AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMBATING TERRORISM: PROTECTING THE UNITED STATES, PARTS I AND II

HEARINGS

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MARCH 12 AND 21, 2002

Serial No. 107–156

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

84–601 PDF WASHINGTON : 2003

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

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

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

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

BERNARD SANDERS, Vermont (Independent)

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

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

ADAM H. PUTNAM, Florida
BENJAMIN A. GILMAN, New York
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia

DENNIS J. KUCINICH, Ohio
BERNARD SANDERS, Vermont
THOMAS H. ALLEN, Maine
TOM LANTOS, California
JOHN F. TIERNEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
R. NICHOLAS PALARINO, *Senior Policy Analyst*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

CONTENTS

Page

Hearing held on:
March 12, 2002 1
March 21, 2002 107

Statement of:
Bremer, Ambassador L. Paul, III, chairman, National Commission on Terrorism, Marsh Crisis Consulting; Randall J. Larsen, director, ANSER Institute for Homeland Security; Joseph Cirincione, Director, Nonproliferation Project, Carnegie Endowment for International Peace; and Henry L. Hinton, managing director, Defense Capabilities and Management, General Accounting Office 44
Keating, Frank, former Governor of Oklahoma; and Edwin Meese III, former Attorney General, co-chairman, Homeland Security Task Force, the Heritage Foundation 7
Verga, Peter, Special Assistant for Homeland Security Office of the Secretary of Defense; Stephen McHale, Deputy, Under Secretary, Transportation Security, Transportation Security Administration, Department of Transportation; William Raub, Deputy Director, Office of Public Health Preparedness, Department of Health and Human Services; Kenneth O. Burris, Director of Region IV, Atlanta, Federal Emergency Management Agency; James Caruso, Deputy Assistant Director for Counter Terrorism, Federal Bureau of Investigation; and Joseph R. Green, Deputy Executive Associate Commissioner for Field Operations, U.S. Immigration and Naturalization Service 115

Letters, statements, etc., submitted for the record by:
Burris, Kenneth O., Director of Region IV, Atlanta, Federal Emergency Management Agency, prepared statement of 146
Caruso, James, Deputy Assistant Director for Counter Terrorism, Federal Bureau of Investigation, prepared statement of 155
Cirincione, Joseph, Director, Nonproliferation Project, Carnegie Endowment for International Peace, prepared statement of 61
Green, Joseph R., Deputy Executive Associate Commissioner for Field Operations, U.S. Immigration and Naturalization Service, prepared statement of 170
Hinton, Henry L., managing director, Defense Capabilities and Management, General Accounting Office, prepared statement of 70
Keating, Frank, former Governor of Oklahoma, prepared statement of 12
Larsen, Randall J., director, ANSER Institute for Homeland Security, prepared statement of 49
McHale, Stephen, Deputy, Under Secretary, Transportation Security, Transportation Security Administration, Department of Transportation, prepared statement of 127
Meese, Edwin, III, former Attorney General, co-chairman, Homeland Security Task Force, the Heritage Foundation, prepared statement of 21
Raub, William, Deputy Director, Office of Public Health Preparedness, Department of Health and Human Services, prepared statement of 135
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statements of 3, 109
Verga, Peter, Special Assistant for Homeland Security Office of the Secretary of Defense, prepared statement of 118

COMBATING TERRORISM: PROTECTING THE UNITED STATES, PART I

TUESDAY, MARCH 12, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shay, Otter, Kucinich and Tierney.

Staff present: Lawrence J. Halloran, staff director and counsel; Dr. R. Nicholas Palarino, senior policy advisor; Thomas Costa, professional staff member; Sherrill Gardner, detailee-fellow; Jason M. Chung, clerk; David Rapallo, minority counsel; and Earley Green, minority assistant clerk.

Mr. SHAYS. I would like to call this hearing on, "Combating Terrorism: Protecting the United States, Part I," to order and welcome our witnesses and our guests.

Yesterday, we paused to remember all of those lost 6 months ago in the deadliest terrorist attack to date within our borders. In the unimaginable horror of those events, we are reminded of another harsh reality, the World Trade Center, the Pentagon, and a field in Shanksville, Pennsylvania, were not the first and will not be the last plots of American ground sanctified by innocent civilian blood.

How prepared are we for the next act of terrorism? Long before the events of September 11, 2001, panels of experts and special commissions identified critically needed actions to improve counterterrorism preparedness and response.

The General Accounting Office, GAO and others, called for timely, integrated threat assessments and a comprehensive national strategy to combat terrorism as early as 1998.

The U.S. Commission on National Security, 21st Century, also called the Hart-Rudman Commission, proposed creation of a cabinet level homeland security department to streamline and consolidate counterterrorism programs spread across more than 40 Federal departments and agencies. Governors and mayors joined the call for better first responder training and improved public health systems.

In the wake of the airline and anthrax attacks last year, air travel has been made somewhat safer, border security strengthened, and medical stockpiles are being augmented. The President created the Office of Homeland Security, and Governor Ridge has as his

first priority formulation of a national strategy framework for domestic preparedness and consequence management.

But there are signs the passage of time and pictures of a war being fought on the other side of the world may be inducing a false sense of security here at home. All checked baggage on airlines is not yet being screened. Seaports remain avoidably vulnerable. Proposals to merge border security functions have met stubborn resistance.

Medical surge capacity to treat mass casualties is not available in most communities. Inconsistency and blind spots continue to plague disease surveillance efforts. Comprehensive long-range strategy to discipline spending decisions will not take hold before the beginning of the 2004 fiscal year, 24 months after the World Trade Center towers fell.

In the war against terrorism, time is not our ally. As we speak, a clock ticks down toward the all but certain hour a chemical, biological, radiological or nuclear weapon will be used against us. We are in a race with terrorists to shut them down before that happens. Complacency, fragmentation, bureaucratic infighting, any short-sighted attachments to the status quo only increase the likelihood and depth of the next attack, the deadliness of the next attack. This is the first of two hearings to assess what has been done, what needs to be done, and what impedes faster progress in defending the United States against the menace of global terrorism.

Next week representatives of Federal departments and agencies responsible for key counterterrorism initiatives will testify. Our witnesses today bring unquestioned expertise and depth to this discussion of homeland security issues. We are grateful for their time and their work and their participation in this hearing.

Our first panel is comprised of the Honorable Frank Keating, the Governor of Oklahoma, and also the Honorable Ed Meese, former attorney general, co-chairman, Homeland Security Task Force and the Heritage Foundation.

And before swearing them in and hearing their testimony, I invite Mr. Kucinich to make a statement.

[The prepared statement of Hon. Christopher Shays follows:]

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
GROC.NS@mail.house.gov
http://www.house.gov/reform/ns/

Statement of Rep. Christopher Shays
March 12, 2002

Yesterday, we paused to remember all those lost six months ago in the deadliest terrorist attacks to date within our borders. In the unimaginable horror of those events, we are reminded of another harsh reality: the World Trade Center, the Pentagon and a field in Shanksville, Pennsylvania were not the first, and will not be the last plots of American ground sanctified by innocent civilian blood. How prepared are we for the next act of terrorism?

Long before the events of September 11, 2001, panels of experts and special commissions identified critically needed actions to improve counterterrorism preparedness and response. The General Accounting Office (GAO) and others called for timely, integrated threat assessments and a comprehensive national strategy to combat terrorism as early as 1998. The U.S. Commission on National Security/21st Century, also called the Hart-Rudman Commission, proposed creation of a cabinet-level homeland security department to streamline and consolidate counterterrorism programs spread across more than 40 federal departments and agencies. Governors and mayors joined the call for better first responder training and improved public health systems.

In the wake of the airline and anthrax attacks last year, air travel has been made safer, border security strengthened, and medical stockpiles are being augmented. The president created the Office of Homeland Security, and Governor Ridge has as his first priority formulation of a national strategic framework for domestic preparedness and consequence management.

But there are signs the passage of time, and pictures of a war being fought on the other side of the world, may be inducing a false sense of security here at home. All checked baggage on airliners is not yet being screened. Seaports remain avoidably vulnerable. Proposals to merge border security functions have met stubborn resistance. Medical surge capacity to treat mass casualties is not available in most communities. Inconsistencies and blind spots continue to plague disease surveillance efforts. A comprehensive, long-range strategy to discipline spending decisions will not take hold before the beginning of the 2004 fiscal year, 24 months after the World Trade Center towers fell.

In the war against terrorism, time is not our ally. As we speak, a clock ticks down toward the all but certain hour a chemical, biological, radiological or nuclear weapon will be used against us. We are in a race with terrorists to shut them down before that happens. Complacency, fragmentation, bureaucratic infighting -- any shortsighted attachments to the *status quo* -- only increase the likelihood and lethality of the next attack.

This is the first of two hearings to assess what has been done, what needs to be done, and what impedes faster progress in defending the United States against the menace of global terrorism. Next week, representatives of federal departments and agencies responsible for key counterterrorism initiatives will testify.

Our witnesses today bring unquestioned expertise and depth to this discussion of homeland security issues. We are grateful for their time and the work each has done to strengthen our defenses against terrorism. We look forward to their testimony.

Mr. KUCINICH. Thank you very much, Mr. Chairman. Welcome to our witnesses, Mr. Meese, Governor.

In over 20 hearings on counterterrorism, this subcommittee has heard a repeated refrain: Priorities, priorities, priorities. Scores of experts have testified before this subcommittee that the administration should take three concrete steps. First, assess and prioritize in a comprehensive way all of the threats to our country. Second, craft a national strategy that addresses these priorities in a most effective manner. And third, align budget decisions according to these priorities.

