AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CREATING A NATIONWIDE INTEGRATED BIOSURVEILLANCE NETWORK

HEARING

BEFORE THE

SUBCOMMITTEE ON PREVENTION OF NUCLEAR AND BIOLOGICAL ATTACK

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 11, 2006

Serial No. 109–76

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

37–062 PDF WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON PREVENTION OF NUCLEAR AND BIOLOGICAL ATTACK

JOHN LINDER, Georgia, *Chairman*

DON YOUNG, Alaska
CHRISTOPHER SHAYS, Connecticut
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

JAMES R. LANGEVIN, Rhode Island
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
ELEANOR HOLMES NORTON, District of Columbia
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable John Linder, a Representative in Congress From the State of Georgia, and Chairman, Subcommittee on Prevention of Nuclear and Biological Attack 1
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island, and Ranking Member, Subcommittee on Prevention of Nuclear and Biological Attack 2
The Honorable Donna M. Christensen, a Delegate in Congress From the Virgin Islands 36
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washinton 37
The Honorable Jim Gibbons, a Representative in Congress From the State of Nevada 34

WITNESSES

Dr. Rich Besser, Director, Coordinating Office of Terrorism, Preparedness and Emergency Response, Centers for Disease Control and Prevention:
Oral Statement 15
Prepared Statement 17
Dr. John Clifford, Deputy Administrator for Veterinary Services, Animal and Plant Health Inspection Services, Department of Agriculture:
Oral Statement 25
Prepared Statment 26
Ms. Ellen Embrey, Deputy Assistant Secretary of Defense for Force Health Protection and Readiness:
Oral Statement 22
Prepared Statement 23
Dr. Kimothy Smith, Chief Veterinarian, Chief Scientist, and Acting Deputy Chief Medical Officer, Department of Homeland Security:
Oral Statement 3
Prepared Statement 5
Dr. John Vitko, Director of Biological Countermeasures, Department of Homeland Security:
Oral Statement 8
Prepared Statement 10

CREATING A NATIONWIDE INTEGRATED BIOSURVEILLANCE NETWORK

Thursday, May 11, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON PREVENTION OF
NUCLEAR AND BIOLOGICAL ATTACK,
Washington, DC.

The subcommittee met, pursuant to call, at 2:07 p.m., in Room 1310, Longworth House Office Building, Hon. John Linder [chairman of the subcommittee] presiding.

Present: Representatives Linder, Gibbons, Dent, Lungren, Langevin, Dicks, and Christensen.

Mr. LINDER. [Presiding.] The Committee on Homeland Security's Subcommittee on Prevention of Nuclear and Biological Attack will come to order.

The subcommittee is meeting today to hear the testimony on creating a nationwide integrated biosurveillance network.

I want to thank our distinguished panel of witnesses for being here today.

Last week, the subcommittee heard from members of the Intelligence Committee on how they were engaging the bioscience community to enhance our understanding of biological threats. What we learned from that hearing is that the U.S. needs to create a community of thinkers that bring together the skills of both bioscientists and intelligence experts to better determine the threat of a biological attack on the United States.

In 2004, President Bush unveiled his strategy on biodefense for the 21st century, an important part of which is creating a state-of-the-art biosurveillance system. Leading this charge is the Department of Homeland Security's effort to develop a national biosurveillance integration system.

This new system is intended to be the central point for collection, analysis and dissemination of 30 different sources of aggregated data from 10 different government agencies, to provide a one-stop shop for biosurveillance information.

That information can be linked with current intelligence and be used to provide situational awareness reports to all levels of government, to help respond more quickly and effectively to prevent or contain the spread of disease and save countless lives.

Today, I hope to receive an update on the national biosurveillance integration system at DHS, as well as a status check on some of the major data that feeds into the system, including the BioSense Program at CDC, the BioWatch environmental detection

system coordinated by DHS, the ESSENCE surveillance system at the DOD, and the multiple animal and plant health surveillance efforts at USDA.

While all the experts and agencies here today form a major part of the community of thinkers, I know that each agency has its own challenges in trying to integrate with each other. The importance of this capability, though, cannot be overstated.

The possibility of an influenza pandemic, for example, demonstrates why we need this capability now, from the USDA's initial identification of H5N1 to the CDC's use of the BioSense system, to tracking the cases, to DHS's coordination with state and local officials. They all need to be at the same table to effectively monitor any outbreak in the United States and prevent its spread. We simply cannot afford the costs that will come with a delay.

As such, I look forward to our witnesses' testimony on the current status and challenges they face in ensuring that such a scenario does not become a reality.

I now recognize my friend from Rhode Island, Mr. Langevin, for the purpose of making an opening statement.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I would like to take this opportunity to thank our witnesses for being here today.

The subcommittee has seen the usefulness and importance of bio-intelligence. Last week, we met, as the chairman mentioned, with the intelligence community to hear about their efforts to incorporate bio-intelligence into their work.

Biosurveillance is an important piece of the puzzle to obtain useful bio-intelligence. I thank the chairman for holding this hearing today.

Each of your agencies has developed biosurveillance capabilities for different reasons and particular purposes. At the Department of Agriculture, it is primarily for the protection of domestic livestock and crops from both endemic and foreign-born diseases. For the Department of Defense, force protection is the motivator. The Centers for Disease Control aims to stop the spread of naturally occurring disease, and the Department of Homeland Security's goal is to protect us against bioterrorism.

Because of the nature of disease, bioterror attack may be indistinguishable from a natural outbreak. An outbreak in animals can spread to humans and the battlelines will not be as well defined as they are in traditional wars. Your missions are becoming more similar, and we have to take into account all aspects of the problem if we are to achieve a nationwide capability.

One likely scenario we will face is pandemic influenza. The administration has determined that a 1918-type epidemic could kill approximately two million Americans. We must do everything possible to prevent such an outbreak, and early detection tracking will be extremely important.

We all have a role to play, and I am very interested in the programs that you are engaged in now, how they work together, and how we can improve them. We need to make sure that your efforts are coordinated and that we are not duplicating programs or leaving gaps in coverage. I also serve on the House Armed Services

Committee. There are many areas where the military has developed programs that could be adapted to civilian use.

I believe we can all benefit from sharing information, adapting ideas that were developed in the military to civilian use and creating joint military-civilian programs. I look forward to hearing about the programs that we can adapt in the capabilities and limitations, and most importantly, what procedures are and should be followed, both before and after a detection event.

It is important that we coordinate who is doing what and how the information is assembled and analyzed in order to spot problems, mitigate damage, and effectively protect the health of our citizens.

So I look forward to the witnesses' testimony, and I yield back.

Thank you, Mr. Chairman.

Mr. LINDER. I thank the gentleman.

We are pleased to have before us a distinguished panel of witnesses on this important topic.

Let me remind the witnesses that their entire written statement will appear in the record. We ask, however, that all witnesses make an effort to limit their testimony to no more than 5 minutes.

Dr. Kimothy Smith is the chief veterinarian and social-medical officer for operations and response at DHS, and is one of the nation's foremost experts on anthrax infection.

Dr. John Vitko returns to us from the DHS. He is currently director of biological countermeasures at DHS, and oversees the biologic program. He comes to DHS from the Sandia National Laboratory, where he led a major portion of Sandia's strategic defense programs.

Dr. Rich Besser is from the CDC, the director of the Coordinating Office of Terrorism Preparedness and Emergency Response at CDC in Atlanta. He is a former epidemic intelligence service officer and is now tasked with managing CDC's nearly $1.7 billion terrorism preparedness and response budget.

Ms. Ellen Embrey from the DOD is the director of force health protection and readiness and director of deployment health support at the Department of Defense. She has held various senior executive positions at the Department of Defense, including acting as assistant secretary of defense for reserve affairs.

And finally, Dr. John Clifford is the deputy administrator for USDA's Animal and Plant Health Inspection Service's Veterinary Services Program. He has extensive experience in the veterinarian medicine field, including being the veterinarian in charge in Ohio, West Virginia, Michigan and Indiana.

Dr. Smith, please begin.

STATEMENT OF DR. KIMOTHY SMITH, CHIEF VETERINARIAN, CHIEF SCIENTIST, AND ACTING DEPUTY CHIEF MEDICAL OFFICER, DEPARTMENT OF HOMELAND SECURITY

Dr. SMITH. Mr. Chairman, Ranking Member Langevin and members of the subcommittee, I am Kimothy Smith, chief veterinarian and acting deputy chief medical officer for the Department of Homeland Security. I appreciate this opportunity to discuss with you the national biosurveillance integration system, NBIS.

I will briefly discuss with you the vision for the NBIS, the relationships and functions which the NBIS requires and exploits, as well as the integrated biosurveillance situational awareness output. I will present for you the challenges as we perceive them, review the current state of NBIS development, discuss the next steps in the development of the system, and respectfully answer your questions should you have any.

The Department of Homeland Security leads the NBIS program. The program began in fiscal year 2005 and has the purpose of integrating and fusing biosurveillance information streams from food, agriculture, public health, environmental monitoring, and intelligence. NBIS was conceived to provide continuous situational awareness, early warning of a possible attack, and a decision support system for event response in the event of a biological incident, whether intentional or naturally occurring.

My colleagues here with me can give you a more comprehensive and detailed description of biosurveillance information streams as the visual aid that you have with you before you, but a few examples of these are the BioWatch program, the food emergency response network, the electronic surveillance system of the early notification of community-based epidemics, the emergency management response system used by the veterinary services of the Department of Agriculture, and BioSense, which has information being collected by the Centers for Disease Control and Prevention.

However, NBIS is more than an information technology solution to the nation's integrated biosurveillance challenge. In fact, NBIS can be viewed as having three vital component parts: a robust information management system; a corps of skilled subject-matter experts; and an established culture of trust, cooperation and mutual support.

Simply put, the heart of NBIS is relationships between people and the agents and organizations that they represent. These relationships will work to develop a culture of trust which, in turn, will facilitate information sharing and will be vital to obtain access to valuable, often sensitive and sometimes classified information being collected and use by the NBIS partners.

Threat stream information will be provided through a primary NBIS partner, the Department of Homeland Security Office of Intelligence and Analysis. Once biosurveillance information is fused with threat information, the completed product will be provided to the Homeland Security Operations Center for inclusion in the common operating picture. The common operating picture will provide near real-time streams of biosurveillance situational awareness product, back to the NBIS partner agencies and organizations continuously.

The NBIS program is faced with three areas of challenge today. A robust information management system is required that must be capable of receiving large quantities of diverse information, structure that information into a standard format, and prepare it for fusion with information from all other sources. NBIS will need staff from our partner agencies that are the best and brightest in their area of expertise, dedicated to participation within the NBIS program.

The competition for these minds is fierce, and it will be incumbent upon the Department of Homeland Security to demonstrate persuasively to its partners that there is substantial benefit to participation. NBIS must personify a culture of trust among our partners in order to allow the sharing of sensitive information that in some cases is unprecedented between agencies and organizations.

Safeguards must be built into processes, and become second-nature to personnel to ensure that the information that is provided to NBIS, along with any resulting interpretations, patterns and trend information, will not be misinterpreted, mishandled or inappropriately released.

The situational awareness product developed by NBIS must be of sufficiently high quality to represent an added value to the information contributors and equal a total that is substantially more than the sum of its independent parts. A pilot information system for NBIS has been established and is functional. The system has provided some operational capability and many insights into the challenges of near-real-time biosurveillance situational awareness.

NBIS currently has a small staff with medical, biological and operational expertise and a limited ability for reach-back to additional subject-matter experts. NBIS is producing daily situational awareness products and weekly situational reports for circulation internal to the Department of Homeland Security, a small number of interagency partners, and the Homeland Security Council.

There is a draft request for proposals out now for information system implementation of NBIS and I anticipate that the contract will be awarded by mid-summer. Once selection of this contract performer has been made, the full implementation of NBIS will begin, and I anticipate rapid progress toward first functionality in 6 months after reward of the contract.

In closing, I would like to say that the national biosurveillance integration system is a top priority initiative for the Department of Homeland Security. Our job is to ensure that the nation has the capability for comprehensive integrated biosurveillance situational awareness.

Thank you once again for allowing me to speak to you. I will gladly answer any questions that you might have.

[The statement of Dr. Smith follows:]

FOR THE RECORD

PREPARED STATEMENT OF DR. KIMOTHY SMITH

INTRODUCTION

Mr. Chairman and Ranking Member Langevin and members of the Sub-Committee, I am Kimothy Smith, Chief Veterinarian and Acting Deputy Chief Medical Officer for the Department of Homeland Security. I appreciate this opportunity to discuss with you the National Bio-surveillance Integration System (NBIS).

The Department of Homeland Security is leading the NBIS program, an effort to develop an integrated and comprehensive bio-surveillance system which will answer the President's call for a 'timely response to mitigate the consequences of a biological weapons attack'. The Department of Homeland Security Preparedness Directorate has responsibility for the execution of this national interagency effort. The National Bio-surveillance Integration System will be the nation's first capability for comprehensive, integrated bio-surveillance situational awareness.

In this presentation I will explain the vision for the NBIS and its relevance to a wide range of federal agencies, state and local government, tribal authorities and the private sector. I will describe the relationships and functions which the National Bio-surveillance Integration System requires and exploits, as well as the results—

the patterns and trends of a comprehensive integrated bio-surveillance situational awareness product as part of a National Common Operating Picture. I will present for you the challenges as we perceive them today and review the current state of NBIS development. Finally, I will present the 'next steps' in the development of the System and respectfully answer your questions if you have any.

VISION

The National Biosurveillance Integration System program was begun in FY05 for the purpose of integrating and fusing biosurveillance information streams from food, agricultural, public health, environmental monitoring and intelligence community from federal, state, private and international sources to provide continuous situational awareness, early warning of a possible attack, and a decision support system for outbreak and event response in the event of a biological incident whether intentional or naturally occurring. It is essential that I convey to you that NBIS is more than an information technology solution to the nation's integrated bio-surveillance challenge. The three vital component parts of the NBIS will be a robust information management system capable of handling large quantities of structured and unstructured information; a corps of specially skilled subject matter experts; and, the establishment of a culture of cooperation and mutual support within a our interagency (and other) partners . The heart of NBIS is relationships between people and the agencies and organizations they represent.

