step to ensure health care professionals avert the collision course we face with lack of hospital staff.

## HOSPITAL CHALLENGES: HIPAA RESTRICTIONS ON INFORMATION SHARING

Hospitals have identified a serious conflict between the privacy regulations set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and efforts to improve hospital disease surveillance capabilities. The HIPAA privacy regulations place unnecessary roadblocks in the path of state hospital associations' efforts to share important health and demographic information with the hospitals in their states. The ability to continue to share such information could be critical to identifying an unusual outbreak of disease symptoms that could indicate that a bioterrorist attack has occurred. While the rules permit state hospital associations to aggregate and analyze medical data from their member hospitals, they would not allow hospital associations to share this "protected health information" from one hospital to another hospital. Further, while the regulations do include an exception that would allow public health agencies to collect "protected health information" without consent, it is not clear that state hospital associations would fall under this exception.

As a consequence, once the regulations go into effect in April 2003, state hospital associations would be barred from sharing critical disease surveillance data with contributing hospitals, thus undermining attempts at early detection of disease outbreaks. Among the data that hospital associations would be prohibited from sharing include county or neighborhood by zip code, specific age of the patient, and date on which the hospital treated the injury or illnesses – data that are critical to disease surveillance activities. At a minimum, HHS should either reform or clarify the rules to allow state hospital associations to share the critical elements of data with contributing hospitals and health researchers. This could be done most effectively by carving out those data from the list of identifiable data included in the rule. In addition, HHS should permit the use of a master business associate agreement under which all contributing hospitals could share such data with their state association.

## RURAL HOSPITAL DISASTER READINESS

While the possibility of a mass disaster may seem improbable in rural America, many areas in the rural United States have major hydroelectric dams, nuclear energy plants, military bases, and manufacturing plants that all could be potential targets for actions by terrorists. In these communities, the local hospital often represents the entire health care system for the community. Also, it must be recognized that the definition of what is a mass disaster is relative, depending on the size of the institution and community. For example, demand for health and hospital care by 200 people could overwhelm a 20-bed facility. Therefore, it is critical that rural hospitals be linked into community-wide disaster plans and continue to upgrade their internal disaster plans to reflect the new kind of threats the nation is facing. In order to be a part of disaster response,

rural facilities will need to have accurate and timely communications systems in place – including access to high-speed, secure networks.

However, due to a difficult financial environment, very few rural hospitals currently have access to such technologies as broadband or satellite networks. According to the March 2001 Medicare Payment Advisory Committee report to Congress, more than one in three rural hospitals have negative total margins. In addition to financial barriers, another impediment is that many rural communities cannot support the market necessary to access these technologies. With such a dire financial picture, rural hospitals and their communities face enormous challenges stepping up their readiness efforts and must depend on outside resources such as the federal, state and local governments, to provide them with funds and other resources to bridge the readiness gaps that currently exist in their facilities.

## CONCLUSION

The United States has been thrust into a new era by the great tragedies of the September 11th terrorist attacks. Our hospitals have always been ready for the foreseeable. Now we must plan for the previously inconceivable. Hospitals are upgrading existing disaster plans, and continue to tailor their disaster plans to suit the individual needs of the community in the face of new threats. America's caregivers perform heroic, lifesaving acts every day. And, in the face of the unexpected, they can be depended on to rise to the needs of their communities.

The AHA has worked closely with the administration on this important issue, especially with Secretary Thompson. We look forward to working with Congress as we help ensure that the people we serve get the care they need in any and all circumstances.

Mr. TOM DAVIS OF VIRGINIA. Dr. Carol Sharrett. Dr. Sharrett, thank you for being with us.

Dr. SHARRETT. Good morning, Mr. Chairman and committee members.

It's an honor to be here this morning to participate in the discussion on the response and information dissemination capabilities of our Nation's public health system to bioterrorism threat or incident. I'm Dr. Carol, Sharrett, a preventive medicine public health physician and the health director for the Fairfax County Health Department.

As the threats of bioterrorism a became reality, our Nation's public health system had to take the lead in protecting the population from disease. The recent rapidly evolving anthrax crisis challenged our ability to respond to new threats and to communicate quickly and effectively. By virtue of the size and capabilities of the Fairfax Health Department, we assumed the leadership role among the health departments in the northern Virginia region.

In collaboration with the Virginia Department of Health [VDH], and the Arlington and Alexandria health districts, we operated a health assessment and treatment clinic for residents of Fairfax, Arlington, and Alexandria who were potentially exposed to anthrax at their work site.

The Fairfax County Health Department routinely collects information on reportable communicable diseases. Other time-sensitive public health data including health alerts, guidelines, and protocols are received through e-mail, fax, and the Internet. During the anthrax crisis, communication between our health department and the State was hampered by temporarily inoperable e-mail systems at both the State and county level. As you recall, this was about the time of the Nimda virus, and Fairfax was hit hard by that. We therefore had to rely on an already overtaxed fax system to collect and disseminate information. The Inova Health System's disease—excuse me, Disaster Support Center gave invaluable assistance to the health department by cooperatively preparing anthrax-related information to blast-fax to all medical care providers including hospitals in the northern Virginia region.

We also provided anthrax information through the Fairfax County Web site with linkage to the Inova Health System, VDH, and the CDC.

On October 12th, the Fairfax Health Department, through partnerships with the medical community, State health departments, and the CDC put in an enhanced disease surveillance system and operation. This has been explained before so I won't go into that. Real-time information sharing occurred by the health department participating in daily conference calls with VDH and the northern Virginia health departments. Another call was with the District of Columbia Hospital Association, which had representatives from all of the metropolitan area hospitals, Council of Governments, the local and State health departments in Maryland, Virginia, and D.C., and we also had a daily conference call with the Fairfax County Emergency Management Coordinating Committee, which consists of 25 county agencies that have responsibility for emergency preparedness.

The anthrax crisis, as has been said before, was uncharted territory. Few health care providers had ever seen anthrax and, with its high fatality rate, they grew increasingly concerned about potentially missing a diagnosis. We received urgent requests from doctors asking what to do with the growing number of people who were demanding testing for potential exposures and what we would recommend for diagnostic procedures and post-exposure prophylaxis.

Initially the lack of CDC guidelines created both anxiety and inconsistency in patient care. Local medical providers and laboratory and hospital emergency staff were all clamoring for information. Although CDC staff were working at D.C. General and the other area hospitals which were treating anthrax patients, their focus was primarily an epidemiological investigation. As a result, the release of information to the State and local health departments was slow, often with relevant information being first reported on Fox Channel 5 or CNN.

We quickly set up a telephone information line to respond to the community's concerns. Calls from the public began right after the anthrax case in Florida was diagnosed, and the numbers increased dramatically after the Daschle letter on October 15th. Our public health nurses were trained to answer citizens' calls regarding anthrax, smallpox, suspicious packages and bioterrorism in general. They operated our health department anthrax information line from 7 a.m. to 11 p.m. This was 7 days a week. Between October 20th and November 16th, we received over 200 calls per day, with 400 at the height of the crisis. Some of these calls came from as far away as England and Germany.

We communicated with the public using anthrax and bioterrorism updates on the Fairfax County Web site and cable television station, anthrax fact sheets, town meetings on emergency preparedness, news releases, press conferences, and local media interviews. The media helped in publicizing the anthrax information line number as well as getting the word out on the regional health assessment and treatment clinic status.

The media reported much information before State or local health departments were made aware of it by the CDC. An example was the change from Cipro to Doxycycline for post-exposure prophylaxis. It became necessary for our communicable disease program staff to listen to NPR, CNN and read the Washington Post prior to reporting to work. Our anthrax information line was affected by the story of the day, requiring additional nurses on the phones to handle the flood of calls after evening news broadcasts.

The media occasionally reported inappropriate advice from television medical consultants as to which individuals needed treatment and testing based on potential exposure at work sites. The CDC formal guidelines arrived later, with the public near panic levels in the interim. Once again, the local emergency rooms, health care providers, and health departments were faced with citizens demanding unwarranted treatment, utilizing scarce resources which should have been conserved for those who were indeed at risk.

An example of media reporting that hampered the ability of the health department to adequately respond to the public involved

nasal swab testing. The media reported that the nasal swab was the test for anthrax when, in fact, CDC was using it as an environmental epidemiological tool. Individuals flooded local emergency rooms, urgent care centers, and other care providers. However, the nasal swab was of no use in determining whether an individual required prophylaxis or treatment. Nasal swab testing only overtaxed medical and laboratory resources, diverting them from medical care that was required during the anthrax crisis.

I notice I'm out of time. I'll just jump ahead since you all have——

Mr. TOM DAVIS OF VIRGINIA. Your entire statement is in the record.

Dr. SHARRETT. I'll go on to the conclusion. In conclusion, the CDC is to be complimented on their prompt epidemiological response to the anthrax crisis. And once medical information was released, it was excellent and extremely useful. Not having a clear understanding of who ultimately was in charge of the unfolding crisis, I believe, was the major reason communication was delayed.

The health of the public can be preserved optimally in the event of a biological attack only with a strong, clear, communication leadership role by the CDC. Controlling the panic that naturally occurs in such a crisis is a primary role of public health. I believe the public would have been better served had the CDC given daily updates on national television to the public and to the medical care providers.

Despite our perceptions, the anthrax crisis unfolded relatively slowly, but had this been smallpox instead of anthrax, our slow transmission of information would have been devastating, with rapid spread of the disease and increased mortality.

The cooperation and collaboration on the local level was extraordinary, with everyone involved providing service to the point of exhaustion, as I'm sure was true throughout the region and also for VDH and CDC employees. To effectively respond to future crises, it is evident that local, State and national public health agencies need additional funding for personnel, training, equipment, supplies, and systems development. Our current capabilities will not adequately protect the public.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Dr. Saunders.

Dr. SAUNDERS. Mr. Chairman, members of the committee, thank you very much for the opportunity to address this group. I would like to speak to you today from a couple of perspectives. The first is as a businessman and president of EDS Health Care Global Industry Group, a company involved with large-scale information technology services. The second, though, is as a physician with a long career in disaster management; having served, for example, for many years as a medical director of the city and county of San Francisco's Department of Public Health Paramedic Division 911 Medical Response. I have been involved in many disasters and multi-casualty events, including managing the medical response to the Loma Prieta earthquake.

Also on September 11th I was at the World Trade Center when the first plane hit, and I spent the duration of that event partici-

pating in that incident, including providing emergency medical care to victims at the scene. So I do have some unique perspectives, I think, both from a practical standpoint and also from an IT perspective.

First of all, a couple of lessons learned. No. 1—and the first thing I'd have to say is I'm always in awe of the American spirit and the resilience and the courage and the compassion and the initiative that individuals undertake these times, and I'm proud to be an American. And that needs to—can't go without saying. But the second thing is that disaster—organized disaster plans are nothing more than educated guesses at the hand you'll be dealt. Oftentimes reality is different. The key to success is fluidity and adaptability of the response, and the key to success there is information and communications. This is exactly where our public health system falls down.

Emergency care workers have no method for providing information in real-time about what's happening from minute to minute in their health care environment. So, the surveillance information that's real-time is lacking. There's no method for rapid dissemination of that information—not only about bioterrorism, but hazmat incidents. In fact, at 2 a.m., if I have a child bit by a dog, I don't know if there's rabies in my community because there's no easy way to access that information at the point of care. There is no effective and reliable way to keep your pulse on the status of our health care capacity, bed capacity, ambulance distributions, the availability of health care personnel and materiel.

And, finally, health care workers are unprepared to deal with rare, but critical events: bioterrorism, hazmat materials, things that they see rarely and perhaps hear about once in medical school, but aren't prepared for.

EDS supports the recommendations of the CDC and the E-health initiative. In fact, I'm on the leadership council of that group. We support the recommendations for a Web-based system for real-time surveillance, including linkage to relevant information systems at the point of care. We also support a mechanism for rapid dissemination of information outbound to health care workers. But I would further add that we can build on that with some additional things to keep in mind that would be of benefit.

No. 1 is a very effective method for Web-based distance learning at the point of care, at the time that it's relevant, when care is being delivered, so the health care workers can understand how to treat these victims. Another is a mechanism for event tracking of both victims and the impact.

At the Loma Prieta earthquake, my colleagues and I published a study of the impact of that, and it took months of research, combing through ER log records to find out, in fact, how many casualties there were and what the distribution was. That's too late to be effective for decisionmaking.

Capabilities for monitoring and allocating health care resources are needed so we don't have 200 physicians showing up at a hospital to take care of victims who all happen to be across town.

And finally, security hardening of our information infrastructure for health care information is also needed. That means redundant systems, hot backups, hardened facilities.

There will be challenges in the implementation of this. First of all, development and maintenance of the applications and the content. Second, integration to the relevant systems in the care environment, whether it's lab systems, the hospital information systems or registration logs and so forth will be difficult. It will be time-consuming and it will be complex. There will be maintenance required on the interfaces.

The education and training of health care workers so we understand how to interface with these systems and how to extract value from them will be a challenge. The policies around privacy and security and access to that information: who's appropriate, who's authorized, and when. And then the business process changes. We have to learn that instead of mailing in a 3-by–5 card to report a reportable event, now we go online to provide information.