The administration has failed to take these essential steps. No comprehensive threat and risk assessment has been conducted. The administration has no national strategy. And the President's budgets proposal fails to address security threats in an organized fashion. What does this mean in practical terms? The dangers that the President's budget allocates funding to programs that are not top national security priorities, and thereby deprives other programs of needed funding. Urgent programs are being shortchanged. And the country's security could be comprised.

After September 11th and in light of the huge infusions of funding from Congress, there is no longer any excuse for operating in the dark. We need an organized plan now. We must assess threats realistically, prioritize them logically, and deal with them efficiently.

We cannot afford to waste billions of dollars for political reasons. For these reasons, Chairman Shays and I, along with Chairman Burton and Ranking Member Waxman, wrote to President Bush in October when he appointed Governor Ridge as director of Homeland Security. We urged the President to take these steps: To analyze all threats side by side. To develop a national strategy. And to align budget decisions to that strategy. We joined together in a spirit of bipartisan cooperation because these issues are some of the most important we will ever face. I would like to make our letter part of the record.

Mr. Chairman, more than 4 months later we have no response from the administration, no comprehensive assessment, no national strategy, and a budget proposal replete with funding that is not aligned with what are current threats. The administration's theological fascination with missile defense is one example.

President Bush is spending $8 billion a year on missile defense, making it the single largest weapon program in the Federal budget. Over the next 5 years the administration plans to spend over $38 billion on missile defense, and the Congressional Budget Office estimates that the full system could cost as much as 238 billion. But no threat assessment exists to justify this spending. In fact, just the opposite is true. Experts, including U.S. intelligence and military officials, have concluded that the threat of a rogue state launching a missile at the United States is not as great as other threats, particularly since such an attack would invite immediate and devastating response.

To the contrary, experts warn that the more urgent threat is from unsecured Russian stockpiles of weapons of mass destruction, nuclear devices and materials, chemical and biological weapons,

weapons expertise. All of these are urgent threats because terrorists are actively seeking these materials and resources.

In testimony before the Senate Select Committee on Intelligence, CIA Director George Tenet said, "Russia appears to be the first choice of proliferant states seeking the most advanced technology and training."

But the administration is spending only 1.5 billion to help secure Russian stockpiles. The pressing question is, how did the administration come up with these two figures? The president wants to spend $8 billion on missile defense and 1.5 billion on Russian stockpiles. Who decided on these funding levels? Upon what were these decisions based? What threat assessments were examined? Were these threats ever analyzed side by side? And, ultimately, how does the administration justify spending so much on such an unlikely threat? These are the questions I hope that we ask in today's heightened security environment.

And finally, Mr. Chairman, I think it is important that we deal with the issue of terrorism without ourself being terrified. Because fear robs us of our capacity to take rational action. Thank you.

Mr. SHAYS. Thank the gentleman.

At this time let me get some housekeeping out of the way. I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record, and that the record remain open for 3 days for that purpose. Without objection, so ordered.

And I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. And without objection, so ordered.

We are blessed with two excellent panels. Our first panel is Frank Keating, who was the former Governor of Oklahoma when the Murrah Federal Building in Oklahoma City was bombed, and 168 precious lives lost. Important lessons were learned from that catastrophe and the Governor is here to share them with us today.

And also welcome the Honorable Edwin Meese, III, who is currently the chairman for the Center for Legal and Judicial Studies at the Heritage Foundation. He was U.S. Attorney General during the Reagan administration, and is co-chairman of the Heritage Foundation report, "Defending the American Homeland."

At this time I would invite both witnesses to stand. As you know, we swear our witnesses in.

[Witnesses sworn.]

Mr. SHAYS. I would like to recognize as well—does the gentleman, Mr. Otter, have any statement that you would like to make?

Mr. OTTER. Thank you very much, Mr. Chairman. My apologies for being late.

Mr. SHAYS. No apologies necessary.

Mr. OTTER. Mr. Chairman, I want to thank you and the ranking member for holding this hearing. I also want to thank Governor Keating from Oklahoma, and the other witnesses for testifying. In the 6-months since September 11th, our country has been guarding against future attacks for the entire country.

The administration has done an admirable job appointing Governor Ridge to run the Office of Homeland Security and creating

the Transportation Security Administration to adopt new security measures for our airway systems. Much remains to be done to protect against, to prepare for the next terrorist attack.

History has shown us that the trend line for terrorist attacks casualties are steadily upward. Should our foes strike again, they will probably dwarf the losses of September 11th. In light of this real threat, we cannot afford to waste resources on duplications and inefficiencies.

As the witnesses will tell us, we are already seeing counterterrorism being used as a justification for every type of spending imaginable. Stronger controls are needed in Washington, DC, to ensure that our spending is directed to the most necessary security measures. More attention must be given to the rural areas of our Nation than the current antiterrorism strategy.

While our great cities will always be at risk of attack, rural areas contain such key critical infrastructure whose destruction would be viewed as deadly for our citizens and dangerous obviously for our economy. Rural areas also are less likely to have the resources in place to deal with a nationwide biological threat or a mass exodus from our cities.

One of the lessons of September 11th is the importance of local leadership and preparation. All of the Federal antiterrorism preparation was of little use to the mayor in New York City that morning, without the city and the State's own years of planning for a worst-case scenario.

If new Federal spending does not support our local emergency services and law enforcement, it will be worse than useless, lulling us into a false sense of security while neglecting the men and women on the ground who bear those dangerous burdens.

History will record that the terrorists who struck this country on September 11th struck without warning or without mercy. We must all work to ensure that when our foes strike again, history does not say of us that we were forewarned and we did not forearm.

So, Mr. Chairman, once again, I want to thank you very much for calling this very important meeting. I would also like to submit my little longer statement for the record.

Mr. SHAYS. Without objection. Thank you.

I would like to thank Ambassador Bremer. We wanted to have two panels and enjoy the synergy, Ambassador Bremer, of you participating in the second one.

So as well, welcome both our witnesses here. We will start off with you, Governor, and then we will go with you, Attorney General.

STATEMENTS OF FRANK KEATING, FORMER GOVERNOR OF OKLAHOMA; AND EDWIN MEESE III, FORMER ATTORNEY GENERAL, CO-CHAIRMAN, HOMELAND SECURITY TASK FORCE, THE HERITAGE FOUNDATION

Mr. KEATING. Mr. Chairman and members of the committee, thank you for giving me this opportunity to once again appear and share some perspectives from the State and local vantage point. First I want to thank President Bush for his leadership in responding to the terrorist events of September 11th and his magnificent

leadership in bringing together the world community to resist further terrorist events.

Second, I want to thank the Congress and the President for their leadership role in providing the assistance to my colleague, Governor Ridge, my former colleague Governor Ridge, in placing an emphasis on homeland security. As the members of the committee are well aware, two-thirds of the Nation's GDP is consumer confidence, and if there are frequent events like those of September 11th, there will be few people traveling, there will be fewer people investing, and it will be calamitous, not only for the people of the United States, but also for our economy as well.

I want to ask that the committee consider the formal presentation that I have placed before it, but I would like to make a couple of comments that might be of some interest or relevance to the membership, from a State and local leader's perspective.

First, I want to thank the Congress for providing some financial assistance to us to prepare and to train. I think as the Governor of Oklahoma during the Oklahoma City bombings and also the worst tornadoes ever to strike an urban area of the United States, the tornadoes of May 3, 1999, I have had regrettably my fair share of man-made and natural disasters. In all of those experiences, I have been enormously impressed with the coordinative mechanism of FEMA, the fact that we are able to draw on other State and local entities to send us assistance in our time of need. I think FEMA is a first-rate organization that does wonderful work, and I commend the Congress for their commitment to that organization.

But I would encourage you to recognize something that many of our citizens, fellow citizens don't recognize, and that is there is no such thing as a Federal posse coming to the assistance of Oklahoma City or Cleveland or whatever community you may be from. There is no such thing as a 747 filled with doctors and nurses from Walter Reed Army Hospital. The first responders are State and local officials. The second responders are State and local officials. The third responders are State and local. All of them are State and local.

When we had to ask for help and received it from President Clinton following the April 1995 bombing of the Murrah Building in Oklahoma City, the Sacramento and the Phoenix and the Los Angeles, Fairfax County, Virginia, Prince Georges County, Maryland, New York—and, yes, many of the New Yorkers who helped us in Oklahoma City were killed on September 11th—all of these were State and local officials. Only the FEMA team from New York had a law enforcement component. All of the rest were strictly firefighters. And, of course, they had knowledge of rescue and recovery procedures, and they were, as members of those teams, first rate and professional.

But it is important, following the events of September 11th, to encourage those other FEMA teams to have a law enforcement component as well. These events are criminal events. There are communities in the United States that do need the assistance of highly trained law enforcement officers as well.

Second, it is very important, I think, to provide that any plan, any system to provide for distribution of Federal funds back to the

States to prepare for another terrorist event be required, first, to be based upon a State plan.

I testified in New York in front of a—with Governor Barnes of Georgia and Governor Bush of Florida in front of a subcommittee of this House. And one of the Members asked me what was the No. 1 issue as a Governor of a State or a mayor of a State that you faced to prepare against a similar national or man-made event, and I said the lack of interoperable radio and communications equipment.

Interestingly, Governor Barnes said exactly the same thing. And obviously Oklahoma is a middle-sized State, Georgia is a much larger State, and Florida is a much larger State still. Governor Bush said exactly the same thing.

We had a tragedy in Oklahoma City, and my youngest is a state trooper in Oklahoma. But we had a tragedy in Oklahoma City where a police officer in pursuit of a criminal, with lights and sirens, went up the interstate in the wrong way. A state trooper coming in the other direction with lights and sirens pursuing someone else, neither of them communicated one with the other, both of them crashed into each other and both law enforcement officers were killed.