NBIS will have relationships with and personnel from a wide variety of federal agencies and other entities including the Department of the Interior, Department of State, United States Department of Agriculture, Department of Defense, Department of Health and Human Services and its operating divisions, the Centers For Disease Control and Prevention and the Food and Drug Administration, and the Department of Veterans Affairs. Trusted relationships will also be established with state and local entities, civil and defense authorities, and with law enforcement, science, academia, health, and commercial sources (amongst others).

The purpose of the relationships which the NBIS will develop is to create a culture of trust which facilitates information sharing. The information acquired from a wide range of trusted partners will be 'fused' within the NBIS and subjected to interpretation and modeling algorithms. Subject matter experts from the various agencies and organizations will examine the collected and fused information providing informed interpretation, iterative modeling examinations and request reach-back consultations and queries when appropriate.

Fused information products, patterns and trends deduced and interpreted from bio-surveillance sources, will be provided to a primary NBIS partner, the DHS Office of Intelligence and Analysis (OI&A) for incorporation with intelligence analysis products. When appropriate the product can be forwarded to the wider Intelligence Community and pertinent threat analysis information then returned back to NBIS. The information can also be forwarded to the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) to inform critical infrastructure and key resource private sector partners. A two-way connection will be maintained between the NBIS, the Office of Intelligence and Analysis and the Intelligence Community since fused information will flow out, and intelligence assessments and analyses will flow back.

The final process of actionable information preparation fuses bio-surveillance patterns and trends with threat information. The completed product will be provided to the Homeland Security Operations Center for inclusion in the Common Operating Picture (COP). The Common Operating Picture is distributed via the Homeland Security Information Network (HSIN). This distribution closes the loop by providing near real-time streams of bio-surveillance situational awareness product back to NBIS partner agencies and organizations.

The National Bio-surveillance Integration System will leverage information sources from NBIS partner agencies and organizations as well as all available open-source information. Going back to the heart of NBIS, the trusted relationships developed with personnel, agencies and organizations will be vital to obtain access to the valuable, often sensitive and sometimes classified information collected and used by the NBIS partners. Information sources include environmental sampling information, for instance Project BioWatch which conducts aerosol monitoring for bio-threat agents in metropolitan areas; human health surveillance (e.g. BioSense which reports syndromic surveillance information from hospitals, clinics, pharmacies, and other sources), animal health and food surveillance such as the Electronic Laboratory Exchange Network and diagnostic results collected through the National Animal Health Laboratory Network, plant health sources as those provided through the National Plant Diagnostic Network, open-source technical, medical, veterinary and non-governmental organization reporting as well as mainstream media sources. In

order to obtain the necessary technical expertise, MOUs with partnering agencies will be developed.

By integrating and fusing this large amount of available information we can begin to develop a base-line or background against which we can recognize anomalies and changes of significance indicating potential biological events whether naturally occurring or from malicious intent.

The near real-time patterns and trends outputs of the NBIS, in combination with the threat streams analysis products for wide distribution via the Homeland Security Information Network (HSIN) realize the situational awareness mission solution-set envisaged in the President's 'Bio-defense for the 21st Century'. There are significant challenges to overcome, nevertheless.

CHALLENGES

I perceive several notable challenges to achieve this vision of a successful National Bio-Surveillance Integration System.

We recognize that a robust information management system is required. I use "robust" to indicate that the system must be capable of receiving large quantities of diverse information, structure that information into a standard format. Information will be sent to NBIS from many sources including federal, state, and local entities; both from civil and defense authorities; and from law enforcement, science, scholarship, health, and commercial sources. NBIS will accept such information from all sources, regardless of format, standardize the information, and prepare it for "fusion" with information from all other sources.

The information management system must enforce access controls for the inherently valuable, often sensitive and sometimes classified information being collected. These controls will be flexible enough to provide "need to know" access to appropriate users with the NBIS team members. NBIS will employ "state of the market" interpretive information analysis systems including automatic cataloging and pattern recognition software but will likely require development of unique algorithms for modeling and interpretation by the NBIS staff.

The NBIS will be a work environment for the best and brightest of all the participating agencies and organizations. Highly skilled and suitably trained subject matter experts must characterize the workforce employed in this dynamic, cross-functional, multi-disciplinary actionable information generating facility. In addition to holding skills important to home agencies such as research, scholarship, military science, intelligence, public health, and so on, analysts at NBIS must be familiar with the disciplines of their co-workers, and must also understand the nature of the information captured by the system, and have the capacity to operate information-merging and fusion applications to yield informed, useful, and actionable products.

NBIS team members must be able to interpret information and make deductions from analysis algorithms, and to ascribe an accurate level of confidence in their findings.

NBIS must personify a culture of trust among our interagency, private sector and government partners in order to be successful. Along with the development of relationships mentioned previously will be the development of this culture of trust to allow the sharing of sensitive information that in some cases is unprecedented between agencies and organizations. A respect and appreciation for these sensitivities, handling restriction and precautions must be demonstrated and a track-record established. Safeguards must be built into processes and become second-nature to personnel to ensure that information that is provided to NBIS along with resulting interpretations, patterns and trend information will not be misinterpreted, mishandled or inappropriately released.

The situational awareness product developed by NBIS must be of sufficiently high quality to represent an added-value to the information contributors and equal a total that is substantially more than the sum of its independent parts. If there is no daily relevancy to the missions of the individual agencies, they will be reluctant to share information collected by their bio-surveillance activities and will not participate as an NBIS partner.

CURRENT STATE

A pilot NBIS Information Management System has been established and is functional as of this calendar year. This system has provided some operational capability and many insights into the challenges of near-real-time bio-surveillance situational awareness, particularly for avian influenza. NBIS is producing daily situational awareness products and weekly situational reports for circulation internal to the Department of Homeland Security, a small number of interagency partners and the Homeland Security Council.

The pilot NBIS information management system has also provided a test-bed environment to further understand the requirements for the full robust information

management system that is required for NBIS. An in-depth study defining the information and technical system architecture requirements for full NBIS functionality has been completed. This study has guided the request for proposals for implementation of the NBIS information management system and the draft Request for Proposals has been issued. If the current procurement schedule remains intact, I anticipate that the contract for this will be awarded mid-summer.

NBIS currently has a small staff with medical, biological and operational expertise and a limited ability for reach-back to additional subject matter experts, some of whom are interagency and interdepartmental. NBIS has one detailee onboard from the National Geospatial Intelligence Agency and expects to have a second detailee from the Department of Defense Northern Command very soon. NBIS operations are currently being staffed 24 hours 7 days per week. The NBIS is staffed at approximately 20% of the anticipated total personnel that will be needed when we are fully operational.

We continue to work to develop an ethos of trust and to educate both ourselves and our partners to optimize the potential of the NBIS. We are working hard to identify the needs and requirements of future NBIS participants and to demonstrate to both existing and candidate mission-partners the benefits NBIS can provide. Partnerships between the Department of Homeland Security National Bio-surveillance Integration System staff and Health and Human Services/Centers for Disease Control, the Department of Defense, United States Department of Agriculture, Department of the Interior and Department of State are being cultivated as the initial high importance participants in NBIS.

NEXT STEPS

As I have already mentioned there is a draft Request for Proposals out now for the information system implementation of NBIS we anticipate that the contract will be awarded by mid-summer. Once the selection of a contract performer has been made, the full implementation of NBIS will begin and I anticipate rapid progress toward functionality with first functionality of the full NBIS Information Management System approximately 6 months after the award of contract.

The partnerships we are developing will increase the interagency NBIS staff of subject matter experts during the summer and fall of 2006 and we anticipate a full complement of personnel as the system is brought to first functionality.

In closing, I would like to say that the National Bio-surveillance Integration System is a top-priority initiative for the Department of Homeland Security. Our job is to ensure that the nation has the capability for comprehensive, integrated bio-surveillance situational awareness, early warning of a possible attack and a decision support system for outbreak and event response in the event of a biological incident whether intentional or naturally occurring.

Mr. LINDER. Thank you, Dr. Smith.

Dr. Vitko?

STATEMENT OF DR. JOHN VITKO, DIRECTOR OF BIOLOGICAL COUNTERMEASURES, DEPARTMENT OF HOMELAND SECURITY

Dr. VITKO. Good afternoon, Chairman Linder and Ranking Member Langevin and members of the subcommittee. I am pleased to appear before you today to discuss the roles of the Science and Technology Directorate of the Department of Homeland Security in creating a nationwide integrated biosurveillance network.

Recognizing that early warning of biological attack is an essential component of biodefense, both the president and Congress have directed the nation to develop an integrated and comprehensive attack warning system to rapidly recognize and characterize the dispersal of biological agents in human and animal populations, food, water, agriculture and the environment.

The biological countermeasures portfolio in DHS S&T has been a leader in fulfilling these responsibilities. We devote approximately one-half our annual resources to fielding and operating biodetection systems and developing the technologies to improve them. To date, we have provided the nation with its first operational bioaerosol monitoring capability, a system known as BioWatch.

We continue to improve that system, introducing new technologies to significantly increase its capabilities and to lower its costs, thereby allowing us to extend it to greater coverage for the nation. We have established an interagency memorandum of understanding to guide the development of a nationally coordinated biodetection system, and we are developing food contamination and agriculture outbreak detection systems to greatly improve surveillance capabilities in those sectors.

The information provided by these systems will be important feeds into the NBIS system you have just heard about. Let me briefly describe some of these accomplishments.

In early 2003, DHS, in partnership with the EPA and CDC, deployed a BioWatch environmental monitoring system to protect our nation's cities from the threats and ramifications of bioterrorist attack. Because of the heightened tensions at that time, this first-generation system was deployed in an amazingly short 90 days. Gen 1 BioWatch uses air samplers distributed throughout a city, with filters retrieved daily or more frequently, and brought to a nearby laboratory response network, LRN laboratory, for genetic analysis.

This system has been operating for more than 3 years and has performed more than 2.5 million assays to date without a false positive. We are now in the midst of enhancing that system, an enhancement we call Gen 2, by increasing the number of collectors in the top-threat cities three-to four-fold, thereby decreasing the minimum attack size that we can detect, and providing added protection for transportation hubs and other critical facilities.

The Gen1 and Gen 1 BioWatch operational costs are dominated by labor costs for retrieving and analyzing filters. These costs limit the number of collectors we can deploy and the frequency with which we can collect them. To overcome these limitations and therefore greatly expand the population monitor by BioWatch, we are developing fully automated detection systems that analyze the air samples at the site at which they are collected and wirelessly transmit the results to an LRN. Field prototypes of these autonomous detectors will be available in 2007, piloted in 2008, and be in deployment in BioWatch cities in 2009.

We are also developing a biological warning and incident characterization system called BWIC to assist local decision-makers in determining the public health significance of any BioWatch positive and also to assist in reconstructing the event to guide the response. To accomplish this, BWIC integrates BioWatch data with plume and disease modeling, and with medical surveillance, for example, from the CDC BioSense program, to provide an improved understanding about the possible origin and extent of the release, and some estimates of its impact. BWIC is currently being piloted in Chicago and Miami.

S&T has also taken several major steps to better coordinate the growing number of interagency biomonitoring and biodetection activities. Jointly with the DOD, we recently completed a program known as BioNet that successfully piloted a coordinated civilian and military concept of operation for biodetection and characterization in the San Diego, California area. We led the development and implementation of an interagency MOU on coordinated biomoni-

toring of biological threat agents, which calls for coordinated architecture, rapid notification of all parties in the case of a confirmed positive, and a process for establishing equivalency among the assays used by the parties to the MOU.

We are also a leader in the applied R&D needed to develop the next generation of technologies to improve these capabilities. We are developing fully autonomous detection systems that will greatly lower the operational costs of BioWatch. We are developing rapid detection systems that can act as a bio smoke alarm for protecting special facilities and event. We are working with the FDA to develop food sensors that could detect the presence of bio agents at central food processing plants prior to the product entering the food distribution stream. And we are working with the USDA to develop high through-put diagnostics to rapidly characterize and contain outbreaks of foreign animal diseases.

In summary, DHS S&T has taken very seriously its responsibilities to the nation, our president and our Congress, to be a leader in creating a nationwide integrated biosurveillance network.

Chairman Linder, Ranking Member Langevin and distinguished members of the subcommittee, I thank you for the opportunity to speak before you, and I am happy to answer any questions when the time comes. Thank you.

[The statement of Dr. Vitko follows:]

FOR THE RECORD

PREPARED STATEMENT OF DR. JOHN VITKO, JR.

INTRODUCTION

Good afternoon, Chairman Linder, Ranking Member Langevin, and distinguished members of the Committee. I am pleased to appear before you today to discuss the role of the Science and Technology Directorate (S&T) of the Department of Homeland Security (DHS) in *"Creating a Nation-wide, Integrated Biosurveillance Network"*.

The importance of this activity and DHS' role in it are clearly called out in the President's *Biodefense for the 21st Century,* which states that: "Early warning, detection, or recognition of biological weapons attacks to permit a timely response to mitigate their consequences is an essential component of biodefense. Through the President's recently proposed biosurveillance initiative, the United States is working to develop an integrated and comprehensive attack warning system to rapidly recognize and characterize the dispersal of biological agents in human and animal populations, food, water, agriculture, and the environment. . . .The Department of Homeland Security, in coordination with other appropriate Federal departments and agencies, integrates these efforts."

The Biological Countermeasures Portfolio in DHS S&T has been a leader in fulfilling these responsibilities, devoting approximately half our annual resources to fielding and operating biodetection systems and developing the technologies to improve them. To date, we:

- Have provided the Nation with its first operational bioaerosol monitoring capability;
- continue to improve that system, introducing new technologies to significantly increase its capabilities and to lower its costs thereby allowing us to extend coverage to greater parts of the Nation;.
- are working with our partnering agencies to develop a nationally coordinated Biomonitoring system; and
- are developing food contamination and agricultural outbreak detection systems to greatly improve surveillance capabilities in those sectors.

In addition, we collaborate and support our interagency colleagues in those biosurveillance areas where they have the lead: e.g. Health and Human Services (HHS) on human health surveillance; United States Department of Agriculture (USDA) on agricultural surveillance; HHS and USDA on food surveillance; and the Environmental Protection Agency (EPA) on water surveillance.