So success, in conclusion, will be based on an effective partnership between the public private sectors of health care, as well as the information technology business community. I think that when these occur—and it will be a journey—it will be of great benefit to us all.

I thank you again for the opportunity to be here.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Dr. Saunders follows:]

**Testimony**

**of**

**Dr. Charles Saunders**

**President, Healthcare Global Industry Group, EDS Corporation**

**Before the**

**Subcommittee on Technology and Procurement Policy**
**Committee on Government Reform**

**U.S. House of Representatives**

**Washington, D.C.**

**December 14, 2001**

Thank you, Mr. Chairman and members of the Subcommittee on Technology and Procurement Policy.

It's an honor to be here representing EDS and the global information services industry at the hearing on "Battling Bioterrorism: Why Timely Information-Sharing Between Local, State and Federal Governments is the Key to Protecting Public Health." I am pleased to speak with you about how digital information sharing can help enable a secure and rapid-response public health infrastructure.

The challenges certainly confronted us before September 11 as evidenced by the report, "Public Health's Infrastructure: Every Health Department Fully Prepared; Every Community Better Protected." Published in March this year by the Centers for Disease Control and Prevention (CDC), the report focused on the shortcomings of the U.S. public healthcare system and recommended a course of action.

CDC's vision of a 21st century public health infrastructure is one we share at EDS. Those of us in private business and public service have a joint responsibility to:

- Unite healthcare professionals and agencies on a secure, shared electronic network;
- Put in place common-sense business practices to make it work easily and efficiently;
- Create real-time mechanisms to educate, equip authorities and alert citizens to potential health risks.

After September 11, the imperatives for improvements—both short- and long-term—to our public health infrastructure escalated. The General Accounting Office's report in September further confirms the urgency and the scope of the task before us.

In essence, we must connect—and digitize—the disparate dots of public healthcare.

**First-Hand Knowledge**

Today, I speak to you from a couple of different perspectives. The first perspective is as a former emergency medical services director and a physician of almost 20 years. The second is as a businessman who knows the power information technology can bring to healthcare.

In both jobs, I've seen disasters and the healthcare responses. From 1988 through 1994, I worked as an emergency physician and was the medical director for the City and County of San Francisco's Department of Public Health's Paramedic Division, which provided 911 medical response to the City. During this time, I was involved in and directed the City's EMS medical response efforts to numerous multi-casualty events and disasters, including the Loma Prieta earthquake, which devastated the Bay Area, killing approximately 270 persons and injuring more than 1,400. I also helped develop the disaster and hazmat response plans for health centers and municipalities, including the University of Colorado Medical Center, which provided emergency medical support for the Rocky Flats Nuclear Arsenal.

Although I have more recently been involved in the business aspects of healthcare information technology, I was recently drawn back to the edge of tragedy by circumstance. On September 11, I was on the street adjacent to the World Trade Center when the first airliner crashed into the building. My colleagues and I dodged falling debris and took shelter in a nearby building, where I provided emergency treatment in a make-shift basement aid station following the collapse of the two towers. Outside, medical and emergency workers risked their lives to rescue thousands of the injured and dying.

As if the trauma of that day wasn't enough, the anthrax scares and deaths soon began. You know that threat only too well in our nation's capital.

These events have taught us something. First, we are continually awed by the spirit of Americans and the limitless scope of individual courage and heroism and initiative and compassion and resilience. Second, we are reminded that disaster plans and response scenarios are little more than educated guesses at what hand the real world will deal us. Our pre-programmed responses must be fluid and adaptable. The keys to success are training, communication and timely information for minute-to-minute decision-making.

In healthcare, this is where we fail. We are sadly disappointed by the limitations of our healthcare infrastructure in responding to the situation—the greatest nation on earth cannot collect and disseminate timely public health information to its caregivers or its decision-makers. As a doctor, I can track stock market fluctuations on my cell phone, purchase a book on-line and track its shipping progress in real-time, and can watch a space craft land on Mars via the Internet. Yet, I remain unaware of critical events and outbreaks of dangerous diseases that might be flooding my emergency room. Our healthcare leadership is unaware of what my colleagues and I are seeing until months afterwards. I work remotely on a laptop computer more powerful than supercomputers of just a few years ago, armed with wireless e-mail access and digital knowledge sharing. Our public health system, however, relies on mailing 3x5 paper cards to report events, which are manually entered into antiquated systems that do not talk to one another and are not accessible by doctors and nurses who work in the trenches.

We can do better as a nation for the health of our people. Our doctors and nurses should not have to rely on CNN or word of mouth for critical public health information. Our healthcare officials should not have to rely on guesswork and luck to take the pulse of our healthcare system.

**Centers for Disease Control and Prevention's Report**

Reading the CDC's report, "Public Health's Infrastructure," one line stands out. It goes: "Either we are *all protected*, or we are *all at risk*."

It's really that simple—and that complicated. Healthcare is global. Diseases and terrorists know no geographic or political boundaries.

The report outlines the threats to public health in terms of infectious diseases, bioterrorism, occupational, and environmental hazards plus chronic illnesses.

To address the threats, we must close the gaps in public health workforce capacity and competency, upgrade information and data systems, and expand the organizational capacities of local, state and federal health departments and laboratories.

**Build on CDC's Recommendations**

CDC's desired state of a public health infrastructure can be realized through a secure, Web-based network that delivers real-time, shared information to virtually any public or private healthcare participant or enterprise.

CDC's vision, in part, parallels the thinking outlined by the eHealth Initiative consortium, as well as our business and technology experts at EDS' Healthcare and Government Global Industry Groups.

The eHealth Initiative is a non-profit organization of more than 60 leading healthcare and technology companies. EDS is a member and I serve on its leadership council.

These companies banded together to improve the quality and cost-effectiveness of healthcare through information technology. September 11 gave us the impetus to expand the use

of digital information and Internet-based communications to help ensure a fast, effective response to large-scale bioterrorism.

The consortium is offering public-private sector collaboration to improve the public health infrastructure and the nation's response to bioterrorism. This initiative builds upon existing healthcare information systems and data streams within America's hospitals and public health systems. By augmenting existing systems, surveillance efforts can reduce the need for double-entry by our nation's physicians and healthcare professionals. This eHealth blueprint calls for:

- Collaborating with federal officials to provide an integrated IT and communications system accessible to federal, state and local agencies, healthcare providers and payors.
- Creating a communications backbone with the Internet and existing hospital IT networks to:
  - capture clinical disease surveillance information at the point of care in real-time;
  - rapidly disseminate information to providers and other public health groups about dangerous disease outbreaks and bioterrorist threats.
- Leveraging existing IT and the National Electronic Disease Surveillance System (NEDSS) to improve real-time responsiveness to threats in our country.

Soon after the September 11 attack, EDS' Healthcare and Government Industries put together a series of recommendations to mitigate terrorism. Many of these are based on work we've already done for our clients. These initiatives include:

- Integrated Web-based systems for disease surveillance and reporting;
- Integrated communications networks for tracking availability of medical capacity and materiel;

- Knowledge management tools educating healthcare workers to diagnose and treat the sick, especially in cases involving dangerous diseases or those involving threats to the public health;
- Biometric technologies identifying victims and hunting down terrorist suspects, including consideration of electronic DNA data banks; and,
- Network hardening to secure critical elements of our healthcare communications infrastructure and data.

During any widespread threat to public health, two areas need the most support. First, you must have your finger on the pulse of your healthcare system to become aware early in the event, and then you must rapidly communicate news about an attack or infection to other healthcare authorities and care providers. You also have to track the capability of the medical system to respond, which means bed capacity, availability of healthcare personnel, drugs, blood products and medical supplies and equipment. This must be part of an organized command-and-control capability that allows for rapid redirection of healthcare resources where and when they are most needed, and for distribution of victims among healthcare facilities, so as not to overwhelm local resources.

Second, you must provide healthcare workers with the knowledge and on-the-spot training they need to render care. Diseases that threaten the public's health are often as uncommon as they are deadly. This means that most healthcare workers may not be prepared nor sufficiently expert in diagnosis and treatment, and may have little time to react. They must have knowledge resources at their fingertips, available at the point of care, 24/7.

The good news is the information technologies exist today to do this work. What's required is adding a dimension or two to the capabilities to fortify the public health infrastructure and combat terrorism. This becomes the digital public health infrastructure.

EDS understands—from a worldwide perspective—the complexity of the issues before us, remembering: "Either we are *all protected*, or we are *all at risk*."

We endorse the shared vision of a "virtual" public health infrastructure that unites local, state, federal—and global—government agencies, as well as private hospitals, physicians and laboratories.

EDS is moving in this direction—along with some of our clients—on several initiatives to make this vision a reality. We believe these initiatives will contribute toward creating the desired state of a connected and responsive public health infrastructure. In addition to the public health surveillance and reporting system, which I have already described and is at the forefront also of the eHealth Initiative, several other initiatives would be important considerations in our overall bioterrorism mitigation strategy. Let me describe these in more detail.

**Global Hazmat/Medical Care Knowledge Management and Event-Tracking Systems**

The first is a hazardous material/medical care knowledge management system and an event-tracking system. The idea is to develop and deploy a Web-based system to give healthcare workers the necessary information to diagnose and treat victims of chemical and biological terrorism in real-time.

Healthcare workers have little experience in peacetime treating victims of bioterrorism, or for that matter, of hazardous materials spills and environmental disasters. Often, they lack the information needed to quickly diagnose and treat casualties. Biological conditions, including

anthrax and smallpox, are normally unfamiliar to most healthcare workers. Hazardous materials, such as nerve gas and nuclear agents, are slightly more familiar—but only for specially trained individuals.

Some regional poison centers provide this information. However, poison center coverage in the United States is spotty. The information is not uniform and coverage is not global in scope. A worldwide, standardized system for rapidly disseminating state-of-the art treatment knowledge is needed, along with a registry for capturing information on events and victims and reporting on treatment outcomes and disposition of victims.

A Web-based system would disseminate medical information and education about the emergency evaluation and treatment of victims of biological and chemical terrorism. This includes data-search capabilities and on-line learning resources.

The system also registers victims and can provide reporting back to government agencies on statistics and incidents.

**Global Healthcare Materiel Tracking System**

Another initiative involves creating and implementing a system to track and deploy healthcare resources and materials in mass-casualty situations using Web-based technologies. Rapid deployment is critical for pre-event planning and post-event response.

A secure, Web-based system would monitor, order and track available healthcare personnel, medical equipment and supplies such as blood, vaccines, antidotes and medical equipment. Such a system could be part of an overall command and control capability for managing allocation of resources and victims within a geographic area.

**Biometric Human Identification System**

The third initiative is a biometric human identification system. This system would rapidly identify victims and terrorist suspects by using biometric technologies—with links to healthcare and law enforcement data.

Quick identification of victims and terrorist suspects requires positive identification. Current methods are cumbersome, time-consuming and can be falsified. New biometric technologies are available such as fingerprint/hand-scanning, face-scanning and retinal-scanning. They are virtually foolproof, although in a healthcare setting, some biometrics are not easily obtainable. Trauma victims with facial or limb trauma, for example, may pose a problem for scanning equipment. Of course, the gold standard is DNA. Biological material can be obtained from any victim. The technologies for DNA typing will evolve rapidly to enable near real-time analysis and codification into electronically bankable DNA fingerprints or signatures. At some point, we should consider the addition of electronic DNA data to provide an air-tight means of identifying individuals, both for security and law enforcement, and for forensic purposes in the identification of remains and body parts.

All forms of biometric data can be linked to softer forms of data. These include healthcare information such as medical claims, laboratory work, prescriptions and demographic data. They allow healthcare personnel—civilian and military—to deliver appropriate treatment under circumstances in which the person's identity cannot be established.

The system provides a registry of casualties that can be used as a global medical record during the treatment and post-event phase. It can be employed to quickly identify terrorists by linking to law enforcement and intelligence data.

EDS has implemented proven systems for biometric identification of individuals in airports and other settings using facial and palm scanning technologies. It can be adapted to incorporate DNA data, and can be linked through a unique identifier to a myriad of healthcare, law enforcement and intelligence data.

**Conclusion**

The September 11 attack on the World Trade Center and the Pentagon changed our lives and culture forever. How much it changes our way of life is, to some degree, up to each of us.

Those of us in private business and public service have a responsibility to do whatever we can, wherever we can, to prepare and be ready to act.

Wielding a powerful public healthcare infrastructure is one of the most effective ways to fight this new threat. Our work in this area is one of the ways EDS will contribute to homeland defense.