This is not uncommon around the United States. And the bill for replacing many of these ad-hoc decisions is to the lowest, best price for communications gear for ours is $50 million.

If those moneys are provided strictly on the basis of local need, I am afraid that we will have the same thing again. Cities will acquire, at the lowest best bid, perhaps utterly incompatible communications equipment and other cities, other counties, other law enforcement agencies, Federal, and of course any out-of-state assistance won't be able to communicate as well. It is very important that whatever we do, we do it with the State planning and regional planning, that the equipment that is purchased is compatible with Federal, State, local, even, for example, electric utilities coming from other States to assist in putting back a communications system or an electricity or a gas system that was disrupted by a natural or man-made event.

It is just very important that we have a State plan. In our State we divided up with the State into eighths. I placed an individual, an ex-FBI agent, and my commissioner of the Department of Public Safety in charge.

The FEMA, or the State version of FEMA, the local rescue and recovery people are a part of that. We have two pieces. We have an avoidance piece, that is a prevention piece, as well as a response piece. I think it is as sophisticated as any State in the union. But it only works as long as all of those people can communicate each with the other. For the first time now we have a public health component, something we have not had before.

By the way, I also would encourage that FEMA be required to have a public health component. When they come into a State, that is something that is extraordinarily important.

Also on that same note, I might add that I know, Mr. Shays, after Dark Winter last summer, I had the opportunity to appear with others to testify before you and the members of this subcommittee. But we discovered then that if there were a bioterror-

ism event and it took many days to determine what in fact had happened, those are many days to create panic, those are many days to create mayhem.

So to the extent that there can be an aggressive research and development program—we defeated the Germans and the Japanese in 4 years in World War II. We ought to be able to provide an ability quickly to identify anthrax or smallpox or some other bioterrorism challenge and not have to wait several weeks before we know if, in fact, there is a problem.

Also—and I appreciate the leadership of the members of this committee as well. It is important for us at the State and local level to know that if an event occurs, what is it that occurred, what kind of dosage units are available and where to provide for vaccinations for our rescue and recovery personnel, and we want to make sure that we can identify whatever that event is quickly so we can vaccinate our rescue and recovery people to prevent them getting sick and provide an opportunity for our citizens to be safe.

As you know, one of the problems is if there is an—if there is—there is a suggestion of a bioterrorist attack, it may well be that if the people working in public health, a third don't show up, because they don't want to get sick, a third may already be affected, and maybe you only have a third of the people who can really address the issue at hand, namely the protection of the public. This is a very complex and a very, very worrisome potential scenario to me. And in our own murder board, if you will, our own actions and reactions at the State level, the public health piece is the one that is the least sophisticated to start, because we never imagined something like this to happen to the United States.

Let me mention something briefly about the avoidance or the prevention piece. There are more State and local law enforcement officers out there than Federal agents. Today most States require police officers in urban areas, even State troopers, to be college graduates.

When I was an FBI agent, you had to be a lawyer, accountant. Many States today, their local police, State police are as well educated and as well trained as any Federal agents. There are a lot more of them out there. And we need obviously to encourage the sharing of intelligence between the Federal authorities and State and local authorities. They are best positioned to identify on the ground what could happen and best positioned—to be in a position if someone is in the United States meaning us harm to make arrests and to avoid—we find in our State the FBI has been excellent in coordinating with us. If there has been a failure it has been on our part to change the open records and open meetings laws to permit them to share intelligence with us. That is something we are addressing this legislative session.

I commend to the members of the committee that is a problem in every State. Every State needs to look at their statutes to make sure that they can coordinate with the Federal authorities. But we are only as good as the intelligence given us. If the intelligence given us is inadequate or incorrect, we will take action or we won't take action to the—to the great disservice of our people. That has to be addressed.

We do need assistance in training. I think it is very important that the Congress provide a seamless mechanism out there where people come to our State or our people go to your State, they know how to react, and they have been trained pretty well similarly.

If you have a regional event, for example, in our State, let's say, a train derails in a rural area right across the border from Texas and it is a much more urban area, the people who will come rushing into Oklahoma will be from Texas, not from Oklahoma. There wouldn't be that number of people in our—in that part of the State to respond. So they need—we need to have intercommunications equipment that is interoperable on the regional level. We have to have people trained on a regional level. We have to have the sharing of intelligence and the sharing of preparation on—in intelligence on a regional level, not just simply on a State level.

I would encourage, and I have to my fellow Governors and mayors, that they look at all of these issues and they focus on the best intelligence provided us by the Federal Government, the best intelligence we develop ourselves and murder board and prepare over and over again, so that in the event something happens we are truly and well prepared so that the public has a sense of confidence and trust.

[The prepared statement of Mr. Keating follows:]

Testimony of Gov. Frank Keating (R-Okla.)

House Subcommittee on National Security, Veterans Affairs,

and International Relations

March 12, 2002

I am grateful to the subcommittee for inviting me to visit with you today.

As you know, during my first months as Governor of Oklahoma, I confronted what was at that time the worst act of terrorism on American soil, the April 19, 1995 bombing of the Murrah Federal Building in Oklahoma City. We learned some important lessons from that tragedy which were repeated in New York and Washington and Pennsylvania on September 11. Last year I also played the role of a state governor in the Dark Winter bioterrorism exercise. My early training was as an FBI agent, assigned to investigate internal security matters. I have been a United States Attorney in my state and later served in the Justice and Treasury Departments, overseeing law enforcement functions. I don't claims to be an expert on terrorism, but I do hope to offer my experience -- some of it hard won -- on this most timely subject.

My written testimony will be relatively brief. I want to confine myself to several issues of importance to the subcommittee's deliberations.

First, we learned some important lessons in Oklahoma City in 1995, and those lessons were reinforced in Washington and New York on September 11, and in the anthrax assaults on Americans

that followed.

First among them is that in any act of terrorism, the first responders will always be local. In 1995, and again in 2001, those first on the scene were local and state law enforcement and fire service professionals -- and we all know how many of them gave their lives in New York. Local and state first responders in Oklahoma City were also joined by federal law enforcement officials from local field offices -- but again, they were local, not from Washington. This was also true in the Dark Winter bioterror scenario; the first responders there, as in the anthrax outbreak last fall, were local physicians and emergency room and public health personnel.

The lesson is clear: the war on terrorism is a military and intelligence battle best fought at the federal level, but the front lines of homeland security remain local. I believe we must strongly resist any effort to repeal or ignore the historic American doctrine of posse comitatus. You cannot federalize local response. Support it, yes, through such outstanding federal agencies as FEMA, the FBI and the Centers for Disease Control. Install umbrella control where and when such control is necessary and logical, as in intelligence gathering and dissemination. But let's remember that the people who died bringing aid to the scene at the World Trade Centers were local fire and police personnel. The sole rescuer killed in Oklahoma City in 1995 was a nurse. These people are the experts, just as Special Forces and CIA teams pursuing terrorists abroad are the experts at what they do. The lesson of Oklahoma City -- and of September 11 -- is to allow the experts to do what they each do best, and to resist the urge to federalize everything.

I also want to note that in Oklahoma we have a unique resource in this effort to better prepare and train local and state first responders -- the Oklahoma City National Memorial Institute for the Prevention of Terrorism, headed by General Dennis Reimer, the former Army Chief of Staff. This organization is rapidly becoming the national and international go-to resource and central clearing house in how to best prepare local and state public safety agencies to respond to -- and hopefully to prevent -- terrorist acts. It is a priceless resource for our nation, and I hope the subcommittee and the Congress will listen to and utilize General Reimer and his staff as you allocate resources and set

priorities.

In my state, and in many others, we now have joint local-federal anti-terrorism law enforcement task forces, which are working well. But the same principle applies: the agencies involved must retain autonomy to each do what they do best.

My second central point has to do with commendable efforts by Congress and the administration to flow federal dollars to the first responder level.

Like other governors, I am heartened by federal efforts to fund and support state internal security efforts. However, there is a danger here -- you cannot devise a one-size-fits-all funding solution, and you cannot dilute those funds by parceling them out among a myriad of local agencies.

For example, Oklahoma has responded by creating eight rapid response districts within our state. The federal government has provided initial funding to operate them, but future federal funds are needed to keep them at peak efficiency, ready to respond to any terror incident or threat. In addition, we learned in 1995, following the Oklahoma City bombing, that we have an "Achilles heel" in our public safety operations . . . the lack of common radio systems and frequencies to allow local and state agencies to communicate in times of crisis. That's Oklahoma's greatest immediate need, to create such a system, and it will cost about $50 million. We won't build it if federal funds flow piecemeal to a hundred local agencies.

Other states have their own unique needs. For example, events near the border of one state could directly affect communities in a neighboring state, as the events in New York and Washington on September 11 impacted surrounding communities. There are no borders to terrorism; as we learned in Dark Winter, biological agents released in one place would rapidly spread across those borders. For that reason, I would urge the Congress and the administration to apportion federal funds designed to assist states and localities in homeland security efforts to the states, in block grants, permitting them to use those funds to fill the most pressing downstream needs among their own local agencies, and to most precisely meet their specific needs. We cannot afford to dilute these funds.

They must be precisely targeted, and I know that most governors have already conducted needs assessments at the state level that have identified what they need most. Let's allow them to spend those dollars to meet those needs.

Seventy-five percent of projected federal dollars in this effort are earmarked for local agencies. I believe it is important to make distribution of those funds to those agencies contingent on the development of a statewide plan, and on how local initiatives fit into that overall plan. Just as the federal government must retain command and control authority over the international war on terrorism, so must the states act in a policy role for the allocation of funding and resources within their borders.