As important and powerful as each of these individual biosurveillance data streams are, they are even much more powerful when integrated to form a common biological operating picture. In its FY2005 Appropriations, Congress assigned the responsibility for integrating these information streams on the state-of-health of people, animals and plants, with environmental monitoring of air, food, and water and with real-time threat information to what is now the DHS Preparedness Directorate and my colleague Dr. Kimothy Smith will summarize those efforts in a separate testimony in this hearing.

For today, I will focus my comments on those areas in which DHS S&T has a lead role.

BIOWATCH

BioWatch is an environmental monitoring system to help provide the earliest possible warning of a biological attack and hence speed the deployment and administration of medical countermeasures to mitigate the effects of such an attack. It is led and funded by DHS and operated in close partnership with the Centers for Disease Control and Prevention (CDC), the EPA and the Federal Bureau of Investigation (FBI). From the outset, the plan has been to field an early operational capability and to then deploy successive generations of technology to improve this capability. These successive generations are referred to as Gen 1, Gen 2 and Gen 3 BioWatch.

Gen 1: This first generation system was deployed in early 2003 and uses air samplers distributed throughout a city, with filters retrieved daily or more frequently and brought to a nearby Laboratory Response Network (LRN) laboratory for genetic (PCR) analysis. Results are available within 12 hours of filter retrieval. This system has been operating continuously—24 hours a day, 7days a week, 52 weeks a year—for more than three years and has performed greater than 2.5 million assays without a false positive. There have been a very small number of 'true positives' in which BioWatch has detected extremely low amounts of naturally occurring organisms when they are 'stirred up' by unusual environmental conditions. These 'environmental positives' have helped us to refine our concepts of operations and attest to the ultra-sensitive detection levels of the system.

Gen 2: In FY05, we began a major enhancement to BioWatch, which we call Gen 2 BioWatch. Gen 2 uses similar technology to Gen 1 but provides a three-to-fourfold increase in the number of collectors in the top ten or so threat cities thereby decreasing the minimum size attack that can be detected and increasing the probability of detection. The additional collectors are placed at locations of the cities choosing, including critical transportation hubs such as subways and airports. Each city also is given approximately 10 spare collectors that they can deploy at special events of their choosing (e.g. conventions, New Year's Day celebrations, "Bowl Games"). Equally important, the LRN laboratory analysis capabilities have been improved and expanded to enable analysis of not just the added number of collectors but also of the anticipated number of environmental samples that would be needed to 'follow-up' on any positive. Gen 2 enhancements will be completed by the end of FY06.

Gen 3: Because Gen 1 and Gen 2 systems involve the manual collection of filters and analysis by laboratory staff, labor costs account for about 75% of the operational costs associated with these systems. This has limited both the number of collectors deployed and the frequency with which filters are retrieved. To overcome these limitations next generation detection platforms are currently under development which will automatically perform the detection analysis at the air sampling sites and wirelessly transmit any positives to the LRN laboratory for human confirmation of the signal interpretation. These systems will analyze the collected air samples four to six times daily and test for approximately 20 agents bacterial, viral and toxin. Laboratory tests will be completed in FY 2006 and field tests in FY 2007. The system will then be piloted in an existing BioWatch city (FY 2008) before initiating full scale deployment in FY 2009.

The autonomous nature of this Gen 3 system and its low operational cost should allow us to greatly expand the coverage provided by BioWatch. Compared with the Gen 1 and 2 systems, when fully deployed the Gen 3 system will monitor more than twice as many people against a ten times smaller attack over a much broader range of agents several times per day and at an operational cost comparable to the current system. In addition, because the Gen 3 technology is fully autonomous and does not require proximity to an LRN it can be used anywhere in the Nation—including smaller cities, towns, critical facilities and infrastructure.

BIOWATCH CONCEPTS OF OPERATIONS AND SIGNAL INTERPRETATION

A positive BioWatch signal by itself does not mean that a biological attack has taken place nor that there is a public health risk? it means that the genetic material

of that organism has been detected. What follows next is a sequence of events to determine the public health and national security implications of such a BioWatch positive. This sequence includes confirmation of the signal, notification of all concerned parties, initial and continuing assessment of its public health and national security implications, and characterization and reconstruction of the event to guide any needed response. Agreed upon interagency guidelines for these concepts of operations (CONOPS) are provided in the *BioWatch Preparedness and Response Guidelines* developed jointly by DHS, CDC, EPA, and DOJ and have been provided to each of the BioWatch localities to guide them in developing written CONOPS reflecting their specific circumstances and needs. Some of the key features of include:

• The local public health department must decide within two hours of a possible BioWatch positive whether it is truly a 'verified PCR positive' or whether there may have been some issues with the equipment, reagents, or protocols.

• If it is a verified PCR positive, then the appropriate local authority must immediately notify the CDC Director's Emergency Operations Center (DEOC), the DHS Homeland Security Operation Center (HSOC) and the local FBI Weapons of Mass Destruction (WMD) coordinator.

• The local BioWatch Advisory Committee (BAC) must have a telecon with State, Local, and Federal stakeholders within two hours of declaration of a verified PCR positive to make an initial assessment of the significance of the event—factoring in the detection data, unusual meteorological or environmental conditions, available health and medical surveillance data, and any intelligence on possible activities of concern in the area.

• When deemed appropriate, conduct environmental sampling in the near vicinity of the positive collectors to provide additional information and hopefully recover a viable (living) organism for subsequent culturing and testing.

Biological Warning and Incident Characterization (BWIC): in determining the public health and/or national security significance of the verified BioWatch PCR positive(s), the local decision maker must assemble, integrate and interpret a large amount of information: e.g. which collectors gave positive signals and which negative; where were they located; what does plume modeling tell us about possible release locations and possible additional sampling sites; are we seeing an increased number of emergency room visits, school absences, or over the counter drug sales in the potential exposure area? In the small number of environmental positives we have had to date, this information has been largely assembled 'by hand' and shared through e-mail in various incompatible, non-mergeable formats and scales.

To address this shortcoming, we have developed and are now piloting the Biological Warning and Incident Characterization (BWIC) system, an information technology framework and set of tools to assist the local decision maker in assembling, integrating, and analyzing the information needed to assess the public health significance of a BioWatch positive. BWIC is designed to be compatible with and integrated with the other emergency management tools used by the locality and not require a stand alone system. It includes a geographical information system (GIS) for registering all information, tailored data bases to reflect the location of BioWatch and USPS collectors and of key local assets and infrastructure; plume modeling tools for assimilating BioWatch collector status and the results of any additional environmental sampling; integration of local and regional meteorological data to improve plume predictions and event reconstruction; disease progression models to project the possible rate of people presenting ill; and linkage to local medical surveillance tools and/or CDC's BioSense data. In use, BWIC will provide the local decision maker with an evolving understanding of the situation and help guide the next steps. For example, the BioWatch readings (both positive and negative) will be used to make initial estimates of possible release locations and possible areas of exposure. This information will then be used to guide local environmental sampling and to estimate the number of potentially exposed people and when they would present ill. Folding in the results of the environmental sampling and of comparing projected vs. actual presentation of illnesses will then result in improved estimates of possible source locations and exposed populations and so on. When implemented, BWIC will allow password protected, role-based access to appropriate local and state personnel and will also export information to the Homeland Security Operations Center (HSOC) and our Federal partners. The first generation BWIC system has been developed and is currently being piloted in Chicago and Miami and is scheduled to begin phased deployment to other BioWatch locales in FY07.

COORDINATION OF INTERAGENCY BIOMONITORING & BIODETECTION

Since the initiation of BioWatch, the United States Postal System (USPS) has initiated the Biohazard Detection System for the monitoring of mail distribution centers and the Department of Defense (DoD) has initiated its Guardian Installation

Protection Program for monitoring of military bases. In addition, multiple agencies are involved in the testing of 'white powders' from various sources. Recognizing the needed for a more coordinated and integrated approach to such biomonitoring, the S&T Directorate has initiated several programs to improve interagency coordination in this area.

BioNet: BioNet is a recently completed DHS funded, DoD executed program to pilot integrated civilian and military concept of operations for the early detection and characterization of biological events. The pilot took place over a period of 14 months in San Diego, CA. and produced:

- Coordinated CONOPS that can be adapted for use by other civil and military communities.
- Recommendations for enhancing the current national BioWatch guidelines.
- An integrated capability for sharing data and information between military and civilian personnel.
- A framework for operational evaluation of biomonitoring equipment.
- Mobile high throughput laboratory capabilities to reduce the processing time needed to support consequence management decision-making.
- Systems modeling and analysis tools to support training, exercises, and studies.

The BioNet program demonstrated that active coordination of local civilian and military organizations can increase situational awareness of potential biological incidents and can improve decision-making to shorten response time.

Biomonitoring MOU: An interagency Memorandum of Understanding (MOU) on Coordinated Monitoring of Biological Threat Agents has been signed by DHS, HHS, DoD, DoJ/FBI and USPS and is currently being implemented:

- An initial draft of a coordinated National Biomonitoring Architecture has been written and is being iterated and refined by the signatories;
- All signatories have committed to prompt notification within two hours of a confirmed PCR positive;
- A process for establishing the equivalency of the different biodetection assays used by the participating agencies has been agreed to and the thousands of samples to be tested have been produced—with testing to commence shortly and concluded later this year.
- The DHS Office of the National Capitol Region has instituted periodic meetings of all the Federal, State and local partners in biodetection in the NCR as a first step in making this coordinated system a reality in the NCR.

This MOU addresses the issues relevant to biological agent detection and characterization necessary to make public health or national security decisions. It does not address subsequent responses which would be addressed by other arrangements and mechanisms.

Public Health Actionable Assays: The Biomonitoring MOU applies not only to bioaerosol monitoring but to all biodetection for homeland security purposed conducted by or on behalf of the signatory agencies. This includes the monitoring of individual mailrooms and of suspicious materials. This presents an even greater challenge since frequently this monitoring is done by commercial services or systems using assays of uncharacterized reliability, with the attendant possibility of false alarms and non-optimal use of resources. The Biomonitoring MOU requires that in the future all such biodetection only be done using assays that have been deemed equivalent in performance by the testing procedures set up in support of the MOU. To better meet this need, DHS in coordination with CDC and DoD, have formulated an approach for working with the private sector to make very high quality, extremely low false alarm rate assays available to them for use in commercial detection technologies. In this approach, the U.S. Government would provide industry with the appropriate signatures to be tested on their detection platforms using their protocols but tested by a U.S. designated independent laboratory. If the combination of signatures, protocols, and platform meet the equivalency requirements established under the MOU then the combination (called an assay) would be designated a "USG—Public Health Actionable Assay" meaning that any positive results would not have to be retested in a government laboratory prior to alerting the Public Health Community. Planning for piloting this approach is now underway. This approach will be piloted later this year.

DEVELOPMENT OF ADVANCED BIODETECTION TECHNOLOGIES

Still more capable biosurveillance systems will be enabled by currently on-going research and development into new detection devices and the associated assays for high confidence detection of biological threat agents. To this end, DHS is developing next generation platforms for both outdoor and indoor bioaerosol monitoring, for

monitoring the food supply, and for rapid characterization of foreign animal disease. Each of these is described briefly below.

Biological Autonomous Networked Detectors (BAND): These are the detection systems for the Gen 3 BioWatch System described above. They must: operate fully autonomously in both outdoor and indoor environments, requiring only monthly servicing; have relatively modest acquisition and operating costs; be capable of simultaneously detecting and identifying about 20 different species of bacteria, viruses and toxins with ultra-high sensitivity (about 100 organisms in 18,000 liters of air) and with false alarm rates of one in ten million or less. We are on track for having field prototypes of this system in FY07 and piloting it side-by-side with BioWatch collectors in FY08.

Rapid Aerosol Detection Systems: These systems seek to detect an aerosolized release of a biological threat agent in five minutes or less, rather than the hours time frame of BAND. They will be used for protecting critical facilities and special events, in a manner similar to a smoke alarm—providing early warning so as to enable protective measures that minimize exposure—e.g. turning off the air circulation systems or evacuating personnel. Because they are designed to operate in confined spaces, their sensitivity requirements are less demanding than those of BAND but because they must "report" every 1–5 minutes, their false alarm rates are more demanding. Field prototypes should be available by the end of FY08.

Food Biological Agent Detect System (FBADS): In coordination with the HHS' Food and Drug Administration (FDA), we are developing a 'food sensor' to detect the presence of biological threat agents in various food matrices at the central processing plants prior to the product entering the food distribution stream. The requirements for these sensors reflect both the challenge of detecting biological agents in various complex food matrices as well as the operational considerations of involved food sectors. A production prototype of FBADS is scheduled to be delivered for testing by the end of FY07.

High Throughput Agricultural Diagnostics: The laboratory surge capacity to rapidly diagnose and characterize the outbreak of a foreign animal disease such as Foot and Mouth Disease is key element of this Nation's strategy for containing any such outbreaks. Therefore, in collaboration with partners in the USDA's National Animal Health Laboratory Network (NAHLN), we are developing a high throughput diagnostic platform that will provide a ten to hundred fold increase in the number of samples that can be analyzed in a day, that can be combined as modular units to provide even greater throughput should that be needed, and that can fit it to a van for mobile deployment to an outbreak site should that be desired. This technology is being demonstrated later this fiscal year and being transferred to the NAHLN in 2007.

Biodetection Assays: the detection platforms described above are only as useful as the bioassays that they contain. The requirements on these assays are indeed daunting. They must: cover the broad range of bacteria, viruses, and toxins of concern; they must detect all strains of the agents of interest and reject all 'look alikes' and environmental contaminants with false alarm rates of one in a ten million or better; they must be capable of working in combination—simultaneously detecting multiple agents to reduce detection times and costs; they should be robust against bio-engineering; and they must only costs cents per assay so as to be affordable for continuous monitoring operations. By end of FY07 we will have such assays available and in validation testing by the CDC for the top 20 agents to be detected by Gen 3 BioWatch. By FY09 all these assays will be tied to 'virulence factors'—genetic features that are essential to a biological agent to cause illness—thereby making these assays extremely hard for the terrorist to use genetic engineering to defeat.