I would like to again thank you, Mr. Chairman, and the Subcommittee members for the opportunity to speak with you today. EDS would welcome any future opportunity to participate and contribute to improving our public health infrastructure.

eHealth Initiative

**Contact:** Ticia Gerber
202.663.8711
ticia.gerber@ehealthinitiative.org

**eHEALTH INITIATIVE AND CDC LAUNCH COORDINATED EFFORT TO ENHANCE BIOTERRORISM PREPAREDNESS AND RESPONSE**

WASHINGTON, D.C. (December 14, 2001) – The eHealth Initiative (eHI), a non-profit consortium of more than 60 leading health care organizations and the Centers for Disease Control and Prevention (CDC), in partnership with the Joseph H. Kanter Foundation, today announced a collaborative effort to bolster the public health infrastructure and improve the nation's preparedness and response to a potential large-scale bioterrorism event. Supported by a grant from the Joseph H. Kanter Foundation, initial work will focus on leveraging current health care information technology (IT) systems and existing data streams within the health care delivery system, to enhance public health data collection, surveillance, and detection processes. "We welcome this public-private collaboration," said Claire Broome, MD, senior advisor on integrated health information systems at the CDC. "Because both CDC and eHI are committed to the coordinated use of IT to enhance the speed and accuracy of public health surveillance and response, we believe that by working together we can significantly enhance capabilities to protect public health."

This collaboration is significant because industry-leading members of eHI provide the hardware and software used in a majority of America's hospitals and many of the nation's clinical laboratories, managed care organizations, physicians' offices, and public health agencies. Together, eHI's members provide critical IT to over 80% of the nation's hospitals.

Russell Ricci, MD, general manager of IBM's Healthcare Industry business and Chairman of the eHealth Initiative, stated that "The combined capabilities of eHI members and the public sector can significantly improve and speed-up response to a public health threat. Our actions will enhance the public health infrastructure and also

**eHEALTH INITIATIVE AND CDC LAUNCH COORDINATED EFFORT –page two**

serve as a critical step in improving the quality, safety, and cost-effectiveness of the *entire* health care system."

Seed funding for the initial work will be provided through a grant from the Joseph H. Kanter Foundation. Businessman, philanthropist, and president of the Foundation, Joseph H. Kanter stated public-private partnerships have been particularly effective in addressing the nation's challenges, as demonstrated most recently by his partnership with the Agency for Healthcare Research and Quality, which is focused on supporting better patient decision-making based on scientific evidence.

"Information is key to quality health care and statistically reliable data can be a powerful tool for combating the threat of bioterror," said Kanter. "The United States has the best health care system in the world, and by effectively sharing what we have learned through this collaboration with the world community, we can unite on this humanitarian effort and create yet another front in the war against terrorism."

eHI members and the CDC will work with providers and state and public health agencies to help identify critical public health data needs and develop strategies to rapidly and effectively capture and transmit such data, including information on specific laboratory and pharmacy transactions, emergency room visits, admissions, symptoms, and diagnoses, using CDC's National Electronic Disease Surveillance System (NEDSS). This work will take place under the Foundation for the eHealth Initiative and involve all critical stakeholders.

Randy Spratt, senior vice president, technology and standards of McKesson Corporation and an eHealth Initiative Board member said "The private sector is uniquely positioned to jump-start CDC's efforts to rapidly expand its surveillance and detection capabilities. Building on existing information systems within America's hospitals is the quickest and most powerful way to provide public health agencies with the data they need to improve preparedness and response".

CDC's Dr. Broome said, "Coordination between the CDC and eHI could permit the information systems of public health departments and a majority of the hospitals in the

**eHEALTH INITIATIVE AND CDC LAUNCH COORDINATED EFFORT –page three**

U.S. to operate in a more interactive, efficient manner that is consistent with national standards. This will also help us address our common health improvement goals."

Depending on the data elements selected, eHI members believe it will take anywhere from three to twelve months to make the necessary changes, once specifications have been identified. In addition, eHI has committed to working closely with providers, the CDC, state and local public health agencies, and other public and private groups to help clear other critical barriers associated with implementation. For example, eHI will help frame issues and develop the necessary safeguards to address privacy and security concerns.

Jon Zimmerman, Vice President for eHealth, Siemens Health Services, said, "Our systems already connect public health agencies to providers and patients throughout the country. We are prepared for and eager to work in this public-private partnership to improve our nation's preparedness and response across the entire public health care infrastructure.

Trace Devanny, president of Cerner Corporation said, "the technology is in place, the need is obvious. We are pleased to put Cerner's knowledge at the service of our country. We look forward to joining forces with our industry colleagues to make the country safer."

This initiative will not only help the public health system, it will do so in a way that results in less burden on providers. Peter Basch, MD, Medical Director for eHealth Initiatives of MedStar Health—a health care organization with seven major hospitals in the Baltimore-Washington region—said, "Coordinating efforts among public health stakeholders and the leading health care IT developers will help our nation's hospitals play their critically important role in surveillance and detection--by improving coordination and standardization and promoting efficiencies that will reduce the amount of burden placed on an already challenged health care system. "

**eHEALTH INITIATIVE AND CDC LAUNCH COORDINATED EFFORT –page four**

eHI members are also exploring other opportunities to improve the nation's preparedness and response through public-private sector collaboration, by leveraging current private sector health information systems and processes which focus on:

- Communicating with health care practitioners in their offices and at the point of care;
- Making the latest guidelines for detection and treatment directly available to a wider health care provider audience;
- Supporting provider follow-up and communication with patients; and
- Expanding efforts to educate the general public with uniform recommendations about prevention, symptom recognition, early detection, and treatment of bioterror-related illnesses.

***About the eHealth Initiative***

The mission of the eHealth Initiative is to drive improvement in the quality and cost-effectiveness of health care through the rapid discovery, development, and adoption of health care information technology. Members represent many of the stakeholders in the health care industry with interests in improving the health care system through the use of technology, including eHealth and technology organizations, health systems, health care providers, pharmaceutical and medical device manufacturers, service providers, and education/research institutions.

For more information about the eHealth Initiative and its preparedness and response strategy, call 202-663-8099 or visit www.ehealthinitiative.org. For more information on the CDC, visit www.cdc.gov. For more information on the Kanter Family Foundation, call 202-638-5687 or visit www.healthlegacy.org.

###

# eHEALTH INITIATIVE AND THE CDC IN PARTNERSHIP WITH THE JOSEPH H. KANTER FOUNDATION

## A PUBLIC-PRIVATE COLLABORATION TO IMPROVE THE PUBLIC HEALTH INFRASTRUCTURE AND THE NATION'S PREPAREDNESS AND RESPONSE TO BIOTERRORISM

**December 14, 2001**

**Overview of the eHealth Initiative-CDC Collaboration**
Through a public-private partnership, the Centers for Disease Control and Prevention (CDC) and the eHealth Initiative (eHI), supported by the Joseph H. Kanter Foundation, are now working on a collaborative effort to bolster the public health infrastructure and improve the nation's preparedness and response to a potential large-scale bioterrorism event. Initial work will focus on leveraging current health care information systems and existing data streams within the health care delivery system, to enhance public health data collection, surveillance, and detection processes.

eHI and CDC will work together with providers and state and local public health agencies to help identify critical public health data needs and develop strategies to rapidly and effectively capture and transmit such including information on specific laboratory and pharmacy transactions, emergency room visits, admissions, symptoms, and diagnoses, using CDC's National Electronic Disease Surveillance System (NEDSS).

This initiative is significant because industry-leading members of eHI (such as Cerner, McKesson, and Siemens) provide health care information systems for 80% of the nation's hospitals.

Depending on the data elements selected, eHI members believe it will take anywhere from three to twelve months to make the necessary changes, once specifications have been identified. In addition, eHI has committed to working closely with providers, the CDC, state and local public health agencies, and other public and private groups to address other critical issues associated with implementation, such as those related to privacy and security--by helping to frame the issues and define the necessary safeguards to address these concerns.

This initiative will not only help the public health infrastructure, it will do so in a way that results in less burden on providers. Because eHI's members provide critical health care information systems to so many of the nation's hospitals, this initiative will result in more coordination and standardization and promote efficiencies that will reduce the amount of burden placed on hospitals.

**The eHealth Initiative**
The eHealth Initiative and its affiliated organization, the Foundation for the eHealth Initiative are non-profit organizations. The mission of both organizations is to improve the quality, safety and cost-effectiveness of health care through the rapid discovery, development, and adoption of information technology.

The eHealth Initiative is a membership organization comprised of more than 60 leading health care organizations that was created to provide a unified voice for the health care industry on eHealth and technology-related issues. Its members represent many of the stakeholders in the health care industry with interests in improving the health care system through the use of digital technology, including eHealth and technology organizations, health systems, health care providers, pharmaceutical and medical device manufacturers, service providers, non-profit organizations and trade associations, and research institutions. Cerner Corporation, EDS, Guidant Corporation, HealthStream, the Health Technology Center, IBM, Johnson & Johnson, McKesson Corporation, Medtronic, SAIC, Siemens, and VHA Inc. and key health care providers such as MedStar Health and CareGroup Healthcare System are all eHI members

eHI's members either represent or have a large national base of clients that include most hospitals, providers, and significant portions of the general public, estimated at:

- 5,000 hospitals
- 370,000 practicing physicians
- 11,000 emergency medical personnel
- 30,000,000 web users

The Foundation for the eHealth Initiative, a 501©(3) organization, was created to serve as a national forum for the discussion of the policy issues relevant to the application of technology to support health and to articulate and execute a vision of a better health care system enabled by technology, to improve the quality, safety, and cost-effectiveness of care, as well as consumers' experiences with managing their health. The work of the public-private collaboration will take place under the Foundation.

**Why is the eHealth Initiative Engaged in this Activity?**
The mission of eHI and its Foundation is to drive improvement in the quality and cost-effectiveness of health care through the rapid discovery, development, and adoption of information technology. Implementation of this proposal would not only have a significant impact on the public health infrastructure, it would also serve as a critical step in improving the quality, safety and cost-effectiveness of care across the *entire* health care system.

**How Will this Initiative be Funded?**
Seed funding for the initial work will be provided through a grant from the Joseph H. Kanter Foundation. The President of the Joseph H. Kanter Foundation, Joseph H. Kanter, is a businessman and a philanthropist who believes in the power of a public-private partnership. He is accustomed to uniting the both the public and private sectors to drive

change and address the nation's challenges, as demonstrated by his work with the Agency for Healthcare Research and Quality on a national outcomes database, which is designed to support better patient decision-making based on evidence. This seed funding will be supplemented by funds received from both the private sector and the government.

**What is the Joseph H. Kanter Foundation?**
The Joseph H. Kanter Foundation is affiliated with the Kanter Family Foundation, an organization which acts as a catalyst and broker to encourage others to undertake outcomes research projects, and promotes efforts to foster public understanding that better treatment outcomes data will improve quality of care by reducing unnecessary treatments and medical errors.

To help patients and health care providers make better-informed decisions about how to tackle illnesses, the Kanter Family Foundation seeks to create an easily accessible, statistically reliable National Health Outcomes Database. This comprehensive and confidential database of patients' treatment experiences would help determine which treatments work best for specific diseases and conditions. The database would foster constructive communication between patients and health care providers.

To pursue its objectives, the Kanter Family Foundation co-founded a unique government-private venture, the Health Legacy Partnership (HELP), with the Agency for Healthcare Research and Quality (AHRQ), an agency of the U.S. Department of Health and Human Services.

Kanter launched the database project to address a glaring need in modern medicine: better information on treatment outcomes. Kanter's vision is to inform patients that they can improve their quality of life and health care by fostering relationships with their doctors to utilize evidence-based medicine and health outcomes research" - the study of "what really works" in treating illnesses.

**What is Unique About this Initiative?**
First of all, this initiative is unique because it is a public-private collaboration, which leverages the skills and expertise of both our nation's public health agencies and the private sector—an unprecedented and extraordinary combination that will result in significant gains for the public health system and all Americans.

Second, this initiative is unique because it calls for *building upon* existing health care information systems and data streams within America's hospitals (vs. creating something new). This is critical, because our hospitals and physicians are currently facing a multitude of healthcare issues. Coordinating efforts among public health agencies and the leading health care IT developers will help our nation's providers play their critical role in surveillance and detection by reducing the burden on an already challenged system. By augmenting existing systems, surveillance efforts can occur "in the background" and reduce the need for "double-entry" by our nation's busy physicians and healthcare professionals.

Industry-leading members of eHI involved in this initiative, including Cerner, McKesson, and Siemens, provide health care information systems for 80% of the nation's hospitals. By working together, they can effectively impact a large portion of our nation's health care information infrastructure.

Finally, this represents a critical first step towards greater standardization and interoperability. The power of combining a national need for interoperable systems with standardized data through CDC's NEDSS, with the vision of Joseph H. Kanter ,and with the expertise and leadership of the health care IT developers who provide software applications for 80% of the nation's hospitals is extraordinary and may provide the catalyst that is needed to drive greater interoperability—a critical barrier to a national health information infrastructure which is greatly needed to drive greater quality of care.

**Scope of Work**
Initial work will focus on leveraging current health care information technology systems and existing data streams within the health care delivery system, to enhance public health data collection, surveillance, and detection processes. The initial scope of work, as outlined in a Memorandum of Understanding between the CDC and eHI is summarized as follows:

- Explore utility of data currently in electronic format for bioterrorism detection and public health response.
  - ✓ CDC will identify selected data potentially useful to detect a bioterrorism event, which represent a range of data categories, such as data from emergency rooms, laboratories, pharmacies, and administrative data.
  - ✓ eHI will evaluate the high-level feasibility of and methods for rapidly capturing and transmitting specified data from hospitals.
  - ✓ CDC and eHI will conduct exploratory analyses to evaluate utility of data (e.g. geographic coverage, timeliness, baseline variability)
- Collaborate on developing an approach to providing access to expanded data of public health importance.
  - ✓ CDC and eHI will develop a process to involve public health partners to identify a more comprehensive set of data potentially useful to detect events of public health importance.