A second immediate priority many governors identified in the wake of September 11 was for a steady and accurate flow of intelligence information to the states. I faced a situation last fall that was almost laughable, if it hadn't been for the seriousness of the times. My state adjutant general received a terrorism warning, but he couldn't brief me, the man who appointed him, or my commissioner of public safety, a retired FBI special agent in charge, because we lacked the proper security clearances!

It does little good to tell state officials that something bad might happen, and refuse to tell them what, where or when.

Happily, we are addressing that problem, and information on security threats is flowing to the states more effectively. As we proceed with the war on terror and our homeland security efforts, I hope we will continue to keep those lines of communication open. Give us the information in a timely manner, and we will continue to be the homeland's front line in defending our citizens against terrorist threats.

I want to conclude with some general comments on the events since September 11. I join all Americans in applauding President Bush's decisive and effective decision to pursue terrorism to its roots. He is absolutely correct to have further identified the "axis of evil" nations as potential threats

to civilized society, and to pursue policies that neutralize those threats. Imagine the lives and misery the world would have been spared had we had a "Bush doctrine" against Hitler in 1938,, instead of Neville Chamberlain's appeasement policies. You cannot negotiate with or appease murderers. Our country is following the right course, and I can assure you that the people of my state, having experienced terrorism close up in 1995, are firmly behind the President in this effort.

As a veteran of the ominous Dark Winter exercise, I also support aggressive efforts to stockpile medications and vaccines, and to pursue new medical defenses against bioterror agents In Dark Winter, more than a million mythical Americans died of smallpox. We must do all we can to keep that exercise a myth, and to prevent it from becoming a horrifying reality.

Finally, I want to commend former Governor Tom Ridge for his leadership. It is not an easy task to pull together dozens of different agencies in a common cause, but he has done well. His was a fine appointment, and I know I join my fellow governors in offering him our support.

I want to thank the subcommittee for holding this hearing, and for your continuing efforts to protect America.

Mr. SHAYS. Governor, thank you. Your oral statement only is identical to your written statement, very thorough and very helpful. I would like to thank you publicly for so many of the families who lost loved ones in the bombing in Oklahoma City, their participation up in New York.

I had a number of families from the Fourth Congressional District who lost loved ones, and they found tremendous guidance and comfort from people from Oklahoma who came to New York.

Mr. KEATING. Thanks, Mr. Chairman.

Mr. SHAYS. Also, just to let you know, on April 23rd we will be having a hearing on the allocation of radio frequency spectrum and proposals to designate certain frequencies for police, fire and emergency medical use, both nationally and, frankly, internationally. So we are going to be trying to followup on that.

Attorney General Meese.

Mr. MEESE. Thank you, Mr. Chairman.

I am honored to have the opportunity to appear before this committee and particularly to join my good friend, Mr. Keating, and my colleague and co-chairman ambassador Bremer.

Mr. SHAYS. We are honored to have you.

Mr. MEESE. I would join Mr. Keating in expressing appreciation for the outstanding leadership of President Bush in dealing with both the international and the domestic aspects of terrorism.

Following the September 11th attacks, the Heritage Foundation established its homeland security task force which brought together some of the best experts in the world on this subject.

It included a former chief of staff of the Army, a former commandant of the Marine Corps, Mr. Keating himself was a member of that task force, a number of police chiefs and others who had particular expertise in this field.

That report and the findings of that commission which, by the way, looked at all previous commission reports and other recommendations to see what had been accomplished up until that time, what continued to need to be accomplished, has been summarized in this booklet, "Defending the American Homeland."

And I would ask, Mr. Chairman, that be entered into the record, along with a full copy of my testimony, since I will be limited in what I can present here.

Mr. SHAYS. That will be done. Thank you.

Mr. MEESE. Thank you. Since that time we have had briefings for White House Office of Homeland Security, Governor Ridge, Members of Congress, and other organizations and individuals that were interested in the subject. We have a continuing dialog with the Office of Homeland Security, including a conference that will take place later on this afternoon.

Basically our report covered four major areas: Protecting the Nation's infrastructure, strengthening civil defense against terrorism, improving intelligence and law enforcement capabilities, and military operations to combat terrorism.

In regard to protecting the Nation's infrastructure, I think it is important to stress what Mr. Otter mentioned earlier, that many of the facilities in the infrastructure are located in rural areas, particularly nuclear facilities, power plants, that sort of thing.

When we talk about infrastructure we really are talking about a variety of very critical items within our Nation, such as communications networks, utilities, water supplies, banking and finance systems, transportation nodes, and intelligence systems.

And that is why this particular recommendation is so important. Part of this also involves local and State officials, because obviously the inventory of the infrastructure assets that need to be protected can best be done at the local level where the officials there will know what are the particular facilities, plants and otherwise that need to be protected, and so it is very important to facilitate the communication on infrastructure issues between the Office of Homeland Security and other Federal agencies and State and local officials.

One of the interesting things in our report was the highlighting of the fact that the global positioning system is one of those critical infrastructure items. And I was pleased to see just within the last week or so that is being recognized by the Federal Government as one of the particular items in our infrastructure that will in fact be protected.

In terms of strengthening civil defense against terrorism, as Mr. Keating mentioned—and one of the critical items is the protection against bioterrorism, since that is the one thing that is new to the inventory of potential disasters. As the Governor pointed out, we have things like railroad accidents, we have hurricanes, we have earthquakes and various other types of major incidents. But our country has never really experienced a bioterrorist attack, and so the chemical and biological aspects of terrorism particularly deserve attention, and the inclusion of the health component in our planning and preparation to deal with those kind of incidents.

I would indicate particularly the importance of, at the present time, I believe the country is without a surgeon general, and that might well be the key place where the Federal Government could concentrate its leadership in terms of coordinating the various Federal agencies, since the National Institutes of Health, the Center for Disease Control and Prevention and other aspects of the Department of Health and Human Services would be involved.

But it is critical that the planning include the State and local officials, officials such as the State departments of public health and county and city departments of public health, as well as extending this cooperation to the medical profession, which is largely in the private sector, as well as, of course, our series of hospitals.

It is my understanding that at the present time that the Center for Disease Control and Prevention has a network of some 115 hospital laboratories throughout the country that are prepared to analyze a potential attack, chemical or bioterrorist attack. But it is important that there be the coordination with the local officials so the information can get from local doctors and local health officials to these laboratories.

In terms of intelligence and law enforcement, one of the critical issues is the one that the Governor mentioned, that is the willingness and ability of intelligence sharing on a two-way basis between or among all of the levels of government.

In the past, much of the knowledge that we have had of terrorist incidents, and I am not—even before September 11th came from

local officials who saw something strange in their particular jurisdiction. In many cases they were the ones that actually apprehended the potential terrorist. It is very important that the steps be taken so that local law enforcement officers have the information, the intelligence that is possessed at the Federal Government level, that there be communication links so that local officials can provide that information to the Federal agencies.

At the Federal level, the principal recommendation in terms of intelligence is that there be a fusion system, so that the information coming in from a variety of sources can be brought together and analyzed and processed in a central clearing house, and that then would be the—would give the ability for this information then to be disseminated out to those agencies at all levels of government where it can be utilized.

The other major recommendation in terms of law enforcement has to do with control of our borders, and the importance of making sure that information particularly is transmitted to those officials who have something to do with the border control or the control of people, particularly foreign nationals, that are coming into this country. A very important element that often is left out is the fact that we can best control our borders by dealing with foreign nationals coming into this country at the source. In other words, at the foreign country location where they receive their visas. And that is why the consular service of the State Department needs to be brought into this whole system of information, particularly about foreign nationals who might have a potential for terrorist activity.

In addition to this, it is important that we control those foreign nationals within our borders. It is estimated that over 300,000 foreign nationals are now illegally in the United States, a large proportion of them illegal in the sense that they have overstayed their visas or they have not complied with other requirements of being in this country. And so aspects of controlling that type of foreign national, which specifically pertains to the people who were involved in the September 11th incident, ought to be a very high priority.

Finally, our fourth area of recommendation had to do with military operations to combat terrorism. And there, it is clear that the most important military element to deal with homeland defense is the National Guard. This involves two major policy changes at the Federal level.

One is to be sure that there is adequate funding for the National Guard in order to provide for their homeland defense mission, which often would otherwise be left to State funding which, as the Governor mentioned, is not really available in concrete terms.

And the other thing is that our national war plan must be reviewed to be sure that we are not depending upon National Guard troops to be serving overseas in the series of military activities taking place in foreign nations at the time that they may be needed for homeland defense within this country.

We also, I think, have to review the issue of to what extent we want National Guardsmen to be on duty essentially full time, as they are presently at the airports, inasmuch as this interferes with the concept of citizen soldiers or citizen military personnel in which

they still have to go about their normal jobs and carry out the responsibilities of their employment.

Finally, Mr. Chairman, members of the committee, let me make a couple of observations that cover the entire report. One is, we believe it is absolutely critical that homeland defense and homeland security be engaged without in any way violating the essential liberties guaranteed by the Constitution. We feel it is possible with the proper planning, with the proper oversight, of the entire homeland security effort that we can indeed continue, even though we may deal—we may have to invade some of the conveniences that people enjoy, such as at airports, which we know about at the present time. But the basic protections of the Constitution must be guaranteed to all U.S. citizens at all times, including time of war.

Second, I would reiterate what the Governor said in terms of the first responders. We know it will be the local police and fire who are responsible, and medical emergency medical services for the initial response. This means that Federal funding must be adequate to give them the necessary planning and coordination capabilities to give them the equipment they are going to need, to give them the training, particularly, and Federal agencies can be very helpful as in the FBI providing intelligence training to local law enforcement.