CONCLUSION

In summary, the Department of Homeland Security's Science and Technology plays a major role in biosurveillance as called out both in the President's *Biodefense for the 21st Century* and in the President's *Integrated Biosurveillance Initiative* as subsequently funded by Congress. We have provided the Nation with its first operational bioaerosol monitoring capability. We continue to improve that system, introducing new technologies to significantly increase its capabilities and to lower its costs thereby allowing us to extend coverage to greater parts of the Nation. And we are working with our partnering agencies to develop a nationally coordinated Biomonitoring system and to develop food contamination and agricultural outbreak detection systems to greatly improve surveillance capabilities in those sectors. All these biodetection capabilities are designed to feed into the National Biosurveillance Integration System (NBIS), being led by the DHS Preparedness Directorate, thereby providing the Nation with the biological situational awareness needed to better de-

tect and respond to any biological attacks on this Nation's people, agriculture or infrastructure.

This concludes my prepared statement. With the Committee's permission, I request my formal statement be submitted for the record. Mr. Chairman, Ranking Member Langevin, and Members of the Committee, I thank you for the opportunity to appear before you.

Mr. LINDER. Thank you, Dr. Vitko.

Dr. Besser?

STATEMENT OF DR. RICH BESSER, DIRECTOR, COORDINATING OFFICE OF TERRORISM PREPAREDNESS AND EMERGENCY RESPONSE, CENTERS FOR DISEASE CONTROL AND PREVENTION

Dr. BESSER. Good afternoon, Chairman Linder, Ranking Member Langevin and members of the subcommittee. Thank you for the opportunity to be here. I am Richard Besser, director of the Centers for Disease Control and Prevention's Coordinating Office for Terrorism Preparedness and Emergency Response.

I am pleased to provide this testimony to update you on CDC's efforts to enhance biosurveillance, to continue implementation of the BioSense program, and the plans under way to enhance collaboration with the national biosurveillance integration system at the Department of Homeland Security. I will summarize my remarks and respectfully request that my complete written testimony be included for the record.

The health and security of the United States depends on our preparedness against terrorism, including bioterrorism, as well as natural public health emergencies. These threats necessitate that we improve our public health and medical systems so that we can respond with greater flexibility, speed and capacity to handle mass casualties and large-scale emergency response in coordination with our traditional emergency response partners, as well as those at the Department of Homeland Security and Department of Defense.

The Department of Health and Human Services is responsible for leading federal public health efforts to ensure an integrated and focused national effort to anticipate and respond to emerging threats from biological and other weapons. Within HHS, CDC supports these activities through a set of strategic preparedness goals and extensive coordination and collaboration with a number of federal departments and agencies.

In collaboration with many crucial partners and stakeholders, CDC has built an infrastructure to catalyze and implement biodefense activities. To support this infrastructure, CDC has established nine agency preparedness goals to strategically direct resources. Taken together, these goals provide a strategic framework from which to establish and implement preparedness programs, and our biosurveillance efforts support this framework.

CDC has made considerable advancements in biosurveillance through the BioSense program. I will focus my remaining time on three specific topics: the description of the BioSense program; evaluation activities and the goals of BioSense; and lastly, current collaboration with the Department of Homeland Security to integrate BioSense data into the national biosurveillance initiative.

BioSense is a national program intended to improve the nation's capabilities for conducting near-real-time biosurveillance in health

situational awareness through access to existing data from healthcare organizations across the country. BioSense receives, analyzes and evaluates health data from numerous data sources such as emergency rooms, ambulatory care clinics, pharmacies, poison control centers, and clinical laboratories.

The visible component of BioSense is a Web-based application which enables healthcare facilities and state and local public health organizations to see data from their own communities. In 2002, BioSense was developed and began receiving data from the Department of Veterans Affairs and the Department of Defense ambulatory care clinics, as well as laboratory test orders from LabCorp, largest commercial laboratory in the United States. These data are currently not transmitted in real-time.

In 2005, CDC received additional funding that enabled BioSense to expand and begin receiving real-time clinical data from public and private hospitals and healthcare facilities. BioSense now receives real-time data from over 30 healthcare facilities in 10 major metropolitan areas in the U.S. In 2006, CDC's goal is to increase these numbers and begin receiving real-time data from up to 40 metropolitan areas, including a total of up to 350 health care facilities.

In addition to adding private and public real-time data sources, CDC is also working with the VA, DOD and LabCorp to begin receiving their data in real-time. And this year, BioSense will begin incorporating data from the American Association of Poison Control Centers. CDC expects the longer-term goals of BioSense to be informed by evaluations and feedback from the users of the application.

CDC recognizes the need to perform evaluations of BioSense as it is developing in order to enhance its capabilities and usefulness. BioSense recently underwent a formal review through HHS's ongoing program to review major IT investments, and the findings were favorable. There are also several evaluation efforts beginning this year. CDC plans to award a cooperative agreement to scientifically evaluate a number of aspects of the BioSense system, including usability, validity of data, and usefulness of data types.

In addition, CDC is working with a major independent IT consulting firm to complete an assessment of BioSense systems and ensure the chosen architecture and implementation approach is in alignment with industry best practices. This assessment started in May 2006 and will be completed over the next 6 months. The intent of the study is to do a thorough review of all aspects of the system, including the architecture platform and operations.

CDC is also seeking input and feedback on BioSense from state and local public health and hospital users in the form of a users meeting scheduled later this month, and a focused discussion with nationally recognized experts in informatics and biosurveillance in June. All of these activities will allow CDC to examine the BioSense system in order to enhance its capabilities.

To conclude my oral testimony, I would like to provide an update on the status of our information-sharing discussions with the Department of Homeland Security on the national biosurveillance initiative. The national biosurveillance initiative, launched in 2005, directed federal agencies to enhance biosurveillance capabilities to

reduce the detection time following an attack, confirm the size and characteristics of the attack, and initiate a response.

The initiative established NBIS at Homeland Security to combine and analyze the information collected from various sources. CDC has engaged in initial discussions with DHS staff to determine how BioSense data will be most useful in data integration efforts of the NBIS system. Specific data-sharing activities will be determined over the coming months as information available through BioSense and other biosurveillance systems are evaluated for validity and usefulness, and through further discussions with DHS personnel.

CDC is exploring options for providing staffing and technical assistance to NBIS, for interpretation of BioSense data, and how that data complements the other NBIS components. CDC is committed to working with DHS and welcomes further guidance in discussions to advance the sharing of critical public health information to enhance homeland security efforts.

Mr. Chairman, that concludes my remarks. Thank you for the opportunity to share this information. I will be happy to answer any questions.

[The statement of Dr. Besser follows:]

PREPARED STATEMENT OF DR. RICHARD E. BESSER

Introduction

Good afternoon, Mr. Chairman and Members of the Subcommittee. I am grateful for the opportunity to be here today to provide testimony on CDC's terrorism and emergency preparedness efforts, our efforts to enhance biosurveillance through continued implementation of the BioSense program, and the plans underway to enhance collaboration with the National BioSurveillance Integration Center at DHS. I am Richard Besser, Director of the Centers for Disease Control and Prevention's Coordinating Office for Terrorism Preparedness and Emergency Response. In this role, I have primary oversight and responsibility for all programs that comprise CDC's terrorism preparedness portfolio.

Overview of CDC's Preparedness Efforts

The health and security of the United States depends on our preparedness against terrorism, including bioterrorism, as well as other public health emergencies including the threat of pandemic influenza. These threats necessitate that we improve our public health and medical systems so that we can respond with greater flexibility, speed, and capacity to handle mass casualties and large-scale emergency response in coordination with our traditional emergency response partners as well as those at the Department of Homeland Security (DHS) and Department of Defense (DoD).

HHS is responsible for leading Federal public health efforts to ensure an integrated and focused national effort to anticipate and respond to emerging threats from biological and other weapons. HHS is also the principal Federal agency responsible for coordinating all Federal-level assets activated to support and augment the state and local medical and public health response to mass casualty events. Within HHS, CDC supports these activities through extensive coordination and collaboration with a number of federal departments and agencies. I will focus my remarks on CDC's role and accomplishments in terrorism preparedness and emergency response, with emphasis on the BioSense program.

CDC'S Strategic Preparedness Framework

CDC has made terrorism preparedness and emergency response a priority and has built an infrastructure to catalyze and implement biodefense activities and collaborate with our Federal, state, and local government partners as well as with the private sector, non-governmental organizations, and tribal nations. To do this effectively, CDC has established nine agency preparedness goals to strategically focus and efficiently direct CDC resources. These goals are aligned under three overarching categories: Pre-Event, Event, and Post-event. Taken together, these goals

provide a strategic framework from which to establish and implement preparedness programs, with the goal of integrating our activities with those of our emergency response partners at all levels of government and the private sector. I would like to share with you some of the key activities CDC has undertaken and our progress toward achieving these goals, particularly in the arena of biosurveillance.

BioSurveillance for Enhanced Situational Awareness

Traditionally, public health surveillance systems were designed to identify trends in health indicators and identify diseases for reporting purposes. Historically, these were manual systems that evolved to computerized systems, but which remained fragmented and slow in exchanging information between clinical care providers and public health. CDC, through its new National Center for Public Health Informatics (NCPHI), has been pursuing fundamental changes in the way public health surveillance is conducted in the United States. NCPHI's efforts have been focused on upgrading information technology, standardizing data across multiple settings, and establishing systems for electronic data exchange. These changes are important to all of our public health efforts—but are particularly critical to our efforts in terrorism preparedness and response. In the event of a bioterrorism attack or widespread outbreak, traditional systems may fail to identify ill persons quickly enough for the delivery of appropriate countermeasures, increasing the likelihood of further transmission of disease or death. To achieve this level of information timeliness, biosurveillance systems must be electronic and enable transmission of existing health information to public health decision-makers in real-time. Such systems will not only assist public health to detect disease early and identify persons affected, but will also help to confirm or refute the presence of illness in a given community, characterize the progression of an outbreak once it's identified, and assess the effectiveness of control measures.

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, required specific activities to improve the nation's preparedness for bioterrorism and other public health emergencies by increasing coordination and planning among federal, state, and local public health and healthcare providers. The Secretary of HHS was required to provide for the establishment of an integrated system or systems of public health alert communication and surveillance networks among (1) federal, state, and local public health officials; (2) public and private health-related laboratories, hospitals and other health care facilities; and (3) other entities that the Secretary determined appropriate. Coordination of these surveillance networks is intended to provide channels for secure and timely sharing and discussion of essential information concerning bioterrorism and other public health emergencies as well as recommended methods for responding to such an attack or emergency.

The 2002 Act clearly highlighted the need for improving public health's capabilities for electronic health surveillance. HHS outlined two strategies aimed at achieving this goal: (1) unifying public health surveillance architectures to allow for the exchange of information among health care organizations, organizations with which they contract, and state and federal agencies and (2) streamlining quality and health status monitoring to allow for a more complete look at quality and other issues in real-time and at the point of care.

BioSense is the response to the Public Health Information Technology Initiative set forth by HHS. BioSense is a national program intended to improve the nation's capabilities for conducting near real-time biosurveillance and health situational awareness through access to existing data from healthcare organizations across the country. The visible component of BioSense is the web-based application which enables healthcare facilities and state and local public health organizations to see data from their own communities.

Overview and Objectives of the BioSense Program

Currently, the majority of health-related information systems that exist nationally vary in their ability to share data to support immediate biosurveillance needs. Many local public health agencies lack the resources, the desire, and/or the needed expertise to develop and support a local comprehensive biosurveillance system. Therefore, CDC is developing a single national system that allows local use of local health data. There is no other system that conducts real-time electronic biosurveillance on a national scale. BioSense will connect existing health information to public health in a way not previously possible, by providing public health access to data from hospitals, healthcare systems, and other sources. BioSense is developing and implementing enhanced capabilities to rapidly detect and monitor bioterrorism, natural

disease outbreaks, and other events of public health importance. In addition to early event detection, BioSense will support on-going investigations and responses of suspected bioterrorism or outbreak events by providing real-time health situational awareness. The primary objective is to expedite event recognition and response coordination among federal, state, and local public health and healthcare organizations by providing each level of public health access to the same data, at the same time.

Specifically, BioSense focuses on:

- Data transmission—to assure the secure, timely, routine receipt of health data for public health surveillance;
- Data analysis—utilize advanced analytic methods to detect events and to enable cities and states to use these methods to interpret results in as close to real-time as possible;
- Data reporting—on a near real-time basis, provide useful views of the data, including time series analysis and geospatial displays, for colleagues in state and local health departments, as well as for CDC program staff;
- Public Health Response—to provide local data to state and local public health officials, and support their use and interpretation of these data for investigations, outbreak response and public health interventions.

Community preparedness is at the foundation of BioSense. State and local public health authorities are one of the real "end users" of BioSense, because they are the first responders to health events. State and local public health authority to investigate and mange outbreaks will not be superseded by CDC. Traditional protocols for public health investigations at the local level will continue be the standard and CDC will only assist public health departments when invited. In alignment with CDC's community health protection goal "People prepared for emerging health threats," BioSense contributes to community preparedness by enabling public health activities related to achieving four specific preparedness goals:

CDC Preparedness Goal #2—Decrease the time needed to classify health events as terrorism or naturally occurring, in partnership with other agencies.

- BioSense will provide, on a near real-time basis, standardized health data with broad geographical coverage to local, state, and federal public health jurisdictions. Currently, public health must rely on an amalgam of electronic and manual processes in a waterfall model of reporting (hospital to local to state to CDC) making the event identification process fraught with underreporting and delay.
- Providing this "window on the status of community health" will reduce the amount of time it currently takes to access data needed to classify naturally occurring outbreaks and potential bioterrorism events.
- BioSense will also employ natural language processing and statistical and science-based algorithms that help recognize potential outbreaks and provide access to supporting clinical data about the cause of the outbreak.

CDC Preparedness Goal # 4—Improve the timeliness and accuracy of communications regarding threats to the public's health.

- BioSense allows for simultaneous access of the same data by all levels of public health and the healthcare systems that are contributing data. If any one level identifies a suspected event, others (including the healthcare organization itself) can be invited into a coordinated conversation based on current, detailed healthcare data. This allows better communication regarding necessary action, further investigation, or mobilization of resources.
- BioSense provides cross-jurisdictional views that can help identify events that may be occurring simultaneously in multiple and/or neighboring jurisdictions. This is not possible with local surveillance systems limited by political, geographical, and jurisdictional boundaries.