- ✓ eHI will work closely with providers, the CDC, state and local public health agencies, and other public and private groups to address other critical issues associated with implementation, such as those related to privacy and security--by helping to frame the issues and define the necessary safeguards to address these concerns.

- ✓ CDC and eHI will collaboratively develop strategies to assist in the rapid capture and transmission of data specified by the CDC and its public health partners from selected hospitals upon such hospitals' authorization, to state and local health departments, using the National Electronic Disease Surveillance System (NEDSS), which is designed to electronically facilitate the collection, management, transmission, analysis and dissemination of surveillance data.

**Who Will Be Involved?**
eHI and the CDC, supported by the Joseph H. Kanter Foundation, will work with providers and state and public health agencies to help identify critical public health data needs and develop strategies to rapidly and effectively capture and transmit such data, including information on specific laboratory and pharmacy transactions, emergency room visits, admissions, symptoms, and diagnoses, using CDC's National Electronic Disease Surveillance System (NEDSS). eHI anticipates that key stakeholders in the initiative will include:

- Public health-related organizations such as the National Association of County and City Health Officials, the Association of State and Territorial Health Officials, the Association of Public Health Laboratories, and the Council of State and Territorial Epidemiologists.
- Hospitals and health Systems
- Physicians, including general practitioners and emergency physicians
- Privacy organizations
- Health care information standards organizations
- Other governmental agencies.

**What is Needed to Make this Happen?**
First of all, two major steps have already been taken. First, the eHealth Initiative member companies have come together and have agreed to collaborate on this endeavor to support the CDC. Second, the CDC and eHI have also agreed to collaborate on this endeavor, with input from state and local public health agencies and other key constituencies.

Appropriate funding for the CDC and the state and local public health agencies will be required. The CDC's NEDSS system will need to handle significant increases in incoming data and analytical tools to utilize that data. It is imperative that funding for CDC and state and local public health agencies cover that which is needed for an *integrated* information system—one which addresses both the Health Alert Network and

NEDSS, as well as any other infrastructure required to support prevention, detection, and response.

Hospitals will also likely have additional costs, however, we believe that by building upon the existing infrastructure and using existing information technology systems and data streams, costs and time/effort on the part of the nation's hospitals will be minimized. Furthermore, changes that will result from this initiative will help to move the "interoperability" agenda forward—a critical barrier to greater digitization of our health care system—which is required to improve both the quality and cost-effectiveness of health care delivery.

Finally, leadership and coordination amongst the federal, state and local governmental agencies, such as CDC, state and local public health agencies, CMS, and other agencies, with significant input from the private sector, is critical for moving forward effectively.

**Key Imperatives**
To be successful this initiative must address the following key factors:

- Maintain a focus on both the larger public health and health care system benefits that can result from this effort.
- Engage the provider community.
- Engage public health at the federal, state, and local levels.
- Utilize a public/private partnership that leverages unique capabilities.
- Demonstrate rapid, concrete and significant results while moving towards longer-term goals.
- Demonstrate feasibility through demonstration projects at the state and/or local levels.

**Other Public-Private Sector Initiatives Related to Public Health**
eHI members are also exploring other opportunities to improve the nation's preparedness and response through public-private sector collaboration, by leveraging current private sector health information systems and processes which focus on:

- Communicating with health care practitioners in their offices and at the point of care;
- Making the latest guidelines for detection and treatment directly available to a wider health care provider audience;
- Supporting provider follow-up and communication with patients; and
- Expanding efforts to educate the general public with uniform recommendations about prevention, symptom recognition, early detection, and treatment of bioterror-related illnesses.

**How Does This Initiative Benefit the Overall Health Care System?**
Changes brought about by the public-private sector partnership will result in improvements across the nation's health care system. Not only will these actions enhance the public health infrastructure, they will also serve as a critical step in

significantly improving the quality, safety, and cost-effectiveness of health care throughout the *entire* health care system."

The health care systems faces many challenges today, including those related to quality of care, medical errors, rising medical costs, and a looming health care crisis. With the expansion of digital technology within health care, we as a nation, can begin to address many of these challenges.

Mr. TOM DAVIS OF VIRGINIA. Thank all of you for your testimony. We have a number of questions. I'm going to begin with Mr. Shays, who has belatedly joined our panel from Occoquan. I guess you're coming down in traffic. Thank you for being here. Of course, you've worked a lot of this in your other subcommittees. We appreciate you being here today.

Mr. SHAYS. Mr. Chairman, I am very grateful that you're holding this hearing and I thank you for putting together such an excellent panel. I have an opening statement which I would like included in the record. I would just ask my—I would first——

Mr. TOM DAVIS OF VIRGINIA. Without objection.

Mr. SHAYS. In regards to the public health's infrastructure, the status report that we're discussing today, I want to read one paragraph that just think says a lot to me. It's on page 8. It says: "work force demands on our Nation's public health information infrastructure has never been greater. Today, global travel, immigration, and commerce can move microbes and disease vectors around the world at jet speed; yet our public health surveillance systems still rely, in many cases, on time-consuming resource-intense pony express system of paper-based reporting and telephone calls."

I think that our world is under tremendous threat. Our country is. We basically have to protect ourselves from a lot of pathogens, just as we would protect ourselves from individuals or armies that might invade us. And the first issue I'm going to focus in on is the whole issue of monitoring. I'm led to believe, but I don't know if this is true, that we are in our—because I'm told it isn't, and I find when people respond to any questions that they're not doing it. Are we monitoring every major urban area's hospital, every day requiring them to give us the potential outbreaks that they might be encountering? So are we getting a handle on a potential outbreak? Because, obviously, if we do, then we have an easier time to respond. I throw it out to the panel and whoever would like to respond to it first would be welcome to. Could we perhaps, Doctor—with you, Dr. Sharrett.

Dr. SHARRETT. We do that daily with all of the hospitals.

Mr. SHAYS. You want to use your mic.

Dr. SHARRETT. We do that daily. And you're right, it is labor-intensive. But all hospital emergency room visits and the intensive care units, all of that is monitored. We do it not only for diseases, but for disease syndromes, so anytime there's any indication of something that would cause you to suspect that there is a potential for any bioterrorism agent, then——

Mr. SHAYS. Define to me "we." Is it we, every hospital, through their public health director or—who is "we"?

Dr. SHARRETT. We, the health department, in cooperation with the hospitals.

Mr. SHAYS. You call them up every day. Do you say, what's your count? Do they call you if you don't get——

Dr. SHARRETT. We physically have a nurse that is in every hospital every morning, or else in touch with the hospital every morning. But if there's something that we think needs specifically going over, we will go to the hospital and go to the record. But we get that information every day.

Mr. SHAYS. Mr. Regan—do I say it correctly, Regan? Among this panel I hope you realize you are first among equals. Hats off to you and the State for how you dealt with the West Nile Virus. Do you get involved in this issue of being aware of reporting, or do you only hear about it if there may be a particular problem?

Mr. REGAN. I get involved with it, particularly with working with our commissioner at the Department of Public Health, who again has outreach to the local hospitals and local communities, again, as the provider of the information technology infrastructure. Anytime there's a requirement for disseminating information through that infrastructure, I am hand in hand with the public health commissioner.

Mr. SHAYS. We did a table-top exercise in Connecticut, and they do it in other areas, where we—in this case, we had a practice where all the communities were involved, the State and the Federal Government, and it was a chemical outbreak in an Amtrak train. The thing that amazed me most was the—when we got all done, the firemen knew what they intuitively should do; the policemen, we learned that they were the canary in the coal mine. That was a shock to them, too, to realize the hit. But the one thing that stood out the most to me was the health people, the hospitals, our health directors, they were the ones who were just kind of in left field, not because—in other words, they knew how to treat, but they were treated like the stepchild, with no disrespect to stepchildren, but in other words, they were not given the kind of respect and attention they should get. Communication was by one, you know, phone that might not work. Their systems didn't coordinate with the fire and police.

Are we finding that is the case in other places besides Connecticut? Could someone speak to that?

Dr. WIESNER. From NACCHO's perspective, Congressman, there is an enormous need to improve the uniformity of capability and capacity throughout the country for doing the kinds of things that you're talking about. For instance, in our three Centers for Public Health Preparedness—one in DeKalb County; Rochester, NY; and in Denver—even in those places that have been working at this for a couple years, there are needs for improving just exactly what you talk about.

So there's an infrastructure improvement that is absolutely necessary. And the kind of description that you provide for it is, in the context, absolutely correct. I want to emphasize one piece, at least from our experience in DeKalb County, is that we take a view to this that we ought to be better prepared every day. I'm sure that's true in each health department. And so we build on past successes. We actually prepared for the Olympics and we had syndromic surveillance within our hospitals in 1996 around heat-related illness and working with the State on food-borne illness possibilities.

Then almost all of the local health departments in the country, to one degree or another, worked on the Y2K problem. And we have—and then, of course, when the East Coast in particular experienced the West Nile Virus presence, we worked with our hospitals to set up syndromic surveillance related to that particular effort. But it must be much more uniform, and the investment in both the technology and in the work force is absolutely critical.

Mr. SHAYS. Thank you. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. Mr. Covert, give us your assessment of the preparedness of America's hospitals to deal with infectious contagious diseases that come to the emergency rooms of those hospitals. I've often had the fear that a lot of hospitals would just be closed down if we had somebody walk in with smallpox, and that would be the end of health care for that community. Are they better prepared than I understand them to be?

Mr. COVERT. To answer your question directly, I think we're getting better prepared. I would tell you that I had some of the same issues myself in the past, and in looking at gearing up. I think we are today, not only from infection control standpoint, but also in caring for patients. However, let me also say that in terms of the actual infrastructure that might be required, let's say if a smallpox—an individual presented themselves smallpox, the ability to isolate that patient and then care for them, I think that's going to be a challenge for many hospitals. And it's one of the issues that we say ourselves that we're going to have to do a better job of physically gearing up for. Do we have medical capabilities and strong infection control programs? The answer is absolutely yes. I'm confident in that regard. But the key is putting these other pieces in place to be able to isolate and then support in care of those patients.

Mr. TURNER. I gather that the larger, more urban hospitals would be better prepared to deal with that than many of our rural hospitals?

Mr. COVERT. I think that would be a fair statement only because of the resources that are generally made available in those kinds of settings. It does not mean that there are not some strong—and as you know from Texas, some strong regional rural institutions, but I would answer your question by saying yes, those institutions that normally would deal with these kind of issues every day are going to be significantly better prepared in responding to the unusual kinds of biological agents that we might be seeing. A lot of the traditional infection, the flu, the other things that we would see, hospitals are prepared and do respond every day in that regard.

Mr. TURNER. Mr. Regan, I think—Mr. Shays is not with us, but I was curious; you made reference to the 90-year-old lady who contracted anthrax and died, and it was suspected that that she contracted it because of cross-contamination of the mail. Was that ever verified and was the path of that—of her mail—traced to the extent that it could have been determined whether it crossed the path of the letters that were sent here from New Jersey to Washington, or was that just speculation?

Mr. REGAN. It was not confirmed 100 percent, but there was a high probability that there was cross-contamination in that case, but could not be by the facts derived at the home—I don't think they could actually prove that they found any anthrax at her home.

Mr. TURNER. Was there an effort actually to track the path of that—of the mail that goes to her residence, to see if it went through locations where the letters that arrived here in Washington also may have traveled?

Mr. REGAN. Absolutely. In fact they were able to establish there was some cross-contamination through one of the processing centers in Connecticut from some of the mail from New Jersey. I think that's where they suspect that there may have been the cross-contamination that ended up at her house. But they were never able to substantially find enough evidence at the house to make that case.

Mr. TURNER. Thank you. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman. I think we're all talking in somewhat the same manner, because it's an involvement of information and getting involvement of the bureaucracies that you face in counties and States. We have an excellent FEMA operation at the Federal level, in my judgment, and most of the Governors are very good at the Office of Emergency Management. And certainly there's been a major role for chief information officers that we didn't have 10 years ago.

I'd be curious with the following situation: I come from Los Angeles County, 10 million people, 83 cities; and the sheriff there, and the surrounding suburbs, which is another 10 million from San Diego to Santa Barbara, and that has been done with pacts, compacts, and information in terms of telephone use, radio, all the rest. Sometimes when they have exercises, we find that, say, a few years ago, the communications were all on the East Coast in terms of their radio frequency. And that sort of gave the West a very difficult situation.

So I'm curious in terms of the following: We do have a law that trucks that go across the country have what chemicals are in that so that if something happens, a fire department knows what they're dealing with. The same with facilities in most jurisdictions; everybody sort of knows. And in our case with the earthquakes, you never know when that's going to come. And it isn't easy.