But particularly the point that the Governor made, which I would like to reiterate and which is contained in our report, the importance of exercises to work out the plans, to see what works and what doesn't, to see what glitches occur, to see what difficulties there are, and I suspect, as the Governor mentioned, the communications difficulties, the interoperability of radios, for example, will be one of the first things that would be recognized if an exercise were held today.

Third, it is important, I believe, that the intelligence, as I mentioned earlier, be shared horizontally among Federal agencies, and then vertically with State and local agencies.

And finally, let me again mention the fact that control of our borders is an absolute key if we are going to provide adequate protection against terrorism.

Mr. Chairman, I believe that concludes my testimony, but I would be happy to respond to any questions.

[The prepared statement of Mr. Meese follows:]

TESTIMONY OF

EDWIN MEESE III

CHAIRMAN

CENTER FOR LEGAL AND JUDICIAL STUDIES

THE HERITAGE FOUNDATION

214 MASSACHUSETTS AVENUE, NE

WASHINGTON, DC 20002

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,

AND INTERNATIONAL RELATIONS

REGARDING:

COMBATING TERRORISM: PROTECTING THE UNITED STATES

MARCH 12, 2002

Good morning Mr. Chairman and Members of the Subcommittee and thank you for inviting me to testify at this hearing on combating terrorism. For the record, I served as the United States Attorney General from 1985-1988; and am currently the Chairman of the Center for Legal and Judicial Studies at

The Heritage Foundation.

The Heritage Foundation is a public policy research and educational organization operating under Section 501(c)(3) of the Internal Revenue Code. It is privately supported, and receives no funds from government at any level, nor does it perform any government or other contract work. In 2001, The Heritage Foundation received 93% of its funding from its approximately 200,000 individual supporters. The remaining 7% came from investment income, publication sales, and corporate contributions.

Few events have so crystallized the threat of terrorism that America's enemies pose to its people, its international stature, and its very civilization as have the attacks of September 11. America is dangerously vulnerable to this new form of terrorism. New means are needed to rapidly strengthen the security of the American homeland —to protect critical infrastructure, boost civil defense, and increase intelligence and military structures in order to prevent future attacks and limit the effects should one occur.

Following the September 11 attacks, The Heritage Foundation established its Homeland Security Task Force, bringing together some of the best experts in the world on the subject of counter-terrorism and homeland security. This Task Force reviewed the vast number of proposals that had previously been put forth by commissions and legislative initiatives. The Task Force then proceeded to develop top priorities for action at all levels of government and to devise concrete steps to implement these priorities and make them operational.

Since the publication of the Task Force report, we have held briefings for the White House Office of Homeland Security, members of Congress, and other organizations and individuals interested in this subject. We have also made copies of the Task Force report available to the public generally.

Our report covered four major areas:

- Protecting the nation's infrastructure,
- Strengthening civil defense against terrorism,
- Improving intelligence and law enforcement capabilities, and
- Military operations to combat terrorism.

For each of these major topics, a series of priorities were recommended:

PROTECTING THE NATION'S INFRASTRUCTURE

Most Americans recognize that protecting critical infrastructure from acts of terrorism is a responsibility that does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's critical infrastructure so that terrorists have less incentive to target them and the nation can respond quickly if they do. The success of efforts to defend and protect infrastructure will rest primarily on the ability of Federal, State, and Local governments to communicate and cooperate effectively with each other and with the private sector.

To protect America's critical infrastructure, such as communication networks, utilities and water supplies, banking and finance systems, transportation nodes, and intelligence systems, the Working Group on Infrastructure Protection and Internal Security has established the following top priorities for Federal, State, and Local efforts.

- **Priority #1: Reorganize by presidential directive all Federal agencies involved**

  in protecting critical infrastructure. The President should reorganize the Federal government to enhance its ability to protect the homeland. President Bill Clinton issued an infrastructure protection directive, known as PDD–63, to assign responsibility for addressing the security of 12 specific infrastructure sectors to various Federal agencies. However, his directive failed to create a system of oversight or establish a clear chain of command to ensure that agency efforts were adequately enhancing the security of these sectors. The new presidential directive should correct this deficiency by requiring annual assessments of Federal agency efforts; clarifying the chain of command for infrastructure protection efforts that involve Congress, State and Local entities, as well as the private sector; and improving coordination and information sharing.

- **Priority #2: Designate the Global Positioning System (GPS) frequencies and**

  network as critical national infrastructure. The GPS satellite network is an enabling system for other infrastructure systems, such as telecommunications, that are vital to the nation's security. Disruption by terrorist groups or hostile states could jeopardize America's homeland security, but the GPS has not been designated as a vital national asset. President George W. Bush should immediately add the GPS to the current list of vital national infrastructure and assign responsibility for its security to the U.S. Department of Defense (DOD). Immediate steps should begin to make the GPS network more secure.

- **Priority #3: Facilitate communication on infrastructure issues between the new**

  Office of Homeland Security (OHS) and State and Local officials. State and Local governments play a vital role in protecting the infrastructure within their jurisdictions. In the event of a possible

terrorist attack, however, they cannot do so effectively without communications from the Federal government. Before such communications—which could include classified information —can occur, many States will need to reform their public meeting disclosure laws so that information concerning suspected terrorist activities and vulnerable infrastructure will not be made public and compromise prevention, apprehension, and deterrence. Appropriate response exercises that include the relevant Federal, State, and Local officials should be conducted for various attack scenarios, which will enable better communications should an attack occur.

- **Priority #4: Enhance the private sector's role in infrastructure protection.**

Market forces provide a strong incentive for the private sector to protect any infrastructure it owns and operates. Government should not inhibit industry efforts to do so, and it should ensure that businesses have the tools they need to increase their ability to protect vital infrastructure, such as telecommunication networks. Congress should remove any legislative roadblocks that exist to improved communications with the private sector, and tax penalties that make it more difficult for private industry to invest in greater security should be eliminated. Moreover, new security standards for protecting each type of infrastructure and new risk assessment programs should be developed and shared with the relevant businesses.

- **Priority #5: Institute new rules to monitor more closely who or what is entering**

America's airports and seaports. Since September 11, new efforts to increase security at vital transportation nodes have focused primarily on manpower, such as federalizing baggage inspectors at airports. A comprehensive program to increase airport and seaport security requires tighter controls on who and what is passing through America's portals. New Federal systems should be developed to share passenger information that would help prevent a potential terrorist from even boarding a plane. A Federal interagency center also will be needed to analyze information about the people and products entering the United States by sea. The U.S. Customs Service should begin experimenting with a point-of-origin inspection program for maritime trade. The Sea Marshals program should be expanded quickly. And the Transportation Security Agency should issue a new regulation to require airports and port administrations to assure that only authorized people can enter secure areas.

- **Priority #6: Secure all Federal networks and information systems.**

The U.S. General Accounting Office has reported that the information systems vital to Federal operations are not sufficiently protected. Without tighter security, continuity of operations cannot be guaranteed. Federal agency technology purchasing guidelines should be revised to place a premium on security. The executive branch also should explore alternatives to the proposed government only Internet system (GOVNET) before making a procurement decision.

- **Priority #7: Accelerate government compliance with the Nuclear Waste Policy Act.**

Despite legislation requiring that it do so, the U.S. Department of Energy (DOE) has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiologic weapons. According to the department, it is already running 12 years behind schedule. Congress should hold hearings to determine how DOE can bring the new storage facility at Yucca Mountain, Nevada, on-line more quickly and improve security.

STRENGTHENING CIVIL DEFENSE AGAINST TERRORISM

Unlike defending the nation from military attacks, civil defense begins with preparation and planning at the local level. The first responders to an emergency are usually local emergency workers and volunteers—a fact poignantly illustrated on September 11. Should terrorism occur again in the United States, America's firefighters, law enforcement officials, emergency medical services personnel, health professionals, and hazardous materials crews will be the front-line fighters. However, they are not adequately prepared today to respond to or prevent a terrorist attack using weapons of mass destruction.

To assist Local, State, and Federal officials in improving their ability to detect and respond to an attack on civilians using chemical, biological, radiologic, or nuclear (CBRN) agents, the Working Group on Civil Defense Against Weapons of Mass Destruction has established the following top priorities.

- **Priority #1: Build a nationwide surveillance network for early detection of**

  chemical, biological, or other attacks. In order to mobilize a rapid response to such attacks, government officials must be able to recognize the initial stages of an outbreak of catastrophic illness or attacks on food and water supplies. This requires a nationwide network of locally based surveillance procedures and systems to monitor these vital sectors, and nationally developed monitoring standards and reporting guidelines so that information can be disseminated quickly. The Federal government should also take steps to foster the development of more sensitive monitoring technologies.

- **Priority #2: Develop a terrorism response checklist and a manual of civil**

  defense exercises to guide officials in assessing preparedness. Local and State authorities must prioritize the elements of any effort to improve the ability to respond to a CBRN event. The Federal government should assist the States by developing national standards of preparedness and by designing new evaluation tools to help them assess their own weaknesses and to determine how best to proceed. The guides, developed by a task force under the direction of the OHS, should be completed within the next six months and made available on the Web site of the Centers for Disease Control and Prevention (CDC). In addition, the Federal government should conduct CBRN response exercises, first with states most at risk of terrorism and building gradually to multi-state exercises over time.

- **Priority #3: Accelerate the development of pharmaceuticals that prevent or limit**

  the spread of toxic agents by terrorists. Given the urgency of protecting Americans from biological terrorism, which followed the recent anthrax deaths, the Federal government should facilitate more rapid development and supply of new and safer vaccines, drugs, and other medicines that would provide immunity to such diseases as smallpox or that would limit the effects of an outbreak after a terrorist incident. This will involve establishing reasonable requests for proposals for developing CBRN-related pharmaceuticals; guaranteeing patent protection for products related to terrorism; improving the fasttrack approval process for these products; and stimulating the development of generic drugs after patents have expired.