CDC Preparedness Goal # 5—Decrease the time to identify causes, risk factors, and appropriate interventions for those affected by threats to the public's health.

- BioSense will employ technological and data standards to connect public health to a breadth of real-time healthcare data not currently available to state and local health agencies and CDC. The focus will be on accessing existing health data from emergency departments, hospitals, clinics, and other related data sources in the major U.S. metropolitan areas. Timely access to the breadth of health data described below will give public health the tools to identify probable disease causes more quickly and make more informed intervention choices.
- BioSense includes the following data types:

- Foundational (demographics, chief complaint, presumptive or working diagnosis, disposition, hospital utilization)
- Clinical (vital signs, triage notes, discharge summary and diagnosis)
- Laboratory (laboratory orders, microbiology results)
- Pharmacy (medication orders)
- Radiology (Radiology orders, radiology interpretation results)

- Having access to a centralized and standardized data set will also provide the ability to perform retrospective analyses across multiple jurisdictions and data types. Information from these analyses can then be applied to future events to identify causes earlier and begin interventions more quickly.

Preparedness Goal # 6—Decrease the time needed to provide countermeasures and health guidance to those affected by threats to the public's health.

- Using BioSense, public health can understand the number of patients presenting at healthcare organizations, what their symptoms are, and what actions clinicians are taking to diagnose and treat. This allows public health to determine what information is needed by clinicians to guide care decisions, and to properly inform the general public regarding actual versus perceived health risks.
- In addition, understanding of available hospital resources, as available in BioSense, allows effective and timely countermeasures and guidance to early responders and officials.

Current Status and Goals of the BioSense Program

After the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 was enacted, BioSense was developed and began receiving data from Veterans Affairs and the Department of Defense ambulatory care clinics as well as laboratory test orders from LabCorp—the largest commercial laboratory in the United States. In 2005, CDC received additional funding to expand BioSense to receive real-time clinical data from public and private hospitals and healthcare facilities. Beginning with hospitals in 10 large metropolitan areas, CDC is developing a real-time clinical information surveillance system that, when fully deployed, will be a rich and timely data warehouse for early event detection and situational awareness. It will require substantial funding, take several years to develop and refine, and require input from the users and other stakeholders, but the potential benefit of this program to public health is tremendous. As national efforts focus on advancing the clinical health information technology component—crucial for the care of each individual patient—it is equally crucial that the overall public health system surveillance component is built to allow for efficient public health response based on accurate and timely information.

BioSense receives, analyzes, and evaluates health data from numerous data sources such as emergency rooms, ambulatory care clinics, pharmacies, poison control centers, and clinical laboratories. In addition to data from VA and DoD treatment facilities, and LabCorp, BioSense also receives data from over 30 health care facilities in 10 major metropolitan areas in the U.S. In 2006, CDC's goal is to begin receiving real-time data from up to 40 metropolitan areas, including a total of up to 350 healthcare facilities. In April, 2006, CDC released a new version of the BioSense application which includes health situational awareness functionality and access to the new real-time data streams.

Evaluation

CDC recognizes the need to perform evaluations of BioSense as it is developing. BioSense recently underwent a formal review under HHS' ongoing program to review major IT investments, and the findings were favorable. CDC is working with the Gartner Group, a major independent IT consulting firm, to complete an assessment of the BioSense system to ensure the chosen architecture and implementation approach is in alignment with industry best practices. This assessment is expected to begin May, 2006 and be completed over a six month period. The intent of the study is to do a thorough review of all aspects of the BioSense technical architecture, platform and operations. The study will identify strengths and weaknesses as well recommendations for improvements.

CDC also plans to award a cooperative agreement to scientifically evaluate a number of aspects of the BioSense system including usability, validity of data, and usefulness of data types. In addition, the National Center for Public Health Informatics at CDC will be engaging Centers of Excellence in Public Health Informatics to provide input and focus on the efforts of the Center, including BioSense. To complement these activities, CDC has also funded four grantees to de-

velop the science of early event detection and situational awareness through the secondary use of existing information in electronic, health-related databases. The grants focus on three broad areas: (1) increasing the sensitivity and specificity of detection algorithms, (2) establishing the efficacy of different data sources, and (3) developing software methods and components compatible with the Public Health Information Preparedness Initiative functional and technical specifications.

In addition, CDC is seeking input and feedback on BioSense from the state/local public health and hospital users in the form of a Users Meeting scheduled for May 23–24, 2006 in Atlanta. The goal of the meeting is to gain vital input and open an ongoing communication channel with the user community. In addition, approximately 25 nationally recognized experts in informatics and biosurveillance are being invited to meet with CDC as a Science Group, planned for June 27, 2006. This group will focus on the science of the system including appropriate algorithms, analysis and visualization techniques, and data streams of interest.

Privacy

Privacy and confidentiality of health data is extremely important to CDC, and in addition to the security measures in place, we have taken several steps to ensure the protections of the data transmitted through BioSense. Most importantly, obvious patient identifiers are excluded from the data transmitted through BioSense. In addition, data sharing agreements are signed with each hospital that define the authorized CDC and public health uses and responsibilities regarding the data. BioSense records are protected by the medical records privacy regulation under the Health Insurance Portability and Accountability Act, and CDC takes even further steps to apply other legislative authorities to ensure these data are afforded maximum confidentiality protections.

Electronic Data Sharing Standards and Information Sharing with the Department of Homeland Security

The work conducted in the National Center for Public Health Informatics, and in particular through BioSense will support the HHS Office of the National Coordinator for Health Information Technology (ONC) Health Information Technology Standards Panel (HITSP). HITSP is a collaborative effort to harmonize health information interoperability standards, particularly health vocabulary and messaging standards. Through HHS' ONC, BioSense also supports the work of the American Health Information Community (AHIC or "the Community") and specifically the BioSurveillance Workgroup. The Community was formed to help advance efforts to reach President Bush's call for most Americans to have electronic health records within ten years. Chaired by the Secretary of HHS, the Community provides input and recommendations to HHS on how to make health records digital and interoperable, and assure the privacy and security of those records. The standards set forth by the HITSP collaboration will be presented to the Community for endorsement. BioSense data standards directly support the work needed to make the AHIC recommendations a reality.

In addition to the support of HHS and AHIC standards, The National Biosurveillance Initiative, launched in 2005, directed Federal agencies to enhance biosurveillance capabilities to reduce the detection time following an attack, confirm the size and characteristics of the attack, and initiate a response. The initiative establishes a National Biosurveillance Integration System (NBIS) at the Department of Homeland Security (DHS) to combine and analyze information collected from human, animal and plant health, food and environmental monitoring systems. Such an analysis, combined with evolving threat and intelligence information, will provide greater context for those making critical homeland defense decisions. This is a broader system which BioSense summary data will complement.

CDC has engaged in initial discussions with DHS staff to determine those data that would be most useful for sharing as part of the NBIS data integration efforts. Specific data types will be determined over the coming months as the information available through BioSense and other biosurveillance systems are evaluated for their validity and usefulness. CDC welcomes further guidance and ongoing discussions with DHS to advance the sharing of critical public health information to enhance homeland security efforts.

Thank you for the opportunity to share this information with you. I am happy to answer any questions.

Mr. LINDER. Thank you, Dr. Besser.

Ms. Embrey?

STATEMENT OF ELLEN EMBREY, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR FORCE HEALTH PROTECTION AND READINESS

Ms. EMBREY. Good afternoon. Thank you very much for inviting me here to join you and the members of the subcommittee today.

I am here to discuss the work that DOD is doing in biosurveillance and to describe how we are working to integrate our existing biosurveillance systems with those of other federal agencies in support of the Department of Homeland Security's national biosurveillance integration system.

Emerging and re-emerging infections such as SARS and the H5N1 strain of avian influenza, along with the continuing threat of bioterrorism, highlights the need for an innovative, integrated national disease surveillance system such as the national biosurveillance integration system.

The Department of Defense has joined efforts with the Department of Homeland Security, CDC, and other government agencies to best utilize existing surveillance capabilities to obtain the most accurate, comprehensive picture of American public health. DOD's electronic surveillance system for the early notification of community-based epidemics, also referred to as ESSENCE, is a critical Defense Department biosurveillance system that supports NBIS.

ESSENCE is an early warning system for biological events, whether natural or caused by the accidental or intentional release of biological agents. DOD shares their ESSENCE outpatient data stream with the CDC for analysis, using their BioSense system, which in turn will eventually provide reports to the NBIS for integration into an overall national picture.

Through an integrated approach to surveillance, CDC and DOD analysts can definitively interpret health data, enhance situational awareness, and improve response capacity. In order to capitalize on current integrated NBIS surveillance capabilities, the Department of Defense is working with the Department of Homeland Security to establish shared reporting and improved communication in support of NBIS. To help reach this goal, the Department of Defense has already placed a military liaison in the NBIS DC office, and we plan to position additional liaisons in various combatant command headquarters.

DOD's ESSENCE is among the nation's largest health surveillance systems, with a considerable domestic and international footprint. ESSENCE gathers health data from more than 440 military clinics and hospitals around the globe. This extensive data-set provides us with significant information on symptoms and syndromes, and allows us to detect outbreaks of infectious disease much sooner than ever before.

Such early detection of infectious disease outbreaks allows us to gain precious time in protecting individuals with immunizations and medical treatment, also to help us better allocate health services and equipment, as well as to enable early as possible use of non-pharmacological and risk communications strategies to limit the spread of disease.

These benefits apply to the community immediately affected, as well as to the region that may eventually be impacted by a disease outbreak or biological event. ESSENCE was originally developed to

enhance our ability to detect as early as possible, and improve our situational awareness for potential bioterrorist attacks in the Washington, DC area.

Through the years, it has evolved to provide important biosurveillance information on human disease. When fully integrated into the networked biosurveillance community, the information gathered through ESSENCE and the military treatment facilities around the globe can help support overall efforts to provide key decision-makers with information that will provide early recognition of biological outbreaks with potential national significance, and thus improve decision-making and facilitate timely response.

In closing, I want to reinforce DOD's commitment to ensuring that the NBIS objectives are met, and I thank you for your leadership in supporting biosurveillance, nationally and in the Department of Defense.

I stand ready to answer any questions that you may have about our systems.

[The statement of Ms. Embrey follows:]

PREPARED STATEMENT OF ELLEN P. EMBREY

Good morning and thank you for inviting me to join you today.

I am here to discuss the work DoD is doing in biosurveillance and to describe how we are integrating our existing systems with those of other government agencies in support of the National Biosurveillance Integration System.

Over the past few years, our citizens have faced exposure to many human and animal biological threats, underscoring the need to enhance our plans to respond to biological events of national significance. The appearance of emerging and re-emerging infections, such as SARS and the H5N1 strain of avian influenza, along with the ongoing threat of bio-terrorism, has highlighted the need for an innovative, integrated national disease surveillance system, such as the one proposed through the National Biosurveillance Integration System (NBIS).

In the U.S. military, we face this challenge with every operation and every deployment. The early recognition of these events using public health surveillance techniques has long been an integral part of our day-to-day work and enhances our ability to respond quickly to protect our service members' health and maximize operational readiness.

Some of the many ways we work to safeguard the health of our service members both at home and in theater include testing air, soil and water in areas where we deploy our troops, assessing their individual health, and monitoring any relevant medical surveillance data The systems that we have sponsored and cultivated can play an important role in a national networked biosurveillance community.

In addition to monitoring the health of service members, DoD has joined efforts with NBIS, Centers for Disease Control and Prevention (CDC) and other government agencies to best utilize existing surveillance capabilities to obtain the most accurate, comprehensive picture of American public health.

ESSENCE, the Electronic Surveillance System for the Early Notification of Community-Based Epidemics, is one of the Defense Department's biosurveillance systems that supports NBIS—national biosurveillance capabilities.

ESSENCE is an early warning system for biological events, including natural disease outbreaks and disease caused by the accidental or intentional release of biological agents. DoD shares their outpatient data from ESSENCE with the CDC for analysis using their BioSense system, which in turn provides reports to NBIS for integration into an overall national pattern. Through an integrated approach to surveillance, CDC and DoD analysts can definitively interpret health data, enhance situational awareness and improve response capability.

In order to capitalize on current NBIS integrated surveillance capabilities, DoD is working in coordination with NBIS' National Biosurveillance Group to establish shared reporting and improved communication. To help reach this goal, DoD has already placed a military liaison in the NBIS District of Columbia office and plans to position additional liaisons at various Combatant Command (COCOM) headquarters.

ESSENCE enables us to identify increases in the frequency of carefully defined categories of diseases occurring at military treatment facilities around the world.

This detection capability provides the Military Healthcare System with the information needed to facilitate informed decision-making and enable timely response, including the allocation of any needed medical assistance, resources and supplies to control disease outbreaks and render timely medical care to those already affected.

The human and materiel resources of the Department of Defense are the most forward deployed of any U.S. government resource, and ESSENCE is no exception. ESSENCE is the nation's largest health surveillance system, with a considerable domestic and international footprint. ESSENCE gathers health data from 313 military medical treatment facilities around the world. This extensive data set provides us with significant information on symptoms and syndromes and allows us to detect outbreaks of infectious disease much sooner than ever before.

The early detection of infectious disease outbreaks using ESSENCE allows us to gain precious time in protecting individuals with immunizations and medical treatment, helps us to appropriately allocate health services and equipment, and affords us the opportunity to engage in non-pharmacological and risk communications strategies to limit the spread of disease. These benefits apply to the community immediately affected as well as to the region at large that may eventually be impacted by the disease outbreak or biological event.

For example, if an unusually high number of people in one area are being seen with influenza-like symptoms and illnesses, that information may indicate the beginnings of an influenza epidemic. By tracking the syndrome of influenza-like illness in ESSENCE, we can lessen the time it takes to determine that an outbreak is occurring. If abnormal clusters of symptoms or disease are occurring, then ESSENCE will trigger an alert to local officials, who can then investigate the situation and determine whether a concerted and coordinated public health response is required.