So I'm curious what the CIOs feel and the epidemiologists do with finding the information and spreading it to the right people at the right time. How do you feel about that, since you're all association leaders that are looking at it from a United States 50-State situation, not just your home situation, but you represent both. So I'm curious, Mr. Regan, do you feel that the CIO situation is well represented, or are there places still in the country where they can't seem to get their computing going?

Mr. REGAN. I think, again representing the CIOs, certainly it is a relatively new position in States over the last 5 to 6 years. I think what our Association has found out and, as is the case in Connecticut, those CIOs that are at Cabinet level, that report directly to the Governor, that have enterprise responsibility for infrastructures across many governmental functions—again, I'm not a doctor, I don't necessarily have a stake in public health, but I provide services to public health, I provide services to public safety, transportation, labor, department of banking, all spectrums of government. So I think that, again, if CIOs—and it's more predominant now than it has been ever—have again a seat at the table with the Governors, with the other Cabinet officials that can look from a broad perspective to deal with these—the multitude of issues and look for, again, effective and efficient solutions across

that spectrum that again looks across the horizontal, is where State CIOs have been very effective.

The issue that you brought up in the frequency spectrum, I'm surprised because we have the situation in Connecticut—I thought it was the West Coast that had all the frequencies, because it certainly has been a challenge. When September 11th happened, there was some issues in terms of communication on the wireless systems across the local and State police systems, particularly in Fairfield County, which was, again, the doorway to New York City from Connecticut.

Mr. HORN. Have the CIOs looked at the September 11th situation nationwide and, if so, what are they; and should we and you be looking at the FCC to see what can be done?

Mr. REGAN. We certainly have. In fact, a month ago at this time, the CIOs met in Washington to essentially focus on security and critical infrastructure protection. One of the components of that, again, is the ability to communicate the wireless. It was not, again, the focal point, but we looked at all the considerations of how States need to coordinate our activities better; who do we coordinate with the Federal Government?

It has been unclear, I think, with the appointment of Richard Clarke, who works in the Office of Homeland Security and cybersecurity and terrorism, it's starting to become more clear, but it still is sometimes very frustrating to find an answer when you're dealing with our Federal counterparts. The States seem to have it together. We seem to be able to communicate very effectively. We're putting processes and plans in place to do just that. And, again, I think what our hope is is to be able to come provide some recommendations to the Congress, to help structure the way, again, we communicate with some of the Federal jurisdictions in this area.

Mr. HORN. Now, your information can go pretty rapidly to rural parts of our States. But in terms of epidemiologists, Dr. Pezzino is not so easy. And the question would be, if they don't have laboratories in the part of the State—let's say Wyoming, even California, part of it is rural, and Utah, Arizona, so forth—are there kits or something that can be put together where, either using a high school chemistry lab or biological lab, and see if certain cases with the local hospital, or they—if they have a local hospital, and sometimes they are 200 miles away—even though some of them are veterans' hospitals and State hospitals, how do you feel about that in terms of what we could do on the spot to do it with a kit?

Dr. PEZZINO. Obviously, Congressman, we all wish that we had the magic test that could be used on the spot and give us within a few seconds the answer that we all want: Is this a real threat or what? I am firmly convinced that ruling out false threats is as important as recognizing true threats. Unfortunately, that's not available. And there are a lot of people at work doing research at an advanced stage, and some kits look very promising. But right now there is really nothing that can assure us that something found on the spot is or is not a threat.

I think when you're talking about laboratories, things look a little better, because one of the purposes of the bioterrorism initiative that was funded through CDC and other sources is to create a lab-

oratory network that reaches down to the local hospital level and can assure that is happening and has happened. It has been tested in the last months and is working. So most laboratory tests can be done in local hospitals. And then if they're not fully negative, then it would have to be sent to a reference hospital, which is usually the State health department or public health laboratory. But at least they are able to rule out what is not a threat.

I also totally agree with Mr. Regan's assessment. I think communication within the State and within the State government is actually not as problematic as communication among States and other Federal partners, and also communication with private partners. That's really one of the weak points that I recognize in my testimony. I think that's where we have to put a lot of efforts, because I have no problem at this point in reaching out to my hospitals in my State, or my local health departments, and my challenge is how to reach out to the physicians who are in the front line of this work.

Mr. HORN. Mr. Wiesner, you represent the county and city health officials, and, Mr. Covert, you represent the American Hospital Association. As I recall, there's accreditation standards for various hospitals. Is that most hospitals have that, or are there some that aren't up to the accreditation?

Mr. COVERT. In response to your question, Congressman, most hospitals almost all have accreditations. And you're referring to the acute care, but also in terms of a number of other specialty hospitals as well. It is very few that are not accredited or do not choose to go through that. Remember, all of them are required through our HHS to have some level of accreditation in order to be able to receive Medicare funding.

Mr. HORN. Well, some of the things we've all talked about, would it be right that the next go-around, we have certain questions for accreditation and, if so, what have you learned to put in?

Mr. COVERT. Let me share with you, that is actually an issue right now that I know that the American Hospital Association and the Joint Commission is actually looking at, and to establish a task force that will look through to ask those questions as you go through that accreditation process in order to be able to respond to the issues that you're raising. And I think that hospitals will do well as they're gearing up and moving forward. But in answer to your question, yes, that is happening right now.

Mr. HORN. My subcommittee has jurisdiction over the federalism of the country. One of the things we're having the General Accounting Office do is look at some of the radiation situation that could be breaking loose—the biological, the chemical, and the water supply. That's all over the United States. And if we have these nuts running loose, we need to do something besides just a fence around the reservoir. And what happens when something happens to the water supply? Are there any of your committees within your associations that are looking at that?

Mr. COVERT. In terms of each of these respective areas, I think they're now beginning that process of gearing up. There have always been accreditation standards and licensure requirements for us to meet and to respond to. So that first basic level, let me give you a level of comfort that it's there. However, in terms of taking

those additional steps and how we prepare and then secure, and how would you deal with the effects of contaminated water supply, as an example as you've brought up, or changes in power supply, that we'd have to respond to. I think hospitals now, as part of their disaster planning, are actually doing that on an individual basis, not just simply what's happening at the national level.

I think that you will see in the next year, as we're going through this process, either accreditation requirements or standards expected of respected institutions and how you respond to those issues, and how you tie that into the entire, obviously, public health setting that we look to.

Mr. HORN. Does every hospital in the United States have a temporary energy supply based on diesel or whatever to keep the lights going and all the rest of the things?

Mr. COVERT. All hospitals are required—you'll see this at the State level as well as from the accreditation requirements, about having emergency backup and supplies to be able to support your OR and emergency room, and to have a certain level or extent of supply, whether that is appropriate backup generators or whether that's oil or gas, inclusions associated with water, to be able to respond if you needed to for a period of time.

I think the challenges coming for us is when it becomes an extended period of time then, that you might see from some kind of biological attack or situation that you have to respond to, that I think is going to be a challenge that we need to plan for. And that I think is one of the areas that the Hospital Association has commented on. Part of the costs associated with this is building that infrastructure, which doesn't exist today, beyond that very short-term capacity. And that's why you see, then, requests for significant number of dollars for individual hospitals to be able to respond to that question.

Mr. HORN. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Mr. Horn, thank you very much.

Mr. HORN. Thank you. We appreciate the witnesses here. Great group.

Mr. TOM DAVIS OF VIRGINIA. I have a technical question, probably everybody understands in the room but me, but I'm going to ask it. Rock, I'm asking you just because you're CIO. CDC initiatives like HAN or NEDS are Web-based. So if you use the existing infrastructure for these initiatives, what's the chance that a typical spike in Web usage at a time of an emergency would render these systems unusable just because you'd have a capacity issue?

Mr. REGAN. As we look at architecting these systems, that certainly is a critical element of how do you look at the spikes, particularly when you need it the most. We as information technology professionals do this every day. It's the same requirements for public safety. Again, if you have a public safety event, you want to make sure that you have the capacity, the ability to have capacity.

Mr. TOM DAVIS OF VIRGINIA. We've seen how cell phones fail at that time.

Mr. REGAN. Yes, absolutely. That's a primary example. I think from an architectural standpoint, some of the things we look at is shutting down traffic that is not important traffic on a network so that, for instance, if you were to have other requests from other

agencies like regulatory agencies in the event of a disaster, we would actually shut those parts of the network down to essentially guarantee network availability and system availability for those that need the information and need it now.

Mr. TOM DAVIS OF VIRGINIA. I see. Rock, while I've got you a couple of other questions. I was under the impression CDC had sought substantial input from States and localities when they were developing HAN and the NEDS standards. Is it your point that the outreach might have extended to health officials but not the CIOs?

Mr. REGAN. I think that's exactly our point, is that a lot of the information that we're talking about here doesn't necessarily go directly to health officials. That, again, there are other elements in government that have to have the information available to them at the right point in time. Again, as CIOs, we provide services to a cross-spectrum of government. So when we look at creating these standards, while they're, I'm sure—in fact, I know they're very good standards—they are, in fact, to some degree stovepipe standards in this element. We certainly would like to look across the spectrum in other instances where we have standards in terms of how they fit.

Mr. TOM DAVIS OF VIRGINIA. OK. Dr. Pezzino, several States have not yet signed onto implementing NEDS. How widespread is acceptance in the public health care community of the NEDs architecture, and do you suggest to CDC anything they can do to obtain more widespread acceptance?

Dr. PEZZINO. I think actually most States have accepted the NEDs architecture as an important step toward standardization. Certainly I would say all States recognize the need for standardization. The main issue when it comes to implementation is, obviously, funding. Unfortunately, there were only a few States that were funded when their application for funds was turned into the CDC, and there were at least 25 States that applied for NEDS money last year and didn't get any funding because of lack of money. So I think what you are seeing is not so much a result of a lack of motivation, but more a lack of funding.

Mr. TOM DAVIS OF VIRGINIA. Let me ask you this. How extensively are the Epi-X updates available through mobile communication devices? The CDC indicated that Epi-X experienced significant challenges on September 11th because many State, you know, health officials were forced to evacuate their offices and they didn't have plans in place for offsite access.

Dr. PEZZINO. That is true. That is certainly one limitation of the system. At present, there is absolutely no capability to make Epi-X available for mobile devices. Another weakness of the Epi-X project is that it doesn't allow any communication between States and their local health departments. That's why we are really strongly supporting an expansion of the Epi-X project to include local health departments, to have State levels of Epi-X that can act almost as independent parts of one bigger picture.

Again, I'm afraid I have to go back to the previous issue of funding. The Epi-X project has had little or no funding at all. It was never, to my knowledge——

Mr. TOM DAVIS OF VIRGINIA. Just ask you to do the same thing—ask you to do more with the same amounts of money.

Dr. PEZZINO. There was not indicated funding for Epi-X. It was internal money that CDC was able to mobilize.

Mr. TOM DAVIS OF VIRGINIA. Dr. Wiesner, let me ask this: What's the status of the core capacities for bioterrorism preparedness for local public health systems?

Dr. WIESNER. That's an important question because the capacity measures are actually part of a broader effort of measuring the performance of infrastructure. And it actually is linked to the earlier question of being able to move health departments to some form of voluntary or formal accreditation.

The situation, as far as the specific performance indicators for bioterrorism, is that a continuing assessment is occurring and there are just large areas for improvement, some of which we've incorporated into the testimony that you've heard earlier, or the written testimony.

Mr. TOM DAVIS OF VIRGINIA. OK. HIPAA has mandated certain information sharing and security standards for health care. Do you feel there's a need for a similar regulation within public health that not only mandates standardization across public health but also ties back to uniform standards with health care?

Dr. WIESNER. Well, I think to the degree that local health departments are engaged in the provision of personal services, we are already subjected to the HIPAA regulation. Our experience with the current threats that we're talking about really does beg for at least a reexamination or looking carefully at the HIPAA regulation.

With regard to the importance of being able to receive real-time syndromic surveillance for the protection of the community for bioterrorism threats, we believe that we have the current authority to receive those with the HIPAA regulations as they are presently stated.

Mr. TOM DAVIS OF VIRGINIA. OK. Mr. Covert, would you agree with that?

Mr. COVERT. Mr. Chairman, I would. And I would also add that I think it's going to be a tremendous challenge for us. We're not just dealing with issues of consent forms, we're also talking about that transmission of that information oftentimes is literally to an individual patient as you then aggregate that data to use it. If you look at the regulations today, there's some question about our abilities to be able to do that.

I guess I should make one other comment. It's not that we have a problem with issues of privacy or confidentiality whatsoever, but when the regulations themselves and then the paperwork and the bureaucracy that goes with it actually, truly get in the way of caring for patients, real time, then that's a challenge for us to address.

So I think that—and as I've shared with the regulatory task force staff folks—Christine Schmidt, who is going to chair Secretary Thompson's task force—is we need better guidance, better clarification on those guidelines, so that we can apply them appropriately, not just in the event of an attack as a result of bioterrorism, but every day.