- **Priority #4: Create a national web of CBRN experts who will train first response**

  teams for an outbreak or terrorist attack. A program that can identify these experts and deploy them in teams to share their expertise and train local first responders would be an affordable and effective way to prepare for a CBRN attack. Congress should provide adequate funding for expanding the Train-the-Trainer programs in the Office for Domestic Preparedness.

- **Priority #5: Simplify the process of obtaining Federal assistance for civil defense**

  initiatives. An OHS block grant program should be established so that State and Local authorities can target federal funding to their unique civil defense needs. Current agency grant programs should be streamlined into a single grant application process administered by the OHS. To ensure that federal funds get to the localities that need them the most to boost preparedness, a new homeland security block grant program also should be established under the Federal Emergency Management Agency (FEMA). All grants should be conditional, non-transferable, and made accountable through new reporting requirements.

- **Priority #6: Sign mutual support agreements with Canada and Mexico on**

  responses to terrorist acts in border communities. The possibility exists that a terrorist could release a biological or radiologic attack on the United States without ever crossing the border, with serious consequences for people in both countries. The United States should sign mutual terrorism support agreements with Canada and Mexico on preventing such attacks and managing their consequences should they occur.

- **Priority #7: Develop a nationwide education and public relations program.**

  In a democracy, governments at all levels must mitigate fears of attack while building support for their efforts to protect the public. Public relations campaigns can be vital to preventing panic, improving civil defense preparedness and responses, and maximizing all efforts to prevent terrorism. Successful campaigns will require a terrorism-related public relations strategy for improving cooperation with local media to enhance the dissemination of information to the public.

IMPROVING INTELLIGENCE AND LAW ENFORCEMENT CAPABILITIES

Since September 11, many are questioning the ability of government agencies to gather and communicate actionable intelligence to enable them to apprehend terrorists before they strike and to deter them in the future. Federal, State, and Local officials recognize that more resources must be focused on improving intelligence so that government agencies, emergency personnel, and first responders can more effectively respond to those who would harm American civilians.

The capabilities of and relationships between law enforcement agencies (LEAs) at the Federal, State, and Local levels and the Intelligence Community have received comprehensive reviews, such as in hearings before the House Permanent Select Committee on Intelligence and in its 1995 report, *Intelligence*

Community in the 21st Century; by the 1996 Brown–Rudman Commission; and in more recent reviews by the Hart–Rudman, Bremer, and Gilmore Commissions. Many of the excellent recommendations made by these commissions and studies have yet to be fully implemented.

September 11 sent a powerful message to decision-makers that much more needs to be done to protect the homeland, and quickly. The Administration and Congress have sought to address some of the bureaucratic problems exposed by the attacks by passing the USA PATRIOT Act (P.L. 107–56) and the FY 2002 Intelligence Authorization Act (H.R. 2883). They recognize that no single action, law, or institution—no one-step remedy—will combat all of the threats the United States and its citizens face.

A multifaceted approach to homeland security is necessary. Building on the recommendations of earlier commissions and post-September 11 legislative efforts, the Working Group on Intelligence and Law Enforcement has identified the following top priorities for improving the ability of law enforcement agencies and the Intelligence Community to protect the homeland.

- **Priority #1: Require the Office of Homeland Security to direct the assessment of**

  threats to critical assets nationwide. The first important step in homeland defense is providing appropriate information to government officials to help them determine what assets, critical to the nation's economy and security, remain vulnerable to terrorist attack and whether the responsible agencies and institutions are organized and equipped sufficiently to protect them. A first step in this process must be the development by the OHS of a uniform methodology for assessing the risk to possible targets and the level of threat to those targets, and establishing the methods for sharing the findings. Based on the compiled assessments, the OHS Director should establish a national strategy for protecting the homeland and direct his office to develop a national alert and warning system.

- **Priority #2: Rapidly improve information-gathering capabilities at all levels**

  of government. For Federal, State, and Local law enforcement officials, a first line of defense against terrorism and other threats to the homeland is access to timely, reliable, and actionable information from both foreign and domestic sources. Rapidly enhancing government's ability to acquire and analyze this information is vital to homeland security. The President should direct the Director of OHS to establish a national intelligence coordinating group whose task is to develop a national strategy for gathering and sharing intelligence. More federal resources should be targeted to strengthening foreign intelligence collection capabilities, as well as domestic sources of information critical to homeland defense. This includes strengthening the measurement and signature intelligence (MASINT) capabilities of the Intelligence Community and maximizing current agency capabilities to cross-cue intelligence and increase human intelligence (HUMINT).

- **Priority #3: Improve intelligence and information sharing among all levels**

  of government with homeland security responsibilities. The need for better sharing and

dissemination of acquired information to all levels of government became clearer in the days following September 11, but improving LEA– Intelligence Community cooperation will have far more to do with changing bureaucratic cultures that resist change than with revising current statutes or regulations. The President should direct the appropriate Cabinet Secretaries and officials to work together to create an all-source Federal-level information fusion center, to which all intelligence information goes and from which it is disseminated on a need-to-know basis. The OHS Director should develop a cooperative structure for the sharing and disseminating of this information, which will include classified information. Federal funding and training should be targeted to assist State and Local LEA information-gathering efforts.

- **Priority #4: Strengthen the visa approval and border security mechanisms.**

  Legally entering the United States was remarkably easy for the September 11 terrorists. America's visa approval and entry–exit processes, and the ability of LEAs to enforce existing immigration laws against aliens who are in violation of those or other laws, should be strengthened. Consular officers need more information upon which to make their decision about granting each visa. A Federal-level lookout database should be created and made accessible to officials involved in border security. The "45-minute" rule that requires Immigration and Naturalization Service (INS) inspectors to clear all passengers on international flights into the United States within that time period should be repealed. The Visa Waiver Program law should be amended to allow the Secretary of State to use it to encourage countries to institute greater antiterrorism border control mechanisms. The U.S. government should expedite the development of tamper-proof travel documents, explore the development of an exit monitoring mechanism, strengthen INS's ability to enforce the law against aliens who violate their visas, institute comprehensive procedures for handling immigration cases that involve classified documents, and help State and Local LEAs develop a standard format for "rap sheets."

- **Priority #5: Eliminate the opportunities for identity theft and fraud in state**

  identity document systems. False identity documents are a major problem, and the terrorists involved in the September 11 attacks exploited the States that have the systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse must recognize that it is placing the lives of Americans in jeopardy. Current procedures for the issuance and recording of identity documents, such as driver's licenses and birth and death certificates, must be tightened and a mechanism developed to deter and prevent identity theft. Development of tamper-proof documents should be a priority.

- **Priority #6: Create a mechanism to monitor recent anti–money-laundering**

  initiatives to obstruct the financing of terrorism. Many of the deficiencies of efforts before September 11 to obstruct the financing of terrorist activities were addressed in the USA PATRIOT Act, but the financial services area is dynamic, and those who seek to harm the United States will continue to attempt to circumvent the current regulatory structures. To better anticipate how existing anti–money-laundering restrictions can be circumvented, the Secretary of the Treasury should create a mechanism to evaluate the current laws.

MILITARY OPERATIONS TO COMBAT TERRORISM

The 1997 National Defense Panel (NDP) report is but one of many that gave clear warnings to the people and policymakers that the United States homeland was at risk of terrorist attack. Other studies made it clear that the U.S. armed forces must be prepared not only to identify impending catastrophic terrorist attacks, but also to preempt or respond to them rapidly, working with the Intelligence Community and Federal, State, and Local officials.

In any restructuring of the forces to meet a rising threat, care must be taken to ensure a continued balance between unconventional and conventional force capabilities. A number of studies have suggested how to accomplish these objectives, but their recommendations have not been systematically implemented.

The Heritage Foundation Working Group on Military Operations has attempted to address this problem by identifying the following top priorities for improving military anti-terrorism operations to defend the homeland.

- **Priority #1: Free the National Guard and Reserves for homeland security and**

  boost port security quickly. Homeland security will require enhancing the capabilities of National Guard and Reserve units to respond to terrorist events. This means freeing some of these units from having to provide combat support and combat service support for the active forces by adding more active duty personnel to current force levels. It means ensuring that the National Guard has standing emergency plans to train and work with Local authorities on homeland defense and consequence management. It will require the development of coordinated public information campaigns. It also will require reinstituting a U.S. Navy–U.S. Coast Guard coordinated port security program to check all incoming ships and containers to prevent weapons of mass destruction from entering the United States.

- **Priority #2: Protect U.S. borders, coasts, and critical national infrastructure with**

  air defense and missile defense. The threat of attack by aircraft, cruise missiles, and ballistic missiles requires that the United States establish a robust air and cruise missile defense system and begin testing ballistic missile defenses on land and at sea at full design capability. Congress should provide additional funding for the deployment of a cruise missile defense system as a component of homeland defense. And the Pentagon should deploy air defense and cruise missile defense systems to defend major U.S. cities and critical infrastructure.

- **Priority #3: Enhance rear-area military operations to protect the homeland**

  and prepare for terrorist attacks. The U.S. military can assist Local, State, and Federal authorities in counterterrorism efforts by identifying critical infrastructure nodes; assessing their security levels; providing protection for them as needed as well as redundant communications, command, and control systems; and procuring and maintaining equipment to assist in the local responses to terrorist attacks. To achieve this goal, the commander in chief (CINC) for homeland defense should be the Joint Forces Command CINC. The Secretary of Defense should develop a refined list of military

responses to domestic terrorist attacks and a network of interactive command-and-control centers and service mobilization directorates to enable better coordination with Federal and State agencies. The service branches should provide training to the National Guard, FEMA, and other appropriate Federal and State agencies on Incident response and mitigation. And all components of the Joint Forces Command should be enabled to task units to respond to incidents around the Entire country.