Since its inception in 1999, enhancements to ESSENCE's analytical capability to detect potential disease outbreaks have been implemented. New features include revised syndromic groups to address a broader range of biological threats and standardized mappings of diagnostic codes for each of the re-designed syndromic groups. Data filters identify reportable medical events like anthrax and new data sources, such as prescribed medications complement diagnostic data. One significant enhancement is the ability to display spatial clusters detected over geographic areas.

These improvements make ESSENCE more flexible in its ability to detect disease outbreaks, more compatible with military and civilian surveillance systems, and more capable of pinpointing outbreak locations that in turn allow for tailored responses by DoD public health professionals. Still, by itself it is just a software application. The critical factor is the human analyst who must interpret the automated alerts and sort out the false alarms from the real outbreaks. The DoD uses a tiered approach. The linchpin is the local military public health professional, who monitors ESSENCE with respect to their local beneficiary population. This individual is in the best position to investigate any unusual trends and immediately determine whether there is a problem and to coordinate with the local civilian public health authorities. However, patterns across a region may also be important, so each of the Services have public health centers where epidemiologists monitor ESSENCE and other health-related data streams, interfacing with the installations and providing consultative support and assisting with on-site investigations as needed. Tying all of these separate public health networks together falls to the Armed Forces Health Surveillance Center (AFHSC). The AFHSC is a new organization that will combine several existing surveillance groups together into a DoD center that will serve as the single official source for all DoD health surveillance information. Key components of the center will include the Army Medical Surveillance Activity, the Global Emerging Infections Surveillance and Response System (GEIS), and the surveillance resources in the Deployment Health Support Directorate. The center is expected to reach initial operating capability in FY08, but it already serves as the DoD liaison with DHS's NBIS, CDC's BioSense programs and other syndromic surveillance research groups, all working together to develop the most effective techniques and methods for detecting symptoms of potential disease outbreaks, an evolving discipline of public health.

ESSENCE was originally developed to enhance our ability to detect, as early as possible, and to improve our situational awareness of potential bio-terrorist attacks in the Washington, D.C. region. Through the years, it has evolved to provide important biosurveillance information on human disease. When fully integrated into the networked biosurveillance community, the information gathered through ESSENCE and the military treatment facilities across the globe can support the overall effort to provide key decision makers with early recognition of biological events of potential national significance, and thus, facilitate national decision-making and enable timely response.

I thank you for your time today and your leadership in supporting biosurveillance in the Department of Defense. We look forward to continuing to play a role in the National Biosurveillance Integration System and enhancing the national biosurveillance network. I appreciate the opportunity to address you today, and would be happy to answer any questions you have about ESSENCE or Defense Department surveillance systems.

Mr. LINDER. Thank you, Ms. Embrey.

Dr. Clifford?

STATEMENT OF DR. JOHN CLIFFORD, DEPUTY ADMINISTRATOR FOR VETERINARY SERVICES, DEPARTMENT OF AGRICULTURE

Dr. CLIFFORD. Chairman Linder, Ranking Member Langevin and members of the subcommittee, thank you for holding this hearing today and for the opportunity to testify before you.

Today, the committee is looking at an important issue, the federal government's plan for the coordinated evaluation of all biosurveillance information collected in the United States. We at USDA are actively engaged in this effort, both internally and with our colleagues from the U.S. Department of Homeland Security.

I am very pleased to provide the following outline of our animal health surveillance programs and how we plan to further analyze this information and provide our findings to NBIS. USDA has been working for decades to enhance and refine our ability to collect information regarding the health of our nation's livestock, as well as our food supply.

The information we collect through surveillance and monitoring channels has long served as the basis for our regulatory, policy and operational decisions regarding U.S. animal health and food safety. Generally speaking, USDA's safeguarding systems are comprised of components such as overseas monitoring of disease events, import restrictions, surveillance efforts here in the U.S., as well as the measures we take to eradicate and control disease and the regulation of slaughter practices to protect the food supply.

Understanding the potential pest and disease threats to U.S. agriculture as they exist in other countries, we can take the necessary steps to keep pests and diseases out of the country, while also looking for any signs of them within our borders. Should our surveillance detect one of these pests or diseases, we would then mount an aggressive control and eradication program, while also closing the pathway responsible for the introduction.

USDA's animal health safeguarding systems have largely stayed ahead of evolving risk and have been highly effective in preventing the introduction of serious animal diseases such as foot and mouth disease and highly pathogenic avian influenza into the United States. For example, APHIS swiftly responded to a detection of high path AI in a flock of 6,600 birds in Texas in 2004. By quickly becoming aware of the situation and working with industry and state officials, we prevented further spread of the virus.

As you know, disease such as high-path AI can also have some human health implications. So it is central that we remain vigilant and ensure we have robust emergency response plans and capabilities at the ready.

Emergency response campaigns actually begin with effective awareness of international animal health situations. APHIS main-

tains this awareness through several different avenues, including participation in international animal health organizations, or OIE, safeguarding officers overseas to collect information on foreign pests and diseases, and monitoring open source information for indications of serious international health events. In total, this information allows us to take proactive preventive measures in response to specific threats before we are faced with potential introductions within our borders.

The next component is rapid domestic detection of foreign animal disease, soon after incursion, before the disease spreads further into susceptible animal populations. By maintaining robust animal disease surveillance programs in the U.S., we are also making a significant investment in our emergency preparedness and response capabilities. Recognizing the critical nature of these programs, APHIS' fiscal year 2007 budget included approximately $156 million for animal health monitoring surveillance activities.

Since September 11, 2001, USDA has also made great strides to expand our mission to include security. The department has been working closely with federal, state and local government partners, as well as industry stakeholders to address these concerns via a sector-wide strategy based on White House guidance.

We are relying on guidance provided in homeland security presidential directive 7, 9 and 10, as well as guidelines under emergency support function 11 under the national response plan. These are strengthening our preparedness for intentional acts of terrorism against food and agriculture, and helping us enhance current programs designed to prevent or control unintentional introductions of agents, pests and diseases that could harm our sector.

In October, 2004, when DHS convened the first interagency national biosurveillance group meeting to begin evaluating additional streams of data in the NBIS, it was clear that information related to domestic agriculture and food safety will be critical to the overall effectiveness of the system.

As a result of careful consideration, in February, 2005 USDA decided to develop a new in-house food and agriculture biosurveillance integration system which we call FABIS, to accomplish two goals: achieve the high level of integration of APHIS' animal health surveillance data with information from the Food Safety and Inspection Service's food safety and testing programs and to support our homeland security responsibilities; and two, to develop a system that also provides the NBIS with concise, analyzed data that can be evaluated as part of a complete assessment of U.S. biosecurity.

USDA is pleased to have a close working relationship with DHS colleagues as we move forward to develop of NBIS. I am happy to answer any questions you might have regarding my testimony.

[The statement of Dr. Clifford follows:]

PREPARED STATEMENT OF DR. JOHN CLIFFORD

Chairman Linder, Ranking Member Langevin, and Members of the Subcommittee, thank you for holding this hearing today and for the opportunity to testify before you. My name is Dr. John Clifford and I am the Deputy Administrator for Veterinary Services with the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS). In this position, I also serve as USDA's Chief Veterinary Officer.

Today, the Committee is looking at an important issue—the Federal government's plan for the coordinated evaluation of all biosurveillance information collected in the United States. We at USDA are actively engaged in this effort, both internally and with our colleagues from the U.S. Department of Homeland Security (DHS). I am very pleased to provide the following outline of our animal health surveillance programs and how we plan to further analyze this information and provide our findings to the National Biosurveillance Integration System (NBIS).

Overview of USDA's Animal Health Surveillance and Safeguarding Programs

USDA has been working for decades to enhance and refine our ability to collect information regarding the health of our Nation's livestock, as well as the food supply. The information we collect through these surveillance and monitoring channels, including our off-shore pest and disease monitoring efforts; cooperative animal disease testing programs; and the established networks of laboratories that support our domestic animal disease testing programs, has long served as the basis for our regulatory, policy, and operational decisions regarding U.S. animal health and food safety. In addition, utilizing this information, we routinely make adjustments to the strong system of overlapping safeguards we have in place to guard against the entry of potentially damaging agricultural pests and diseases that are exotic to the United States.

Generally speaking, these safeguarding systems are comprised of components such as overseas monitoring of disease events, import restrictions, surveillance efforts here in the United States, the measures we take to eradicate and control disease, and the regulation of slaughter practices to protect the food supply. In a nutshell, by understanding the potential pest and disease threats to U.S. agriculture as they exist in other countries, we can take the necessary steps to keep the pests and diseases out of the country, while also looking for any signs of them within our borders. Should our surveillance detect one of these pests or diseases, we would then mount an aggressive control and eradication program, while also closing the pathway responsible for the introduction.

We customize the safeguarding systems to meet the unique challenges significant foreign agricultural pests or diseases present to our domestic industries. Therefore, our safeguarding systems against viral animal diseases, such as swine vesicular disease, take into account different risks and corresponding import controls (live swine and swine products are prohibited entry into the United States from countries affected by the disease) than our safeguarding systems against exotic pests, like some species of ticks, that can be mitigated by treating the animals with a pesticide prior to their entry into the United States. But in all cases, our safeguarding systems complement one another in that they draw on our extensive animal health surveillance systems and have one main objective: protecting the health and marketability of U.S. agriculture and the domestic food supply.

USDA's animal health safeguarding systems have largely stayed ahead of evolving risks and have been highly effective in preventing the introduction of serious animal diseases, such as foot-and-mouth disease and highly pathogenic avian influenza (HPAI), into the United States. As you know, diseases such as HPAI can also have some human health implications, so it is essential that we remain vigilant and ensure that we have robust emergency response plans and capabilities at the ready.

A recent case in point is our swift response to a detection of HPAI in a flock of 6,600 birds in Texas in 2004. By quickly becoming aware of the situation and working with industry and State officials to depopulate the flock, carry out onsite cleaning and disinfection, and look for signs of disease in surrounding operations, we prevented further spread of the virus. We also prevented a costlier eradication program by USDA and State officials, as well as protracted trade restrictions on U.S. poultry and poultry products by our trading partners.

I want to note here that emergency response campaigns actually begin with effective awareness of the international animal health situation. APHIS maintains this awareness through several different avenues, including by participating in international animal health organization, or OIE, meetings; placing safeguarding officers overseas to collect information on foreign pests and diseases in their countries of origin; and monitoring open source information for indications of serious international animal health events. In total, this information allows us to take proactive, preventive measures in response to specific threats before we are faced with potential introductions within our borders.

The next component is rapid domestic detection of a foreign animal disease soon after incursion—before the disease spreads further in the susceptible animal population, or populations. By maintaining robust animal disease surveillance programs in the United States, we are also making a significant investment in our emergency preparedness and response capabilities. Recognizing the critical nature of these programs, APHIS' fiscal year (FY) 2007 budget included approximately $156 million for

our animal health monitoring and surveillance (AHMS) activities, an increase of $10 million, or seven percent above the (FY) 2006 enacted. Overall, this is an increase of $81 million (+109%) since FY 2001.

USDA's Food and Agriculture Biosurveillance Integration System (FABIS) Since September 11, 2001, USDA has also made great strides to expand our mission to include security. The Department has been working closely with its Federal, State, and local government partners, as well as with industry stakeholders to address these concerns and others via a sector-wide strategy based on White House guidance.

We are relying upon guidance provided in Homeland Security Presidential Directive (HSPD)–7: *Critical Infrastructure Identification, Prioritization, and Protection,* HSPD–9: *Defense of U.S. Agriculture and Food, and HSPD–10: Biodefense for the 21st Century,* as well as the guidelines under Emergency Support Function 11 (protection of agriculture and natural resources) under the National Response Plan, to strengthen our preparedness for intentional acts of terrorism against food and agriculture and for enhancements to current programs designed to prevent or control the unintentional introduction of agents, pests, and diseases that could harm our sector.

One of USDA's key goals is to expand the surveillance and monitoring systems to provide early detection and tracing of diseases and outbreaks. In addition to expanding our systems, it is important to integrate them at a higher level, enabling us to notice aberrations across mission areas and across sectors. Intelligence is also essential to awareness and warning so that we are knowledgeable of any information related to potential acts of bioterrorism.

In October, 2004, when DHS officials were engaged in the design of the NBIS and convened the first inter-agency National Biosurveillance Group meeting to begin evaluating additional streams of data into the system, it was clear that information related to domestic agriculture and food safety would be critical to the overall effectiveness of the system.

As a result of careful consideration, in February, 2005, USDA decided to develop a new in-house Food and Agriculture Biosurveillance Integration System (FABIS) to accomplish two primary goals: (1) achieve the high-level integration of APHIS' animal health surveillance data with information from the Food Safety and Inspection Service's (FSIS) food safety and testing programs to support our homeland security responsibilities; and (2) develop a system that also provides the NBIS with concise, analyzed data that can be evaluated as part of a complete assessment of U.S. biosecurity.

Currently, USDA is developing a concept of operations plan for the FABIS. Efforts are also underway to evaluate information technology systems, as well as upgrade and integrate the involved APHIS and FSIS databases.

We expect to finalize the concept of operations for FABIS in the near future, and then our efforts will turn to constructing the system (including the necessary interface with the NBIS) and hiring analysts. These individuals will be responsible for analyzing the surveillance information, correlating data, making necessary connections, and providing their assessments to USDA officials, as well as the NBIS. We expect that the FABIS analysts will have broad experiences in, among others, the fields of animal and plant health (epidemiology), food safety, port operations and inspection, agriculture security, and risk analysis and communication.

Once fully operational, FABIS will produce a comprehensive and fully coordinated view of FSIS' and APHIS' surveillance information. This will facilitate timely analysis of data across both agencies and provide a common operating picture of the health of U.S. agriculture. We expect that the results, among others, will be:

- Increased situational awareness and early warning capabilities;
- Better information to assist with estimating risks to animal—, plant—, and food-related human health, and the agricultural economy;
- Enhanced responses to recognized, emerging, or potential threats to U.S. food and agriculture supplies;
- Significant savings in terms of disease containment;

USDA and DHS Cooperative Biosurveillance Efforts

As the narrative above illustrates, USDA is pleased to have a close working relationship with our DHS colleagues as they move forward with development of the NBIS. USDA officials have been active participants in the interagency planning meetings on NBIS convened by DHS. We recognize the important benefits further coordination and analysis of information collected by our animal health surveillance systems will bring to our safeguarding systems, emergency preparedness, and homeland security missions.