The dollars that we're talking about spending, even at the Hospital Center alone just to comply with regulations—several millions of dollars not even related to the issues that we are here talking about today from an infrastructure standpoint, from an information

systems standpoint—is going to be significantly greater. So I think it's going to be a challenge. And I would agree with Dr. Wiesner.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. Dr. Sharrett, in your statement you noted that the county health department in Fairfax lacks the ability to seamlessly connect the local, State, and Federal data systems as well as the capacity to send and receive confidential health information and to broadcast health alerts. What initiatives do you see the Commonwealth of Virginia doing to improve that situation? Do you know what I'm talking about?

Dr. SHARRETT. Yes, I do know what you're talking about. I think that's a difficult question because it goes into confidentiality issues. And again, I think we need new systems that are secure, and funding to acquire those new systems. And I don't know, in relation to privacy, when you have a national emergency that perhaps some of that would——

Mr. TOM DAVIS OF VIRGINIA. Get compromised. OK. I think in your testimony you noted that an important communication was delayed because there wasn't a clear understanding of who was in charge. To your knowledge, if you see any changes that have been made to address the problem from where you sit?

Dr. SHARRETT. I guess I'm not aware of that. From——

Mr. TOM DAVIS OF VIRGINIA. It will almost take another emergency to find out.

Dr. SHARRETT. Well, other people may know. I must say I do not know that. One of the problems that we had was, related to communicating with the post office. And, how you cross from CDC recommendations to implementation within the post office and having someone directly in charge of all of that was an issue. And I don't know if that is—I can't say that has been resolved.

Mr. TOM DAVIS OF VIRGINIA. OK. Thank you.

Let me turn to Dr. Saunders for a minute. EDS's recommendations for mitigating terrorism seem really far-reaching and, I would say, forward-thinking. But fully implementing those recommendations would likely be costly and, from a governmental perspective, probably not feasible in the short term.

Has EDS researched the cost and time required to implement these solutions and, if you've given any thought, what would be your highest priority?

Dr. SAUNDERS. I view where we need to go is a journey rather than something that's going to be accomplished next year. It is important to have a vision in mind as we overhaul our public health infrastructure. You know, the challenge is to think about what the goals and vision are for the system that we want in the United States next year, 5 years, 10 years, so that all of these are part of some logical plan. So I wouldn't say that the costs and the timelines are fully scoped out, but it's probably, a 5 to 10 year journey for a lot of these different components.

Probably the highest priority would be the kinds of things that the health initiative is focusing on, which gets to real-time surveillance of critical reportable events. But it needs to be a two-way street for returning that information to care workers so that they can actually make use of that information and make some impact in the care environment. That would be the highest priority.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. Mr. Turner.

Mr. TURNER. Mr. Saunders, there is one other item you mention in your statement, the biometric human identification system. Give us a little insight on the state-of-the-art in biometric human identification.

Dr. SAUNDERS. EDS has been involved in implementing biometric systems. For example, the system—the biometric system in use at Ben Gurion Airport in Tel Aviv, for example, is implemented by EDS. That involves hand recognition. There are other elements that we've done in a couple of other places as well, including the face identification.

I mentioned that which you're referring to because I think the technology is evolving very rapidly, and there are ultimately some limitations to biometrics that we know of.

The thumb and face are not always capturable in some circumstances, based on the conditions in which those are captured. Oftentimes, we have people that need identifications who can't communicate soft data elements, or maybe that body parts have been damaged so that they can't really provide a biometric source.

So I think at some point we are going to have to look at—not this year, next year or so in the future—how we incorporate elements that are 100 percent gold standard like DNA information in selected circumstances—whether it is identification of body parts at the scene of the World Trade Center or other types of things, and the ability to link that to law enforcement and terrorist data bases.

I mentioned that because I think the opportunity to start thinking down the road of things like DNA data banking—as a part of our biometric human identification system—is something that we ought to look at.

Mr. TURNER. You, of course, are familiar with the efforts of the CDC. And testimony today talked about three of their major initiatives. Do you see anything about those initiatives that you could offer suggestions for improvement, and are they consistent with moving to the next step, which seems to be what you are talking about in your testimony? Is there anything that would be conflicting or inconsistent with that move?

Mr. SAUNDERS. I think that there is nothing inconsistent. These are good first steps, but the focus of this has been around bioterrorism. And as an emergency physician, I can tell you that is a tiny, tiny slice of the kinds of problems that we deal with every day that have a critical public health impact.

There are also hazmat circumstances. There are multicasualty incidents. There is tuberculosis and all of those sorts of the things that would benefit from the same kind of infrastructure, not just around bioterrorism. So how can the scope of this be appropriately broadened to serve a greater public health need if we are laying down this infrastructure? I think that would be an important issue.

The other issue I think is going to be that the devil is in the details on those things. When we get into the actual challenge of integration into care systems: we are going to find a lot of very challenging issues, dealing with master person indexes and the multiple different ways that the same person is represented in different systems and resolving those challenges; and maintaining interfaces to those systems. Who is going to pay for it is going to be very difficult. So the devil is in the details.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Mr. SHAYS. Thank you again, Mr. Chairman, for holding this hearing. I—I would like to—we wrestled shortly after September 11th as to what to tell people, and it is amazing the quantum leap we have come. Shortly after, some of us were saying what we felt to be the truth, which was it is not a matter of if there will be a chemical or biological attack, it is a question of when, where and of what magnitude, and our view was you tell the American people the truth, and, like adults, they will tell you to do the right thing.

And our view was that people aren't going to realize this is a war unless you tell them why it is a war. It is a war because we are in a race with the terrorists to shut them down before they develop the delivery system for chemical or biological agents or, heaven forbid, get radioactive material in a dirty bomb or nuclear weapon. So that is why we are fighting this.

What I want to ask you all is, how—besides this infrastructure that we want to develop, what kind of debates did you start to find as we—as to who should disseminate this information and who should have it and so on.

Maybe, Mr. Regan, I could ask you first. I mean—for instance, with anthrax, was it viewed that it was important that the Governor be the one to talk about the woman who was afflicted in Oxford?

Mr. REGAN. The Governor certainly made that decision to be the focal point of disseminating the information. And, again, as part of that he clearly made it understood as to who was going to deal with the communication at the local level. So it was the public health commissioner and the Governor who made that decision based on the information that came to them.

Mr. SHAYS. The local health director in the Oxford area?

Mr. REGAN. Oxford as well as the commissioner of public health for the State of Connecticut.

Mr. SHAYS. Do you all get involved in any of these debates as to who should be providing this information, or can you tell us any anecdotes about how you are trying to resolve those issues?

Mr. WIESNER. From NACCHO's perspective, the most important piece there is to actually have a plan for doing that ahead of time, and that is one of the things that has occurred as a result of our starting in 1999 in DeKalb County with a plan.

Mr. SHAYS. Intuitively I could be able to tell you why I think you do that, but I would like you to put it in your own words. Why was it important to be prepared to do that and know who would do it before the crisis occurred?

Mr. WIESNER. Because the public needs a credible spokesperson that has timely and accurate information. And one other related factor to that——

Mr. SHAYS. I just want to emphasize your point about not just being accurate, but it being timely as well.

Mr. WIESNER. One other factor about that. At the local health department level throughout the country, we have to increase our capacity of working with the media and establishing those relationships at the local level.

I was surprised during the anthrax things where we didn't have anthrax in our area. The nearest case was 300 miles away, and we had significant media interaction around this. I had complete strangers that I didn't even know coming up to me and saying, Dr. Wiesner, I am happy that you are on the television because I have seen you before, and I recognize that what you were saying was useful and in the interest of the health. That is what we call the local presence for public health in the community.

And we really need to be sure that is uniform. Now, that is a different level when you are speaking at the State and national level. I remember very clearly a discussion with our public safety director on one of these roundtable—tabletop exercises where we had public safety people, hospital people, private physicians, and somebody said, well, who is going to speak to the press? And—you know, as part of that exercise. And they looked to the local health director in that particular scenario that we were dealing with.

But the most important piece is that you have a plan beforehand, and that you have incident command that includes communication and media relationships in your plan.

Mr. SHAYS. May the record note that Mr. Covert has been nodding his head the whole time that you have been speaking. I don't know if you want to add anything.

Mr. COVERT. Congressman, I would agree with Dr. Wiesner. Thank you. I know, even from your own experiences internally, and obviously being in the middle of D.C. and having the press right there, the pressures that the institution faces to respond to the community.

On the other hand, when you only have a piece of the larger information as to what is going on, you really need to look—you need to be able to look to the—to your public health leadership to be able to provide—not only to calm fears, but to provide good information and accurate information as to what is happening.

I think that is one of the things why I tried to emphasize in the testimony of incorporating hospitals literally into that infrastructure so that you have that group together and plan together in how you effectively communicate, because you should be able to look to your public health leadership. My bias is, having been a former health director, you want to be able to respond in an accurate and, if I can only reinforce exactly what you said, in a timely way, and I think that was part of our frustration here during those early days was that ability to be able to put out information in a timely way.

I would also make one other comment to you that I think becomes a challenge for this body as we walk through this is the issue of jurisdiction. I know you heard from Dr. Sharrett and the issues in northern Virginia. We had those exact same issues in Maryland. We have those exact issues in D.C., and who was going to then represent exactly what was happening, again, using the term Nation's Capital area.

I can take and apply that same situation, Congressman, to an area far away from here in—let's say in the heartland. What would I do if I was the Quad Cities or some other area along the way in terms of who would be in charge, for example, of trying to share that kind of information, particularly if it would be dealing with

the kind of threat that would expand over the boundaries that Dr. Wiesner had talked about.

So I would concur with you that there needs to be better direction in that regard. I think we should be able to look to our public health leadership, and that it does need to be planned in advance.

I think we can take a lesson also, to some extent, from what we have learned from those entities, those settings where you see major disasters in the past, let's recall them, weather-related kinds of disasters where they have learned to kind of have to come together to be able to then respond. This is a different issue, but the same principles would apply.

Mr. SHAYS. Let me quickly—I am not sure if I have a second more, but—maybe I will get no answer here, but is there anyone on this panel that would argue that not telling the—I will say it in the positive—that telling the truth in the long run ends up to be essential, and that the attempt to gloss it over, understate it and so on doesn't end up to result in some problems in the future? In other words, is truth the best policy when it comes to disclosing the public health care threat?

Dr. SHARRETT. Absolutely.

Mr. SHAYS. Absolutely. Yes. A lot of nodding of the heads.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman.

I just want to say that I watched very closely what was done in the Washington area. The Mayor, I thought, did an excellent job, and when people were sort of ducking some of the questions, he had the health authorities right there. And I think since the Mayor is well known, through—by his citizens, that is one good way, because he is very articulate.

Mr. TOM DAVIS OF VIRGINIA. Well, thank you very much. This has been a lively discussion, and I appreciate all of the testimony in your followup answers to the questions that were posed to you.

Before we close, I want to again thank everybody for attending the oversight hearing today. I want to thank the witnesses. I want to think my counterpart, ranking member, Congressman Turner, and the other Members for staying here through the hearing and participating.

I want to thank my staff again for organizing this. It has been very productive. And, again, you will have up to 10 days, if you want to supplement anything you said, anything occurs to you you want to get in the record, we will be happy to do that.

These proceedings are closed.

[Whereupon, at 12:10 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

United States House of Representatives

Government Reform Committee

Subcommittee on Technology and Procurement Policy

Testimony of the

Association of Public Health Laboratories

Friday, December 14, 2001

Mr. Chairman and distinguished members of the subcommittee, the Association of Public Health Laboratories (APHL), representing state and local public health laboratories across the nation, is honored to submit this written testimony in support of the National Electronic Disease Surveillance System (NEDSS) and the important role it will play in rebuilding the information technology capability of public health laboratories. Although a common goal exists between NEDSS and PHLs, the limiting factor for PHLs participation in NEDSS is the lack of information technology (IT) capacity. Recommended solutions are presented.

Background:

PHLs: The responsibilities of public health laboratories (PHLs) have expanded well beyond traditional testing and analysis functions. PHLs continue to provide laboratory support for epidemiological studies and to analyze diagnostic tests that may impact the treatment of individual patients. However, they also provide leadership to establish laboratory regulations, serve as the standard-of-excellence for local and private laboratory performance, perform specialty testing, provide short- and long-term training nationally and internationally, measure toxic agents to determine the extent of a community's exposure to environmental hazards, and, significantly, are often the first to detect and recognize potential communicable disease threats. Much has been said about the decline in public health infrastructure, but the problem is most severe in regards to the ability of public health laboratories to fulfill their essential role in monitoring the public health through the reporting of laboratory test results.

NEDSS: CDC defines NEDSS as "a broad initiative to use data and information systems standards to advance the development of efficient, integrated, and interoperable surveillance systems." NEDSS capitalizes on information technology to electronically exchange data important to public health. The emphasis on national standards allows the scope of NEDSS to be broad and to eventually include both infectious and non-infectious diseases. Significantly, the use of the NEDSS identified standards will allow utilization of new data sources for public health surveillance, including clinical data, health care system information, and vital statistics. Although not considered a new data source in this context, laboratory information is a critical data source for electronic

exchange of relevant public health information under the NEDSS umbrella. Public health surveillance depends on laboratory data for confirmation of diseases (anthrax, influenza), for identification and control disease outbreaks (West Nile virus), as well as for recognition of emerging health problems (i.e., from trend data and "sentinel events"; antibiotic resistance). NEDSS is a framework from which standardized - and therefore interoperable - solutions can be designed and software developed. Importantly, NEDSS is the first initiative that provides PHLs and other public health entities an opportunity to address information-age technology on a national level.