- **Priority #4: Provide intelligence support for military operations.**

  Effective military operations depend on timely and accurate intelligence about enemy forces, movements, capabilities, and intentions. Real-time, all-source intelligence fusion centers are required for effective counterterrorism military operations and homeland defense. Several of the September 11 terrorists were on different government watch lists, but these databases were not linked for common retrieval of information. To protect the homeland, the U.S. Department of Defense should institute local, low-level counterintelligence source operations for force protection near military installations. To give DOD access to cross-referenced strategic and critical databases, which are currently housed in various Federal agencies, will require establishing fusion centers at the Federal, State, and Local levels (where necessary) and staffing them with personnel who have appropriate clearances for classified information.

- **Priority #5: Ensure clear command and control of overseas anti-terrorism**

  operations. Regardless of whether military operations are of an offensive or defensive nature, the geographic Unified Command (such as PACOM, or CENTCOM, which is directing the war in Afghanistan) must be the command- and-control headquarters for overseas military operations. In military parlance, this means that the geographic Unified Command will be the supported command and the war fighter. The United States Special Operations Command (SOCOM) should be the primary force provider (supporting commander in chief or CINC), not the major war fighter, and the specified supporting command for managing counterterrorism operations. The Secretary of Defense should ensure that SOCOM has the authority and resources it needs to carry out this mission. The CINC for homeland defense should prepare pre-planned force packages for initiating rapid responses to terrorism contingencies.

CONCLUSION

Finally, let me make a few brief observations that pertain to the entire report. First, it is our contention that terrorism can be combated and homeland security be protected without giving up any of the civil liberties guaranteed by the Constitution. While certain adjustments need to be made by the public, in the area of privileges and conveniences (such as air travel requirements, etc.), the basic protections of the Constitution must be guaranteed to United States citizens at all times, including time of war.

Second, it should be noted that the first responsibility for responding to terrorist attacks, and also a major role in the prevention of such incidents, must necessarily be carried out at the state and local level. It is local fire, police, and emergency medical services that will be the first responders to any terrorist incident. It is therefore critical that there be coordination at all levels of government—federal, state, and

local—to be sure that all governmental agencies work together. It is particularly important that adequate funding be made available to local governments so that the planning, coordination, equipment, training and exercises can be carried out by police, fire, and emergency medical services at that level, so that they will be thoroughly prepared for any contingency that may occur.

Third, it is also essential that intelligence be shared both horizontally among governmental agencies at the federal level and vertically between the federal government and state and local agencies. This sharing of intelligence must be a two-way street with information passing both ways.

Fourth, a critical area of activity in preventing terrorism involves improving control of our borders. This is a task that is primarily the responsibility of the federal government, although state and local governments also can cooperate in such an effort.

We believe that if the recommendations that I have described above are followed, and if there is effective cooperation and coordination among all levels of government, the United States can discharge its responsibility to keep our people safe and free.

Mr. SHAYS. Mr. Meese, thank you very much. And thank you for such a thorough statement in writing. You couldn't possibly cover it in 10 minutes, the four areas. The significant number of priorities you stated in each area are very helpful to the committee, and I have a feeling very helpful to Mr. Ridge's office as well. So I thank you for that.

First, let me just recognize the presence of a very active Member, Mr. Tierney from Massachusetts. We are going to start with Mr. Otter. If you wanted an opening statement, we will have you use the opening statement in the next panel, if you want to use an opening statement because we are somewhat under a time restraint with this panel. Mr. Otter.

Mr. OTTER. Thank you very much, Mr. Chairman. And I would like to start out with the Governor. I happened to be in the audience 2 weeks ago in Boise, Idaho, Governor, where you gave a very comforting speech. I will tell you that the thousand people in that room went out of there feeling like we truly did have the leadership at the State level, in many of the States, and it was a great source of comfort to most of those folks, because they hadn't had the opportunity obviously to hear a Governor speaking from a national level on the importance of our readiness and on the importance of this war against terrorism.

Your State was the first one, I should say was the State prior to September 11th that had witnessed—had been the victim of the worst terrorist attack on the United States prior to September 11th. And I know that you stated during your opening statement that there were several conditions that the Federal Government did not seem to be prepared for when they came to Oklahoma City to help you assuage the problems that were created by that terrorist attack.

I am also familiar that you did make many recommendations, or many recommendations were made as a result of that terrorist attack to the Federal Government. Could you briefly go through those for us and which ones the Federal Government did adopt and has not yet adopted that may have helped us greatly with the events of September 11th?

Mr. KEATING. Mr. Otter, after the April 19, 1995 tragedy in Oklahoma City, I had occasion to share my observations and experience with many different Federal agencies and individuals, and I think those suggestions and observations were placed in action plans and were in fact a part of the response suggested in the event of a national or man-made calamity.

The challenge, of course, is that you have a rescue and recovery mission on the one hand, and a criminal investigation on the other. In Oklahoma City, for example, with wind and with rain, with a building that could collapse at any minute and literally kill hundreds of additional people who were rescue workers in that building, the FBI was conducting a comprehensive criminal investigation and found the key, as a matter of fact, some blocks away to the rental truck that was responsible for taking the bomb to the site. So it was an extraordinary cooperative venture.

We could not prepare for such a thing. We did not because we never anticipated it. But because of rough weather in our section of the United States—some sections of the country have hurricanes

and some floods and some mud slides and some forest fires. We unfortunately have been plagued obviously by tornadoes in the central part of the United States. We had prepared for those kinds of scenarios, bringing together the hospitals and the rescue workers and the police and fire and the like where they did know what to do. And that was basically the response to the terrorism event. I think the suggestions we had about using the military, and having military assets quickly available, having FEMA come within 24 hours, and do the superb job, the excellent job that FEMA does do, all of those things that were suggested, all of those things that worked, I think worked in New York.

I can't think of anything—for example, providing perimeter security. That was something we suggested, not only to avoid looting, but we had 320 buildings damaged or destroyed. We had no act of looting at all. New York was slow in getting their perimeter established.

But the other things that we suggested were done. But what was not done was interoperable communications gear, because the people who come from out of State have their own systems and their own frequencies. Even the people within State. In the event of a massive—and, Mr. Otter, you are right. I think that if bad people continue to do bad things, we may have other events like September 11th. If you have a huge onslaught of professionals, firefighters, police officers, rescue workers, public health professionals, they had better be able to talk to each other, because they have to warn each other of what is ahead as well as suggest a response.

That is—that was, in my judgment, the biggest missing link in Oklahoma City, and the biggest missing link on September 11th, the fact that a lot of those people could not talk with one another.

Now, the FEMA teams are highly trained. The problem is, you want to make sure that all of our local law enforcement know what they are going to do, the local fire service, they are all trained together. They speak the same language regionally and nationally and, of course, locally. They identify the same problem. They respond, especially in a bioterrorist or radioactive challenge, in the same way. That is the thing that most concerns me, that we are not dealing with one bomb and one building that knocks down 320 other buildings, but perhaps a regional challenge, or a very large metropolitan challenge, to be able to have many other agencies together.

We do practice, as Mr. Meese has indicated, but we really need to make sure that we are practicing on a national scenario plan more than just simply our little local challenges.

Mr. OTTER. Thank you. My time is up. But I just want you to expand just a little bit on that because I see a potential for us here in citing and recognizing the common denominators in a terrorist attack that would be the same throughout the United States. But I also see some geographic discipline that is going to be needed, because there are—there is terminology, there are many situations. And I think Mr. Meese mentioned a couple of those with infrastructure, that are particularly unique to the West or perhaps to the Pacific Northwest, that we are going to need some regional geographic discipline as well, aren't we?

Mr. KEATING. Absolutely. In our planning process, State by State, that is the missing piece, to regionalize the response, because you have sometimes highly urban populations up against very rural borders. And you may have an event, let's say a fuel spill, I mean a train derailment, or in Oklahoma's case, for example, you have most of the pipelines in the United States go through that State. If you were to have an event there, you need to know are there people coming who have knowledge of how to respond to this, and is there a regional response able to come, not just simply local. That may actually be further away than a regional response.

Mr. OTTER. Mr. Meese, would you like to respond to that? I see you getting to the edge of your chair.

Mr. MEESE. No. That is fine.

Mr. OTTER. Thank you, Mr. Chairman.

Mr. SHAYS. Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Chairman. I want to thank the witnesses and say to Mr. Keating when I read your testimony about the importance of involving State and local responders, you know, you certainly have the experience on this. And I, by having been a mayor, I can tell you that I understand totally the points you are making, as well as addressing the issue in your statement of avoiding Federalizing local response.

I think that is a particularly important point for this government to keep in mind, because there are great constitutional implication there. And your speaking out on that, I think, is extremely important. And I want to let you know that I support that.

I would like to, for the moment, turn to the testimony that was provided by Attorney General Meese, and say that first of all the presentation that the Heritage Foundation's homeland security task force has come up with is quite comprehensive. I think that many of us in Congress would agree with most of it. You might understand not all of it, but most of it. And the—you know, it shows a well thought-out approach.

Mr. MEESE. Thank you.

Mr. KUCINICH. But there is one area in particular that I thought would be interesting to talk about, given our next witness. And that is, the section of military operations to combat terrorism.

Priority No. 2, protect U.S. borders and critical national infrastructure with air defense and missile defense. I would like to focus on that part of your testimony and ask you on what basis of a threat assessment do you conclude that the threats of an attack by cruise missiles and ballistic missiles requires that United States establish a robust air and cruise missile defense system and begin testing ballistic missile defenses on land and at sea, on full design capacity, and that Congress—and the—that the Congress should go ahead with providing additional funding and that the Pentagon should deploy these defense systems? Can you share with this committee the basis of that threat assessment?