USDA is therefore working as expeditiously as possible to develop the FABIS and, once operational, connect the system to the NBIS. USDA looks forward to entering into a formal agreement with DHS in the future that outlines how we will share information from FABIS, as well as the kind of information we can expect to glean from the NBIS. This agreement will also cover the detail of USDA analysts to NBIS to assist with the examination and coordination of agriculture-related data. We fully expect a successful partnership and, again, look forward to the many benefits for U.S. agriculture.

Summary of USDA Animal Health Surveillance Programs

I'd like to conclude my testimony by briefly summarizing several of APHIS' existing animal health surveillance systems that will contribute data to FABIS and, by extension, the NBIS. I would like to note that these systems encompass both domestic and international surveillance efforts. Again, by closely monitoring pests and diseases, we can better protect U.S. agriculture by adjusting our safeguarding systems, to include, when necessary, additional border controls, enhanced domestic surveillance, and greater emergency preparedness. I am happy to provide more specific information on these systems and how we utilize them following the conclusion of my testimony.

Offshore Pest Surveillance

APHIS currently maintains the Offshore Pest Information Program (OPIP). OPIP is a structured, risk-focused process designed to collect, synthesize/analyze, and communicate relevant offshore agricultural pest and disease information. APHIS plant and animal health specialists located overseas monitor and track agricultural pest and disease situations for OPIP reporting. In addition, domestically, APHIS has the capability to monitor pest and disease events in other countries, and this information is added to OPIP as well. APHIS then utilizes all this information to adjust our safeguarding systems accordingly.

Laboratory Networks

USDA coordinates three laboratory networks—the National Animal Health Laboratory Network (NAHLN), the National Plant Diagnostic Network (NPDN), and the Food Emergency Response Network (FERN).

The NAHLN supports APHIS' animal health testing efforts and is comprised of State and university diagnostic laboratories (currently 49 laboratories across 48 states), which can rapidly and accurately detect and report to APHIS possible occurrences of significant animal diseases. NAHLN ensures sufficient capacity and timeliness in veterinary diagnostic testing. Through a standards-based approach, the network provides reporting for foreign animal disease agents, as well as more routine domestic animal diseases, such as bovine tuberculosis and brucellosis. The NAHLN electronically sends testing information to APHIS' other pertinent databases that collect animal disease surveillance information.

The FERN, a joint effort between USDA/FSIS and the Department of Health and Human Services' Food and Drug Administration (HHS/FDA), is a nationwide laboratory network that integrates existing federal and state food testing laboratory resources capable of analyzing foods for agents of concern. The primary objectives of the FERN include prevention (federal and state surveillance sampling programs to monitor the food supply); preparedness (strengthening laboratory capacity and capabilities); response (surge capacity to handle terrorist attacks or a national emergency involving the food supply); and recovery (supporting recalls, seizures, and disposal of contaminated food to restore confidence in the food supply). There are 130 laboratories representing all 50 states and Puerto Rico that have satisfactorily completed the FERN laboratory Qualification Checklist, which provides vital information to determine if a lab meets the criteria for participation in FERN and is eligible for Federal funding.

In FY 2005, FERN was able to offer cooperative agreements to 26 State laboratories, which enhanced the current capability and capacity of the USDA and FDA laboratories participating in FERN. Of these 26 laboratories, FSIS has cooperative agreements with the 18 State microbiological laboratories to begin to build what is, at this time, a very limited capacity to test for biological threat agents in food, while HHS/FDA has agreements with 8 State chemical laboratories to develop capacity to respond to chemical attacks on the food supply. Due to the critical importance of FERN, USDA's budget request for fiscal year 2007 included an increase of $15.8 million for food and agriculture defense. Of this, $13 million will go to build laboratory capacity for FERN, and $2.5 million will be used for a repository for analytical methods and electronic communication in real-time between the laboratories for more rapid, timely information sharing and response. With the $13 million FERN

request for FY 2007, FSIS will be able to ensure that the original 18 laboratories plus five additional laboratories are fully operational FERN labs.

EMRS

The Emergency Management Response System (EMRS) is a web-based incident management system used by APHIS during emergency situations at the Incident Command Post level to manage and investigate outbreaks of foreign animal diseases in the United States. In the event of such situations, maps of real-time outbreak areas and premises data from the EMRS can assist USDA officials in making decisions regarding the size of quarantine zones and appropriate movement controls to prevent further disease spread. APHIS also utilizes EMRS for information on routine reporting of foreign animal disease investigations, State-specific disease outbreaks or control programs, and natural disasters involving animals.

eVe

APHIS' Emerging Veterinary Events database (eVe) is a system for event-based animal health information. The system collects, tracks, analyzes, and forecasts emerging animal health events. The system also serves as an information-sharing tool. Information entered into eVe comes from electronic open-source searches, personal contacts, field reports, and outside communications. The open source electronic material in eVe is mainly obtained through a data-mining effort using sophisticated software. Analysts at APHIS' Center for Emerging Issues, a part of the Agency's Centers for Epidemiology and Animal Health in Ft. Collins, Colorado, run information collected from news services, web sites, and listserves through specialized queries, manually filter the data extracted by the queries, and save relevant animal health event information in eVe for further sharing and analysis. This information can also be combined with other existing animal health information contained in the OPIP and EMRS databases to provide APHIS officials with more complete assessments of potential animal disease risks to the United States from sources abroad.

GDB

APHIS' Generic Database (GDB) helps to provide animal health program management for the Agency's routine surveillance programs. Information on cooperative Federal/State efforts such as herd health inspections, herd certifications, vaccinations, herd inventories, and related activities is contained in the GDB. Information on active surveillance activities is also coupled with NAHLN data. Among other initiatives, the GDB will soon capture routine avian influenza surveillance data. Numerous testing programs are underway to look for specific strains of the avian influenza virus (H5 and H7 strains) that, if not addressed, present a risk to poultry health and can also potentially mutate into more virulent disease strains. Aggressive surveillance testing is being done for commercial poultry prior to slaughter, in wild birds migrating through the United States, and poultry that pass through live bird markets.

Conclusion

Collectively, USDA's efforts are an important part of the Federal government's plan for the coordinated evaluation of all biosurveillance information collected in the United States. Thank you again for the opportunity to testify before the Subcommittee on behalf of USDA. I am happy to answer any questions you might have regarding my testimony.

Mr. LINDER. Thank you, Dr. Clifford.

Dr. Smith, are you working with any of the international firms like FedEx and UPS and most of our major computer manufacturers have locations over in the Far East. First of all, they have an interest in knowing if something is going on over there, because of their workforce, and they could pass information on to us.

Have you considered working with them?

Dr. SMITH. Mr. Chairman, that is an excellent question.

Currently, we are not. Internal to the Department of Homeland Security, we have discussed such information sources and the value of the commercial sources working with industry could provide, and other private sources.

I can tell you that as we develop in this, and as NBIS moves from standup to steady-state operation, we are looking at open source information first, our federal source data next, and then we

will progress on specifically to the sector-specific leading agencies. And then as we move into commercial areas, data that might be available, these types of relationships could and should be exploited in a better relationship to them.

Mr. LINDER. Dr. Vitko, is it on the near horizon that we will see these BioSense or biological sensors be computerized such that any information gets immediately transmitted via satellite to a location, without having to go out and physically get the test and take it to a lab?

Dr. VITKO. The answer is yes, Mr. Chairman. We expect to do a field prototype of that system in 2007, pilot it in 2008, and begin deploying it to the field in 2009. What it would do is do the same kind of analysis or comparable level of analysis that is currently done in a laboratory response network, and wirelessly transmit to the public health system.

Mr. LINDER. Dr. Besser, how are you getting real-time data from these health institutions? Is it computerized?

Dr. BESSER. Yes, sir. The way the BioSense system works, we develop a direct relationship with a hospital, go in and provide technical assistance, and help them to hook up their data-stream, their existing data, so that it can flow to CDC.

Mr. LINDER. Is that a good algorithm that picks up certain kinds of spikes and things like that?

Dr. BESSER. Yes. In terms of the analytic component, what we are working on is developing the algorithm, the aberration detection, so that we are able to look at existing clinical data and look for events of interest that could either be a signal for a bioterrorist event or would help give us situational awareness to what is going on during an existing event.

I would like to say regarding that that at the same time that data is coming from the hospital to the CDC, it is also going to their local health department, to their state health department, so that we are working on this jointly.

Mr. LINDER. Ms. Embrey, how are you getting your information through ESSENCE? Is that real-time data you are getting from these 400-some institutions?

Ms. EMBREY. It comes in as it is provided. We collect it from a central—

Mr. LINDER. A written report?

Ms. EMBREY. No, no. It is electronic. We receive it electronically. We aggregate that information and provide it to CDC about every 8 hours, daily. Sorry about that. Daily. My expert is behind me. I apologize. Daily we provide it electronically to CDC.

Mr. LINDER. Since I have DOD and a CDC person in front of me, I have for some time believed that all of our embassies which have medical officers, who are not necessarily epidemiologists or even physicians, should somehow have a basic training in epidemiology at the CDC for 6 or 8 weeks before they get assigned to a position overseas.

What do you think of that?

Go ahead, Rich.

Dr. BESSER. I think that would be extremely valuable. I think the more people understand epidemiology and what it can provide, and understand public health, the more the clinical community can

be pulled in as the eyes and ears on the ground. That would be very valuable.

Mr. LINDER. Dr. Vitko, we talked about false alarms in the BioWatch system. Can you talk about the recent tularemia positive that we had in DC? How did we respond to that?

Dr. VITKO. Yes. In setting up BioWatch, we established very clear algorithms of what constitutes a positive. So what we look for are multiple signatures that indicate the presence of an organism. So just like you would want to do identification on person not just with their driver's license or their baptismal certificate or stuff like that, we ask for multiple signatures.

On the mall with the tularemia, what we had detected were several collectors who gave us partial signatures for the presence of that organism, but none of us gave the multiple signatures that were required by a hit. That is the appropriate protocol as determined by CDC, and that is the way it was.

Mr. LINDER. Thank you.

Mr. Langevin?

Mr. LANGEVIN. Thank you, Mr. Chairman.

Thank you all for your testimony. I have often said that to be forewarned is to be forearmed, and the earlier we have information that we need to keep our people safe, the better. So the work you are doing is exceptionally important.

Just to build off of that question with respect to tularemia on the Washington Mall. If you could just clarify for me, Dr. Vitko. You would be the right person to answer to this, I believe. I understand there was some confusion about how the information was shared and that local Washington, D.C., officials were not informed of anything for approximately 1 week after detection.

Can you talk about exactly what happened and what was in fact supposed to happen?

Dr. VITKO. Yes. What I will say is that everything that is supposed to happen, happens, so let me tell you about the process. As I said, it is not until all the signatures, all multiple identifiers, I won't go into the number, but all multiplier identifiers for the presence of the organism of tularemia, is there a confirmed positive. On the detection of a confirmed positive, then, notification is supposed to happen within 2 hours of that detection and that notification.

As it turns out, not all the signatures were present. It was not a confirmed positive, but even then because several collectors went off, vigilant laboratory folks on the following day said, we know this is not a confirmed positive; we should look into it further, and they pursued that. A week later, they still did not have a confirmed positive, but they had enough information to notify folks and say, this occurred; we are still chasing it down; that is where it is.

Mr. LANGEVIN. Thank you.

The electronic surveillance system for early community-based epidemics, as you were just referring to, Dr. Embrey, the ESSENCE program, is designed to bring together health indicator data from both military and civilian communities. By evaluating the nontraditional data sources, new analytical techniques are developed to identify abnormal health conditions. This has been expanded to include data from purchases of medicines at pharmacies and mental health areas after a stressful terrorist attack.

I agree with this idea, and I basically offered this idea as an amendment to a bill that we were working on regarding BioShield, but because it referred to the national biosurveillance integration system, NBIS, it was outside the scope of the bill.

So my question is, do you think that this kind of information should be tracked as part of NBIS?

You might take that on, Dr. Embrey and Dr. Smith. You might want to both address this.

Ms. EMBREY. I can speak for DOD. We find it to be quite valuable at the local level to help those individuals take action locally as appropriate.

With respect to NBIS, I defer to the DHS.

Dr. SMITH. Yes, sir. In my opinion, I believe that all sources of biosurveillance information streams, with the proper interpretation and understanding, would be incredibly valuable to give us a national integrated biosurveillance picture. So in short, I would say, yes, it would be very valuable.

Mr. LANGEVIN. Thank you.

I guess the last question that I have is, could you advise us of other things that we could and should be doing to enhance biosurveillance? As professionals in the field, are there things that you need, that Congress could be doing to support you and your efforts, to make sure this biosurveillance effort is as robust as possible?

Dr. Smith, do you want to start and go right down the line?

Dr. SMITH. Yes, sir. I think that as we continue to develop a culture of trust that I have mentioned, as we continue to develop the relationships that we have between the agencies, as we learn to appreciate the sensitivities of each other's data and information and how to treat that, I think that we understand the problems faced at this time, and understand what our mission is, and the wisdom of the White House and the Congress to enact and conceptualize the national biosurveillance integration system.

I feel like we need to continue to move out smartly and in all cases examine where we can accelerate the pace and to move out on the best course, and continue to move quickly. That would be my only advice on how we could improve.

Mr. LANGEVIN. Thank you.

Dr. Vitko, do you have any observations?

Dr. VITKO. Actually, I think this hearing is a very good step that you have taken to do. It clearly communicates to us the import that you put on the system and the support that we have for doing it. To me, that is a very important piece of the information.

Dr. BESSER. Thank you very much for that question.

CDC has been receiving extensive support from Congress and the American people for implementing national electronic surveillance, and we greatly appreciate that support.

An important component of that is the development of national standards for data transmission such as has been done as part of the BioSense project in conjunction with the American health informatics community, AHIC. We appreciate the support Congress has given to that process.

This hearing in particular, asking us to discuss how we are working jointly with DHS, I think is very important.