A Common Goal:

In 1999, APHL identified no fewer than eleven core functions typically assumed by the nation's public health laboratories, ranging from routine disease surveillance to emergency response activities to policy development and communication[1]. Among these, the capacity for "integrated data management" stands out as a common goal that is entirely consistent with the principles and activities that fall under NEDSS. As with NEDSS, the development of laboratory "integrated data management" will:

- Ensure a rapid response to acts of bioterrorism as well as rapid dissemination of laboratory information on a regular basis to identify, understand, and control disease outbreaks.
- Provide a statewide, laboratory based disease-reporting network, with centralized facilities for receipt, storage, retrieval, and analysis of data.
- Capture clinical laboratory data essential for public health analysis, program planning, and policymaking.
- Assure the usage of standardized data formats to maintain and communicate clinical and public health laboratory data.
- Allow participation in national information systems (e.g., NEDSS) as the primary partner responsible for collecting, monitoring, and analyzing laboratory data.

Critical Nature of PHL data:

Given the comprehensive nature of NEDSS, the Association of Public Health Laboratories (APHL) recognizes that PHL participation in the design and implementation of the system is critical for at least two reasons. First, PHLs create much of the data that the system will utilize. Second, PHL staff possess valuable, specialized knowledge that will lead to a stronger and more complete, nationally integrated information system. Moreover PHLs:

- Account for a significant proportion of reportable disease testing (approximately 40 million specimens each year).
- Are front-line laboratories where unusual diseases associated with bioterrorist activities will be evaluated (i.e., the first case of anthrax was recognized by a Florida laboratory).
- Are key to the early recognition and confirmation of infectious diseases.
- Have frequently been the first to recognize unusual findings that have led to the discovery of infectious disease outbreaks and identification of mutational variants or antibiotic resistance isolates.
- Have expertise in newborn testing, Lead poisoning prevention, blood alcohol, water quality, radiation, and environmental testing.
- Perform specialized testing not available in the private sector.

Challenges:

PHL Information Technology capacity: There is convincing evidence that the nation's PHL infrastructure has experienced a loss in capacity in the past few years. Furthermore, PHLs are suffering a severe deficit in resources and training that, in effect, are preventing PHLs from taking advantage of new information technologies. For example, only a few state PHLs have the level of IT capability required for active participation in NEDSS. Shockingly, many state laboratories do not even have the necessary equipment or personnel to participate.

Electronic Data Interchange: NEDSS identified standards are used to develop a framework for electronic transmission of public health data. For example, the system architecture for NEDSS is

[1] "Core Functions and Capabilities of State Public Health Laboratories". 2000. Association of Public Health Laboratories.

based on eight developmental elements and it is these elements that provided the framework used by CDC to develop software for electronic epidemiology case reporting of notifiable diseases (CDC's Base System currently being piloted in two states). Although all eight NEDSS developmental elements are relevant to PHLs, the single most important priority (a serious challenge) is electronic data interchange for reporting laboratory data (analogous to epidemiology case reporting of notifiable diseases). The NEDSS system requirement for electronic exchange of data is dependent upon the ability to produce and receive electronic messages, i.e. specifically HL-7 messages. In a recent APHL survey 78% of PHLs (31 states responding) do not have the ability to produce or accept an electronic standardized HL7 messages - herein is a major limiting factor for including PHL data in the Base System. In fact, CDC chose commercial laboratories for pilot studies because in many states it is easier to get electronic data from a private or commercial laboratory than from the state public health laboratory.

Laboratory Information Management Systems (LIMS): An equally important IT challenge for PHLs (separate capability yet required for optimal interfacing with CDC's Base System or other NEDSS compliant disease reporting systems) is the development of computerized laboratory information management systems (LIMS). It is important to understand the functional differences and the interrelationship between LIMS and CDC's Base System, other NEDSS compliant state reporting systems, and other national information systems. LIMS are specifically designed to fully integrate the daily functions of a laboratory and are inclusive for laboratory information covering a variety of diverse public health programs. Only a subset of LIMS data is relevant to various reporting or national information systems. However, without a modernized LIMS, public health reporting and surveillance is compromised. 70% of 32 state PHLs responding to APHL's survey indicated an immediate need to modernize their LIMS. To the laboratories a modernized LIMS (1) is web-enabled with remote data entry, (2) has HL7 messaging capability for electronic exchange of laboratory data (essential for NEDSS participation), (3) provides real-time access, (4) and has an inventory and financial accounting functionality. Clearly, without a modernized LIM system having electronic data interchange capability, laboratory data cannot be efficiently provided to support the diverse functionalities that fall within the purview of PHLs, such as disease diagnosis, epidemiological support, environmental quality, radiation monitoring, food safety, newborn screening, blood alcohol determinations, and utmost in our minds today -- bioterrorism.

Significantly, PHLs have not been able to utilize vendor-developed LIMS software for two reasons. Expense is a major obstacle (One state public health laboratory received commercial vendor quotes from $650,000 to $1.2 million depending on the desired features. Several participants had similar quotes). More significantly, however, vendors cater to clinical/hospital labs and pharmaceutical companies and consequently, they have little experience in development of systems for public health reference laboratories. Consequently, modifying vendor software to meet the needs of reference laboratories drives the cost up. As a first priority, it is extremely critical for public health that every state PHL be supported for the either purchase or development and maintenance of a LIM system to meet their functional needs and to ensure participation in NEDSS as well as other public health information system initiatives.

**Recommended Solutions:**

Overall, PHLs perform several functions that are unique and are crucial to the future development of NEDSS and ultimately to the advancement of public health. PHLs perform a significant portion of reportable disease testing and case reporting within states and to the CDC. This data must be captured by NEDSS. PHLs can also provide input into NEDSS to construct a system that supports their role in the early recognition, confirmation, control, and prevention of infectious diseases. The scope of Public Health Laboratories goes beyond infectious diseases, as does the scope of NEDSS, and as NEDSS migrates beyond infectious diseases, technical input from PHLs will become even more important.

APHL submits the following recommended solutions:

1. It is critical that PHLs are funded to engage in NEDSS-related activities. APHL recommends the appropriation of funding to all U.S. state PHLs in the amount of $25 million to enact these activities and to ensure adequate information technology capability. On a state basis this funding would support $100,000 for personnel and $400,000 for developing and enhancing laboratory information system hardware and software.

2. Public health laboratory participation in the development of NEDSS is critical and is largely dependent on closing IT capacity gaps. APHL recommends that a national meeting be convened in the near future to identify the requirements and develop a process to incorporate PHL information into NEDSS surveillance activities (infectious and noninfectious diseases). Priorities will be to increase the ability of PHL to electronically report laboratory test results; to define the relationship between LIMS and NEDSS; and to propose concrete projects to strengthen the participation of laboratories (public and private and/or commercial) in NEDSS. The meeting should include PHL directors, CDC's senior advisor for CDC's Integrated Health Information Systems, NEDSS staff (CDC/state), representatives from private and/or commercial laboratories, state epidemiologists, other appropriate state health officials and representatives from the partner organizations.

3. The Centers for Disease Control and Prevention should implement the following steps to close the gap in PHL participation in NEDSS:

   - Make specific provisions for the inclusion of PHLs in the next phase of NEDSS design and implementation grants, especially in the areas of newborn and child health testing, lead testing, environmental sampling, and water quality management.

   - Encourage interaction between PHLs and private sector laboratories by funding collaborative projects on electronic data interchange.

   - Work with APHL to define and document the relationship between LIMS and NEDSS so that state LIMS are developed according to NEDSS standards.

3. Establish a funding mechanism to ensure the participation of public health laboratories in the electronic reporting of notifiable diseases. The PHLs should be able to fully participate in NEDSS developmental element #2, " to accept, route and process electronic HL7 messages containing laboratory and clinical content." This funding should provide

for laboratory based information technology specialists, as well as the purchase of laboratory information management system hardware and software.

4. Develop a national strategy with the first goal of linking the CDC to all state and county public health laboratories and the second goal of connecting the state public health laboratories to every private or commercial laboratories in each state. Such a communication network is essential if the United States is to achieve a truly workable National Laboratory System.

The NEDSS system provides an opportunity for synergistic data interchange between all levels within the public health community and the medical community to track and ultimately limit public health threats and ultimately reduce rates of preventable morbidity and mortality. APHL expresses our enthusiasm for the advancement of the NEDSS initiative that will directly impact every facet of public health.

**Michael H. Covert, FACHE**
*President*

Washington
Hospital Center

January 18, 2002

The Honorable Tom Davis
Chairman
Subcommittee on Technology and Procurement Policy
Committee on Government Reform
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Mr. Chairman:

I am writing in response to your letter requesting additional information in connection with my testimony provided to your Subcommittee on December 14, 2001. On behalf of the American Hospital Association, I appreciated the opportunity to present our views on our nation's health care facilities' readiness to deal with a potential terrorist attack utilizing chemical, biological or radiological (CBR) weapons. I am also pleased to provide the additional information you request below:

Q: The potential or real impact of HIPAA requirements on sharing of time-sensitive health surveillance data. How do we balance the privacy concerns in HIPAA with this need to share info quickly?

A: We agree that protecting an individual's private health information is of great importance. We believe, however, that the regulatory burden of the HIPAA requirements will consume vast amounts of hospital resources that are critically needed to address immediate problems related to the threat and the reality of bioterrorism. The resources required are of the same order of magnitude as those consumed by the Y2K conversion process, but unlike the Y2K initiative, establishing HIPAA compliance is in no way essential to our ability to continue ordinary operations.

Getting access to patient-related clinical information is one of the hardest and most time-consuming things clinicians do, and we are working hard to provide better access to the information that drives patient care. Regulatory requirements such as HIPAA that restrict and encumber our ability to share health care information have a negative effect on patient care. Such restrictions also present a direct impediment to our bioterrorism

*MedStar Health*
110 Irving Street, NW, Washington, DC 20010-2975
*phone:* 202 877 6101 • *fax:* 202 877 7826 • *e mail:* michael.covert@MedStar.net

surveillance efforts, which require that we aggregate patient-identifiable data across institutions and share that data with public health agencies.

In the history of medicine, many millions of patients have been cared for with very few examples of abuses related to breaches of patient privacy. The HIPAA requirements have created an immense industry offering expensive and complicated solutions for a problem that is relatively miniscule. Patient data has historically been aggregated and shared for research and surveillance purposes with great success and very little in the way of real problems related to patient privacy. Because of the importance of this information to hospitals and the public, HIPAA emphasis needs to be shifted to permit hospitals, and their state associations, to continue to collect and report this crucial information, none of which is facially identifiable or would ever be used by a hospital or its association to identify an individual patient.

Q: What is the best or most urgent area where federal resources could be applied to help facilitate better information sharing regarding alerts and surveillance data? Is there any reason to believe that existing federal resources could be better coordinated or managed to produce quicker results?

A: Information sharing, alerts and surveillance data distribution are just one part of the communications equation. These items are often thought of as "public health" information. The bioterrorism bills currently pending in conference committee seek to enhance these important functions, and we support these efforts.

To truly solidify response readiness, the federal government should help establish an emergency communication and transportation strategy that would include not just the "public health" side of the equation, but all of the "public service" players such as fire, police, hospitals, etc. Information sharing regarding alerts and surveillance data is important. However, during the recent attacks, street closings and clogged roads impeded EMS workers as they tried to reach the affected areas, and hindered quick access to hospitals. No-fly zones were implemented to prevent other air attacks, but those zones hindered med-evac helicopters and other air transports that shipped blood and bandages to hospitals in dire need. Hospitals need assistance from Federal Aviation Administration officials to keep the skies open to critical medical aircraft. In addition, any biochemical attack will require the coordination of local, state, and federal agencies. In response, the Centers for Disease Control and Prevention have invested in and upgraded state-of-the-art labs to identify and monitor reports of suspicious cases of illness across the country. Working in conjunction with state and local epidemiologists, they will communicate their findings to government agencies.

The frontline responder community, fire services, EMS, emergency physicians, hospitals, public health departments, and law enforcement, however, depends on effective communications to provide emergency medical care, rescue accident victims, respond to natural or manmade disasters, including disease outbreaks, and investigate crime. One of the key lessons learned from the September 11th terrorist attacks is that we must enhance our ability to gather information and to communicate it efficiently to all relevant parties.

In disasters, particularly those involving large numbers of casualties, it is critical that frontline responders have established communications linkages that are reliable and interoperable. Most frontline responder organizations have experienced problems with interoperability. During disasters, communications often degrade as a result of saturated cellular phone systems and wireless communications systems that interfere with public safety communications.

The best or most urgent area where federal resources could be provided is to upgrade, modernize and link frontline responder communications systems and to address interoperability problems. We further suggest that Federal funds earmarked for this purpose should be distributed equally to public health agencies and to the hospitals and other private entities that need to participate in the new data-sharing and communications infrastructure. This will facilitate development from the group up as well as from the top down, leading to a faster and more effective solution to our common problem.

Q: Systems redundancy and back-ups: is this something that should be addressed now or can it wait until other basic infrastructure investments are done? What are we talking about in terms of money given the scale?

A: Built in redundancy, back-ups, and other methods used to ensure that communications systems operate in times of crisis are of primary importance. Not all of these systems are expensive. For example, one hospital familiar with tropical storms and hurricanes has developed an antennae that can be raised by a weather balloon in case its actual antennae fails or is blown over. Novel solutions such as this, however, are no substitute for making solid investments in redundant systems. Now, the sheer magnitude of the number of hospitals in the United States, nevertheless, requires federal investment in this area that may range into the billions.

Sincerely,

Michael H. Covert, F.A.C.H.E.
President

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE

ONE HUNDRED SEVENTH CONGRESS

# Congress of the United States
## House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

RECEIVED
DEC 26 2001
OFFICE OF THE PRESIDENT

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

December 19, 2001

Mr. Michael H. Covert
President
Washington Hospital Center
110 Irving Street, NW
Washington, DC 20010

Dear Mr. Covert:

Thank you for participating in the Subcommittee on Technology and Procurement Policy's December 14, 2001, oversight hearing to discuss the response and information dissemination capabilities of the nation's public health systems to a bioterrorism threat or incident. I appreciated their insightful testimony and comments. As promised, I have prepared follow-up questions I would like you to address. Please provide your responses within 30 days.

- The potential or real impact of HIPPA requirements on sharing of time-sensitive health surveillance data. How do we balance the privacy concerns in HIPPA with this need to share info quickly?

- What is the best or most urgent area where federal resources could be applied to help facilitate better information sharing regarding alerts and surveillance data? Is there any reason to believe that existing federal resources could be better coordinated or managed to produce quicker results?

- Systems redundancy and back-ups: is this something that should be addressed now or can it wait until other basic infrastructure investments are done? What are we talking about in terms of money given the scale?

Thank you in advance for your responses. If you have any questions, please contact Melissa Wojciak or Bill Womack at (202) 225-6751.

Sincerely,

Tom Davis

Tom Davis
Chairman
Subcommittee on Technology
and Procurement Policy

*Health Care Global Industry Group*

H3-6A-85
5400 Legacy Drive
Plano, Texas 75024

February 18, 2002

Honorable Thomas M. Davis
Chairman
Government Reform Subcommittee on Technology and Procurement Policy
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Mr. Chairman:

Thank you for the opportunity to testify before your Subcommittee about the need to unite healthcare professionals and public agencies in a secure, rapid-response public health infrastructure. It was an honor and a privilege to represent EDS on this most important issue. Attached are the responses to your questions regarding improving our public health infrastructure.

This country, more than any nation in the world, possesses the people and resources to create an integrated digital health infrastructure. The need certainly existed before September 11. The demand for it now calls for public and private commitments, a shared roadmap for success and a timetable that compresses best intentions into rapid actions to safeguard the American public.

As the leader of EDS' Healthcare Global Industry Group, I welcome the opportunity to participate in future hearings. You have my commitment to do whatever I can to help ensure homeland defense through shared electronic information services.

Sincerely,

Dr. Charles Saunders
President
EDS
Healthcare Global Industry Group

***Question #1***
***Can you comment on the eHealth Initiative?***

The eHealth Initiative (eHI) is a rapidly growing, non-profit organization comprised of more than 70 leading healthcare and technology companies and organizations. eHI was launched in April 2001. Its membership has increased since the hearing in December of last year. EDS is a member and I serve on its leadership council, which includes many of the industry's healthcare and technology leaders.

eHI's overall purpose is to drive improvement in the quality, safety and cost-effectiveness of healthcare through the adoption of technology. Essentially, eHI and its foundation, the Joseph Kanter Foundation, seeks to build a strong base for the organization by increasing public awareness about the role of information technology within the healthcare industry and addressing key barriers.

eHI's members represent a broad range of industry stakeholders, including 5,000 hospitals, 370,000 practicing physicians and 11,000 emergency medical personnel. Among the e-health and technology companies and organizations are:

- pharmaceutical companies
- medical device manufacturers
- service providers
- non-profit groups and trade associations
- research institutions

eHI's work complements the ongoing efforts of EDS to improve the administration and delivery of healthcare worldwide through digital information services. We believe the application of real-time information technology will enhance the accessibility, quality and affordability of healthcare in the public and private sectors.

***Question #2***
***How will the eHI-CDC collaboration assist in timely information sharing?***

An integrated, rapid-response public health infrastructure requires a public-private partnership to succeed. The Centers for Disease Control and Prevention (CDC) and eHI – supported by the Joseph H. Kanter Foundation – are collaborating to:

- bolster America's health infrastructure
- improve the nation's preparedness to handle any large-scale bioterrorism.

Initial work focuses on leveraging current healthcare information systems and existing data networks to enhance public health data collection, surveillance and detection.

eHI and CDC will work with providers and state/local public health agencies to help:

- identify critical public health data needs
- develop strategies to quickly capture and transmit information – such as pharmacy transactions, emergency room visits, admissions, symptoms and diagnoses – using CDC's National Electronic Disease Surveillance System (NEDSS).

This initiative is significant because eHI members provide healthcare information systems for 80% of U.S. hospitals.

The collaboration's real power will be realized through improved speed at which public health information is shared – and actions are taken – within our healthcare system. Today, surveillance and detection are communicated by telephone calls, faxes and post cards. They are neither real-time nor efficient ways to do business. The exchange flows something like this:

- Information about an incident originates from the provider to the local health department.
- Next, it's communicated to the state health department.
- Then, the state health department passes it on to the CDC.

The hand-offs, even when executed well, still can take days. Infectious diseases or weapons of bioterrorism move much faster.

The public-private initiative, however, will enable surveillance to occur using *existing* information systems and data networks within the nation's hospitals. This is important for two reasons:

- The electronic transmission of standardized data from existing healthcare information systems means important public health information often can be communicated more quickly.
- Collaboration among public health agencies and leading healthcare IT developers will help providers play their critical role in surveillance and detection by reducing the burden on an already challenged system. By augmenting existing systems, surveillance efforts can occur "in the background" and reduce the need for "double-entry" by busy physicians and healthcare professionals.

***Question #3***
***What obstacles has this project encountered to date?***

Rather than dwell on obstacles, I prefer to highlight accomplishments and outline actions for future success. As for accomplishments:

- First, eHI members determined this approach is technically feasible.
- Second, eHI member companies, which often are competitors, are banding together on this homeland defense endeavor to improve the nation's public health system.
- Third, the CDC and eHI are collaborating with help from state and local public health agencies and other key constituencies.
- Most recently, the Centers for Medicare and Medicaid Services (CMS) joined us. CMS recognizes the systems transmitting public health information can be leveraged to support manual clinical data collection processes, which occur to monitor the quality of care delivered to Medicare beneficiaries.

As for future actions:

- Appropriate funding for the CDC, state and local public health agencies will be necessary to fully do the job. CDC's NEDSS system will need to handle significant increases in activity.
- Most likely, hospitals will require additional costs related to surveillance. It should be noted, however, standardizing processes and building upon the existing healthcare technology infrastructure will minimize the expense, time and effort for this important work.
- Coordination among federal, state and local governmental agencies – strengthened by significant support from companies – is essential.

# Council of State and Territorial Epidemiologists

Executive Committee:

President:
Matthew L. Cartter, MD, MPH
Epidemiology Program Coordinator
Connecticut

Vice President:
James J. Gibson, MD, MPH
State Epidemiologist
South Carolina

President-Elect:
Gianfranco Pezzino, MD, MPH
State Epidemiologist
Kansas

Secretary – Treasurer:
John P. Middaugh, MD
State Epidemiologist
Alaska

Members-at-Large:
Ursula Bauer, PhD
Chronic Disease Epidemiologist
Florida

Jesse Greenblatt, MD, MPH
State Epidemiologist
New Hampshire

Suzanne R. Jenkins, VMD, MPH
Assistant State Epidemiologist
Virginia
Infectious Disease Epidemiology

Steven C. Macdonald, PhD, MPH
Epidemiologist
Washington
Environmental Epidemiology

Bela T. Matyas, MD, MPH
Medical Director,
Epidemiology Program
Massachusetts

C. Mack Sewell, DrPH, MS
State Epidemiologist
New Mexico

Executive Director:
Donna Knutson

December 28, 2001

The Honorable Tom Davis
Chairman
Subcommittee on Technology and Procurement Policy
Committee on Government Reform
2157 Rayburn House Office Building
Washington, DC 205 15-6143

Dear Honorable Davis:

I am writing in reply to your follow-up questions on the hearing to discuss the response and information dissemination capabilities of the nation's public health systems to a bioterrorism threat or incident.

Your first question was, how are states managing the new CDC initiatives while continuing to use the existing surveillance systems? For states that rely on old CDC-produced proprietary software for surveillance activities, the main challenge has been to assure that the concept of building one integrated system would reach all the decision-makers at the CDC program level who are often responsible for new versions of the software. While some programs have been very supportive of integration and NEDSS, others have been more slow and reluctant to embrace those principles. As I indicated in my hearing testimony, institutional memories may be hard to change. CSTE has been actively involved in the efforts to have all programs at the CDC accept and support the new NEDSS standards. Another challenge has been that the long-promised NEDSS-based software that the CDC is designing for state-based surveillance (to replace old CDC-produced systems) has not been completed yet. This has forced some states to operate with old, inadequate, non-integrated software.

Other states chose in the past to develop their own surveillance applications, rather than relying on products delivered by the CDC. Since NEDSS is an open architecture based on commercially available standards, the integration of these existing state-based applications with other NEDSS tools is possible, to the extent that all these applications share some common architecture. To this purpose, some states are redesigning some components of their applications. Other applications, particularly older ones, need to be totally rebuilt. While this may be a painful process, most states recognize the importance of having, after years of confusion, some standards to look at when designing and

National Headquarters: 2872 Woodcock Boulevard • Suite 303 • Atlanta, Georgia 30341-4015
phone: 770.458.3811 • fax: 770.458.8516
www.cste.org

deploying public health applications. Some limited funds have been available for states that need to redesign their systems to make them NEDSS-compliant, but the amount of funding is well below what is needed. The current fiscal constraints that many states are facing make it even more important that part of the NEDSS funds be directed to states that need to modify their existing systems to align them with the new NEDSS architecture. Failure to do so may result in an incomplete integration of these system, thus undermining the whole NEDSS project at the national level.

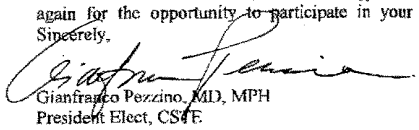
Your second question was whether HAN and Epi-X were used effectively during the anthrax events. My answer to that question is that there is ample space for improvement. Both projects provided independently some good information and features: for example, the HAN used broadcast fax technology that enabled state public health departments to receive faxed information in a timely fashion. Also, HAN produced some excellent educational satellite sessions to address training issues, as they arose. Epi X provided a good forum for discussion and an alert system based on pagers and automated voice messages that was also helpful. What was missing was a coherent plan to use these resources in an integrated fashion. For example, it would have been helpful for state and local officials to have a biref (i.e., a few hours) preview of the CDC recommendations and guidelines before they were made public, to allow some study and preparation for field questions expected from the public and the media. Since these guidelines were transmitted by HAN through fax, they became in essence public knowledge immediately after they were received by public health agencies. Posting them a few hours earlier on a secure Epi X forum would have avoided this problem. Another problem is that some CDC staff did not feel comfortable sharing information in secure Epi X forum, since they were not sure that this information could remain confidential and not be subject to freedom of information requests. In summary, I think that Epi X has not been seen as a helpful tool that could be integrated in the HAN project and provide some strengths to its process, as it should be.

Your final question deals with what a reasonable timeframe could be to provide an adequate information technology infrastructure to local health departments. The answer to this question is not easy, and will probably vary from state to state and from locality to locality. In my state (Kansas), the HAN project has provided high-speed Internet connections to all local health departments where such service is offered, but there are parts of the state where only dial-up Internet service is available. This limitation is a problem that is beyond what public health agencies alone can solve, and is a reflection of more general issues of how information and telecommunication technologies are deployed in our communities. A reasonable goal could be to provide high speed Internet access within one year to all local health departments where this service is available, and dial-up to all others, with the plan to upgrade them when service coverage reaches their areas.

In addition, I would like to stress once again that focusing only on advanced technologies may be misleading. For some health departments, it is far more important to secure more basic resources than the most recent, fastest computer technology. For these agencies, the problems are more what to do when the only nurse is out sick or on vacation, or how to assure that the clinic is open every day, or sometime even how to pay for the phone bill if they have to have a dedicated phone line to connect to the Internet! Strengthening basic capacity in all local health departments is at least as important as assuring the deployment of these technologies.

I hope that this addresses your questions. If you would like further information please do not hesitate to contact me at 785, 296-6536 or gpezzino@kdhe.state.ks.us. I would like to thank you again for the opportunity to participate in your committee's important and timely review.

Sincerely,



Gianfranco Pezzino, MD, MPH
President Elect, CSTE