Mr. LANGEVIN. Ms. Embrey?

Ms. EMBREY. Two observations.

One, I think that we need to do a better job of aligning what we do in the human world with what is being done in the animal world, and make sure that there is close and effective relationship between the information we are getting and how we act on it.

The second would be, it is important for the federal interagencies to work together, but I do believe we need to have as very close partners the states—the public health infrastructures there and the counterterrorism organizations that exist and recommend to the governors.

They have an important role in all of this, and I think we need to maintain a continuous dialogue with the states on what they believe their needs are and make sure that we are addressing not only their needs, but the nation's needs.

Dr. CLIFFORD. I would just like to second what has been said here. I think it is the development of relationships and trust and the proper utilization of the data, and make sure that there is a good understanding of the purpose and the use of that data between each of us, both at the national level and definitely at the state levels.

Mr. LANGEVIN. Thank you all for those observations. I appreciate it.

Thank you.

Mr. LINDER. Mr. Gibbons?

Mr. GIBBONS. Thank you very much, Mr. Chairman,

And to our panel, welcome to the committee. We are very pleased at your presence here today and your testimony.

Let me ask a very brief question because I see the government sitting here, everything from the Department of Agriculture, the Department of Defense, Homeland Security, CDC. Does the national biosurveillance integration system contain private sector people in it as well? Or are you just one big organization of government groups?

Dr. SMITH. Thank you for that question. I think that is a very good question.

Certainly, as I describe the progression of the standup of the national biosurveillance integration system, the initial data-streams will be open source, are open source. And next, we are integrating federal source data.

In terms of involvement of the private sector, the proper entry for private sector people and information is through the leading federal sector. So for agriculture, the Department of Agriculture would be the appropriate entry point for private sector of agricultural companies, people, organizations. Public health would be through the CDC.

So in terms of participation at a lower level feeding up through federal agencies, yes, there is currently.

Mr. GIBBONS. Over the course of the information you get, which I am sure is tremendous in its volume because you are taking in information from a great number of organizations whose tentacles reach out to a great number of communities of interest to all of this, do you have automated analytical services to look at this?

In other words, is it gone through by human eyes only, or do you have a computer data approach analysis to what you are seeing when you collect and look at this information? How is that done?

Dr. SMITH. Sir, currently there is no automated analysis of this data other than what is provided from the federal source data or from the open source information. We are in a pilot information management system mode at this time.

Once there is a stand-up of the full information management system for NBIS and we begin implementing that, there will be computer analytical automated systems put in place very slowly, very carefully, always with a human mind and interpretation there overseeing, not just trusting what the machine says, if you understand.

But primarily, the interpretation and analysis, it will be done in cooperation primarily by the lead federal agencies for that information for that.

Mr. GIBBONS. Knowing, from a layman's point, there are limits to the effectiveness of the analysis based on just requirements. Take, for example, privacy. A lot of the records and information you are going to get comes from medical records. There is an issue of privacy.

What limit does that place on your ability to do your analysis?

Dr. SMITH. Certainly, respectfully, I don't believe that that places a limit upon on NBIS to perform analyses, whether human eyes, human mind, or in an automated fashion. The specific lead agencies, public health information, private information from the CDC, those people understand the HIPAA restrictions. They understand and appreciate these.

That is why we work with them in regard to that, and I would defer actually to Rich to pick up with that limitation. We fully appreciate those limitations, but they will not inhibit the interpretation and analysis in the broader global integrated sense of the fusion of that information.

Mr. GIBBONS. Dr. Besser, do you have a response to that?

Dr. BESSER. Yes, Congressman Gibbons. Thanks for that question.

To pick up on your first point about the private sector and that data source, CDC has been involved in many discussions through the CDC corporate roundtable. We view the private sector as a very strong and important partner in this area and a potential source for very useful data about situational awareness in the international setting, information on employee absenteeism and things going on on the ground in areas where we just don't have the eyes and ears.

BioSense, what I have been talking about here, is one component of many surveillance activities that are under way at CDC. The HIPAA issue is an important one. CDC, as a recognized public health entity, is able to receive information from other public health sources, and we can analyze that data and provide aggregate data to others.

As part of BioSense, we enter into direct agreement with hospitals in terms of what information will be shared and with whom. That does not prohibit us from analyzing data and sending the analysis forward. It would require us to revisit those agreements

if we were sending raw data that contained patient identifiers and specific personal information.

Mr. GIBBONS. Thank you, Mr. Chairman.

Mr. LINDER. Dr. Christensen?

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

Thank you for your testimony, to our witnesses.

One of the concerns that always comes up is who has responsibility, who is accountable for certain things. My first question would be, which agency has overall responsibility for detecting potential pathogens, like anthrax, in the environment?

We heard during the Government Reform Committee hearing on Tuesday that there was some confusion about this. Keith Rhodes of GAO testified that he had no doubt in the law and practicality that the Department of Homeland Security should be in charge. But Susan George, deputy director to Dr. Vitko, said that DHS was operating under a homeland security presidential directive 10, which, in their reading, places EPA, which is not at the table, their administrator, in charge.

Can someone help me clarify that? Which agency is overall in charge?

Dr. VITKO. I will try to help you clarify that.

HSPD–10 has four key pillars. One of them is surveillance and detection. In there, it has two main activities, one is attack warning; the other is attribution. In both of those areas, DHS is given the lead for coordination of the activities among the agencies.

So for attack warning, that is, has an agent been released in the environment, in the food supply and whatever, DHS has the lead responsibility for coordination.

Part of the confusion that came up in the hearing on Tuesday was over—

Mrs. CHRISTENSEN. And for detecting it?

Dr. VITKO. For detecting it, yes.

Mrs. CHRISTENSEN. Okay.

Dr. VITKO. That is for detecting a release, as opposed to going in and asking, is a building contaminated or not. And that is where the confusion came up. So yes, DHS clearly has the responsibility for attack warning.

Mrs. CHRISTENSEN. Okay.

Dr. Smith, you talked about three pillars, the NBIS that is going to be set up by mid-next year, as I understand it, your information system, which has a contract, and the request for proposal is out. The second one was experts, and the third part was the relationship, that core of trust that you talked about.

We know how problematic that has been since Homeland Security has been set up, but I am going to focus on the second one. The NBIS won't be up for more than 6 months.

Do you have your full staff of experts in place?

Dr. SMITH. No, ma'am, we do not at this time have our full staff of experts. As we have moved through the stand-up phases—

Mrs. CHRISTENSEN. What percent of your staff do you have?

Dr. SMITH. As we have moved through the stand-up phases of the NBIS program, we have averaged between 10, 15 to 20 employees, depending upon which phase of the operation we were standing up. I anticipate that as we continue to move to first functionality, and

then full functionality, that we will end up with somewhere between 25 to 30 employees, with a small fraction of those full-time employees, full-time-equivalent FTEs.

I would estimate at this time that we have between 10 and 20 percent of our full complement of subject-matter experts. This is a little bit difficult. I don't dodge your question, but I tend to consider reach-back to subject-matter expertise both within the Department of Homeland Security and also through the partner agencies.

If I can just be personal and candid, at this time we have reached back through Dr. Clifford's organization, to the Department of Agriculture when we had some things to discuss that are inappropriate to discuss in this forum.

As well, I have picked up the phone and called Rich Besser at the table here and discussed with him, and with Rich Meyer, who is also a colleague of his at the CDC.

So I hope I addressed your question.

Mrs. CHRISTENSEN. So perhaps the coordination and the relationships are working better than they used to in our experience at the department?

Dr. SMITH. I would be hesitant to give a retrospective, but I can tell you that I am enjoying tremendous relationships with these individuals as we continue to build the culture of trust between the Department of Homeland Security and our interagency partners.

Mrs. CHRISTENSEN. Okay.

Dr. SMITH AND DR. Besser, was NBIS or BioSense used to track the recent mumps outbreak, and if so how did that work? Was there a response triggered?

Dr. SMITH. I can say certainly that the NBIS personnel were aware of this. I can say that it was on our radar screen, if you will, but I will defer any details of that, of course, to Dr. Besser.

Dr. BESSER. Thank you, Congresswoman Christensen.

The BioSense system was not used for tracking mumps. BioSense is in its infancy and at this point doesn't have the number of institutions where it would add to what we are getting from clinical diagnosis.

When it comes to surveillance, there is no system that is going to replace the astute clinician on the ground. Something like mumps is something that in general will not lead to a hospitalization. It will be seen in a doctor's office.

So our regular reporting system and our alert systems have been what has been most useful for tracking that epidemic.

Mr. LINDER. Mr. Dicks?

Mr. DICKS. Thank you. I regret that I was not here for all of the testimony, but I do want to ask a couple of questions.

First of all, the BioNet program, Ms. Embrey, you are involved in that, right? The Department of Defense?

Ms. EMBREY. The Department of Defense is engaged in BioNet, yes, with other agencies.

Mr. DICKS. Okay. Let me just ask you something. The BioNet program was intended to develop interoperable military and civilian concepts of operations and integrate military and civilian capabilities to detect and characterize a biological event. It provides common situational awareness to ensure timely, effective, and con-

sistent response actions. BioNet is a collaboration among Navy Region Southwest.

Why is it only in one part of the country?

Ms. EMBREY. I believe it was a pilot project.

Mr. DICKS. So it is a pilot project.

Dr. VITKO. I can speak to that definitively.

Mr. DICKS. Yes, go ahead.

Dr. VITKO. It is, in fact, a pilot project between the DOD and the civilian side, funded by DHS, executed by DTRA, the Defense Threat Reduction Agency, and it was piloted in the San Diego area because both civilian and military had detection capabilities there.

The idea was that they shouldn't be stovepiped; that if something happened in the community, whether on the base or elsewhere. So that was to develop a—

Mr. DICKS. What is it supposed to do?

Dr. VITKO. What it was supposed to do is actually to develop an initial template to say, this is how it could work, and then generalize that to other bases and commands and cities.

Mr. DICKS. Well, it is because you have a very large military population and a very large civilian population.

Dr. VITKO. Absolutely.

Mr. DICKS. By that, I mean civilian government workers. I just didn't want anybody to forget that in the Pacific Northwest, we have some Navy installations up there as well.

Dr. VITKO. Exactly, and we think it needs to be extended to the rest of the country.

So one of the things that was in part an outgrowth of that, and part of something else, we also—under this question that Congresswoman Christensen asked about, our leadership role—we led the formulation of this memorandum of understanding on coordinated biomonitoring among the five agencies, DOD and DHS being two of those five. And for all that, it calls for the development of these integrated CONOPS and architecture as well. So it should expand to the Northwest.

Mr. DICKS. Then you have ESSENCE, which is designed to bring together health indicator data from both military and civilian communities. What do we get from ESSENCE? Why is this important?

Ms. EMBREY. It provides us the information about the symptoms of outpatients, as well as the data about cold medications and other kinds of things, what they are buying at drug stores, some other things to help us understand earlier than people showing up at the doctor's office what is going on generally with the health of that population. It provides us just a little bit earlier indication of something going on in a community.

Mr. DICKS. Now, I missed BioWatch, the part about what this is. Apparently, you have 4,000 atmospheric monitoring stations to detect atmospheric pollutants in 30 U.S. cities. But it is not real-time.

Why is that? I notice that veterinarians collect their information in real-time. Why is it that we can't do real-time for BioWatch? Are we trying to move toward real-time?

Dr. VITKO. We are trying to move toward every several hours in an automated fashion. BioWatch represents a family of systems which detect the agent in plenty of time to begin treatment to miti-

gate its effects. It is limited by the technology that currently exists. We are developing new technology to speed up those times.

Mr. DICKS. How can we have real-time in the veterinarian field? Dr. Clifford, are you the veterinarian here?

Dr. CLIFFORD. Yes, sir. I think it depends somewhat on what we refer to as real-time.

Mr. DICKS. What "real-time" means.

Dr. CLIFFORD. Yes, sir. I think, for example, I some areas when we are talking about surveillance activities and collection of samples, we are talking about real-time as far as testing and techniques, you know, with hours versus days.

Mr. DICKS. But 4 hours I think certainly would be adequate. I mean, if you have tests coming in, test results every 4 hours, I mean, you are going to pick up on something if it is significant right away.

Dr. VITKO. Absolutely.

Mr. DICKS. What are your major concerns? What areas are you worried about in terms of what needs to be covered out there? What are the problem areas that you have in this emerging system to detect with these various sensors? What are you worried about?

Dr. VITKO. In the case of the next generation of BioWatch?

Mr. DICKS. Right.

Dr. VITKO. There are several key factors that drive the design. One is we want to expand the range of agents from where they currently are, to handle a larger range of agents. But the biggest driver is in fact to have this fully automated system, so we can get the human out of the loop. That will reduce the cost.

It will also make it accessible to smaller cities and towns, not just because it costs less, but because it doesn't have to then be near a laboratory response network. The way the system currently works, air is collected on a filter like a little vacuum cleaner filter. The filter is manually picked up, driven over to a laboratory response network, because you want to use very precise assays that don't have false alarms with them, to analyze. So to be useful, it has to be in proximity to an LRN.

When we go to a fully automated system, it will do a comparable kind of analysis, but instead of picking up the filter, it will wirelessly transmit that signal to the public health laboratory, and the same technical folks that could interpret that signal will be able to see it and act on it promptly. That means it could be placed in a building, in a local community, anywhere where you establish correct protocols.

So making it a fully automated system in a cost-affordable way and qualifying the assays so that you have the same confidence for what is done in the field as you do in one of these very well-controlled laboratories is what we are working the technology to do.

Mr. DICKS. Do you have any problem working with the Department of Defense?

Dr. VITKO. No. We work extremely well with the Department of Defense. As you heard, we have the BioNet joint pilot exercise. We just held a review of my program this past week in which we had three to four DOD participants across that. I meet monthly in a teleconference with the head of the DTRA Chem-Bio program. We

all work through an interagency community and we have these established MOUs.

Mr. DICKS. Good. Well, it sounds very positive. And when it is homeland security, it is very nice to have something very positive. Thank you.

Dr. VITKO. We thank you for that.

Mr. LINDER. Thank you. Thank you all.

This hearing is adjourned.

[Whereupon, at 3:12 p.m., the subcommittee was adjourned.]