Mr. MEESE. I would be happy to. As a matter of fact, there are a number of sources of this. One of the important aspects of this was the Rumsfeld Commission, which during the last administration looked into this at the behest of Congress, and found that there were—that there were a number of nations now that have ballistic missile capability, and that many of these nations also had

the capability for weapons of mass destruction, not only in the nuclear field, but also in the chemical and biological field, and that this was true, and there has been other studies since that time that verify this. It was true not only in terms of the importance of ballistic missile defense to protect the United States but also to protect the lands of our allies, such as the Republic of China and Taiwan and other places.

And so the ballistic missile defense I think has repeatedly come to the attention of both the public and the U.S. Government as a key part of our total homeland defense here, as well as the ability to carry out our international obligations.

Mr. KUCINICH. I thank the attorney general. The question, of course, was raised with respect to defense of this country. It is my understanding that the Rumsfeld Commission focused on speculation regarding a medium-range missile, known as Typo Dong that dealt with the capacities of North Korea.

I am going to have to be more specific, Mr. Attorney General, and ask you on what basis should the United States deploy a missile system to defend against long range, intercontinental ballistic missiles? What is the threat assessment?

Mr. MEESE. We have a number of countries that either have or are developing an intercontinental ballistic missile system. And——

Mr. KUCINICH. Which countries are those?

Mr. MEESE. Well, obviously the former countries of the Soviet Union, several of them have intercontinental ballistic capability. There is talk about Iraq developing a longer range ballistic missile capability, as well as in North Korea. So there are a number of countries.

There is also the possibility of this technology being seized by rogue elements of the military. This is particularly true in some of the countries of the former Soviet Union. So there are a number of threats. But the fact that this—we also have, of course, the potential in Iran. There are other countries as well.

The fact that this technology is being exchanged or could be exchanged between countries that have it at the present time, and those other countries that might use it to our disadvantage, indicates that we should be working on this at the present time.

The time that you need a ballistic missile capability or any defensive capability is not when the attack comes, and particularly with a complex system such as this. It takes many years of development in order to have it ready when the time comes that you need it. It is very similar to the research and development that went into other major advances in warfare such as the airplane, certain types of ships, nuclear submarines and the like. And so it is the time length that is involved in developing these that means that we should not be behind the curve.

Mr. KUCINICH. All right. Mr. Chairman, I would just like to submit for the record—I thank the gentleman. And I would say to the gentleman again, I appreciate the tremendous work that Heritage has done on this. The one area that I have great concern about is on the area of threats assessment, Mr. Chairman. I want to submit for the record this study of threat assessment done by the Carnegie Endowment for International Peace, which says actually that the trend on threats, threat assessment for intercontinental range bal-

listic missiles is down, that threats—intermediate range ballistic missiles down, the threats for nations with ballistic missile programs of concern, down. The potentially hostile nations with ballistic missile programs, down.

And I think it is important that as we get into these discussions that we try to use the most available information. Thank you.

Mr. MEESE. Mr. Chairman, if I might respond to that, because I read that report. And I noted that it was a very subjective report designed to—where the—even the charts there were designed to reach a certain conclusion that the authors had in mind, which was not borne out by the factual material that they even included in their report.

One of the things we have to recognize, that while indeed there may be fewer nations, only because of some of the international things that have occurred recently, the fact that the potential that those nations have, has increased considerably in recent years.

So I would say if you look at the whole report and the underlying data, it gives a very different picture than the conclusions that might be reached.

Mr. KUCINICH. Thank you very much, Attorney General. I would like to associate myself with your remarks with respect to the Rumsfeld Report.

Mr. SHAYS. Bottom line, this committee will be, at the request of the minority, holding a hearing on national missile defense, so we will probably get into more of that. It is only a small part of the overall picture here, but a legitimate question to ask our witnesses.

Mr. Keating, I am very interested in getting a sense of what kind of clearance problems you might have encountered or if you anticipate there are potential clearance problems. Let me just illustrate. We had police chiefs who basically came before us and said that—Mr. Meese, happy to have you respond to this as well—saying that they had personnel assigned to work with the FBI and other offices of the U.S. Government in which their officers had clearance, but the chief of police was not told what was going on, and he or she did not have clearance.

I am wondering if the same thing applies to Governors as well.

Mr. KEATING. Regrettably, yes. As a matter of fact, I had a similar incident. I appointed the adjutant general of Oklahoma, who served our people most capably after the Oklahoma City bombings. I am the commander in chief of National Guard of Oklahoma. Bob Ricks, who is our commissioner of the Department of Public Safety, former DEA general counsel, former deputy assistant director of the FBI, special agent in charge of the FBI during the Oklahoma City bombing, General Korite came to the two of us and said, well, I have got some information that I have to share, but I can't share it with the two of you because you are not cleared.

Well, I was his boss. And obviously Commissioner Ricks is the chair of our response and avoidance team. He needs to know. Well, I don't question the need for clearance. What I hope is that those clearances can be speedily provided to those public officials, like mayors, like Governors that have to take charge and respond to a national or man-made disaster, particularly those that require some degree of clearance.

There is a level of discomfort and embarrassment over this but it needs to be addressed and in our case it has been addressed. But still it's disquieting.

Mr. MEESE. I would certainly concur with the Governor. Both he and I, for example, had the highest security clearance you could get but when we served in the Justice Department I don't think it would be very hard for them to update those clearances rather quickly. I would suspect that in most cases the background investigations could be performed quickly on police chiefs, mayors and Governors. But I think it's absolutely critical that those people in the chain of command where there would be a response or the need to prevent a terrorist incident have the necessary clearances available so that no intelligence would be kept from them.

Mr. SHAYS. One of the untold stories, frankly, with the past administration continues today. This one is the number of security clearances that have not been done. Hundreds of thousands backlogged. So even the private sector that hires people that need clearances, they may be on the payroll for 9 months, say, at Sikorsky or United Technology, Pratt & Whitney and not be able to do the job they're paid to do because they don't have clearance. So it's a major problem.

We knew it was a problem with the chiefs of police. I am frankly very surprised to learn that it would be with the Governor and, obviously, mayors on occasion need it as well. So Governors, mayors, chiefs of police, anyone else that strikes you that we need to be looking at in terms of trying to encourage clearance?

Mr. KEATING. I think that would be obviously the centerpieces of an intelligent avoidance piece. Obviously we're not talking about response here. I don't think we have a problem in most—in most response incidents. But the problem is every State if they're doing it wisely, for that matter every city, you have to have the sharing of information between the Federal and the State and local authorities so that we can avoid another calamity like September 11th. If you can't share that information to put people on high alert, you obviously are taking the risk of having another similar incident. But I didn't want to admit to my wife that I wasn't cleared, but it was rather awkward and embarrassing during that period of time.

Mr. SHAYS. The amazing thing is as soon as you're elected as a Member of Congress you have automatic clearance. I think we will be able to address it fairly quickly.

Mr. MEESE. I think, Mr. Chairman, it's particularly relevant now because the Office of Homeland Security is, as you know, kind of refining their system of alerts. It was indicated only within the last 24 hours I believe the new system they've developed. And with that needs to come the information that underlies those particular alerts so the proper response and the proper protective measures can be taken. That necessarily implies the people like Governors, commissioners of public safety, mayors and chiefs of police in determining how to deploy their forces in response to the particular alerts.

Mr. SHAYS. State Attorney Generals as well.

Mr. MEESE. I would certainly think that the State Attorneys General. The people who have command responsibility for law en-

forcement and for emergency response, that would include directors of the State offices of emergency services, for example, others that might have a need to know. And that's been pretty well—the need to know concept has been pretty well established in the Federal Government. I think it could be extended today to State and local governments.

Mr. SHAYS. I think we've made it pretty clear. I think the record would show that. But, I mean, in this process of I think five gradations of alert—are there five? Right. Bottom line you could have a very serious warning and yet under present law I'm gathering the Governor might not be able to be told exactly whatever the basis is for this alert.

Mr. KEATING. As Attorney General Meese said, some attorneys general are strictly civil officers. Some don't have any command and control responsibilities. But others do have responsibility for law enforcement, Governor is commander in chief of the National Guard and/or responsibility, in my case, for law enforcement as well. I mean for me not to be able to take that alert and reassure the public or take that alert and take action to prevent an event in my State certainly appears reckless not to be able to do that because you're denied information.

As you know, we know from our own experience these clearances can be reasonably quickly obtained. They can be updated and there are gradations of clearance. All we're asking for is information which will protect us and provide us an opportunity to respond, which I don't think is too much to ask.

Mr. SHAYS. I have about 5 minutes more of questions. But I'm happy to follow you, Mr. Otter, if you like.

Mr. Tierney, any time you want the floor you can claim it.

Mr. TIERNEY. No, thank you. I'm all set.

Mr. OTTER. Yes, I have a couple that I would like to followup both with the Attorney General and with the Governor. First would be on the security clearance. As we establish a pro forma for security clearances and the type of information that we put out with that, then how do we govern the distribution of that? We were told, this very subcommittee was told when the Army Corps of Engineers, for instance, made an assessment of the vulnerability of all of the infrastructure, whether it was the dams or power corridors or pipelines, whatever it was, how vulnerable we were, anybody that wanted to tap into and go online could have figured out not only where we were the most vulnerable but in many cases where exactly a small device could be put within a nuclear plant in order to blow up the plant and create the greatest amount of damage.

So as we provide security for those that need it, security clearances for those that need it, how do we then govern the distribution of that information so that it doesn't get into the wrong hands?

Mr. MEESE. Well, this is always a problem with any information. And the need is to then, obviously concurrent with the clearances, provide necessary training to the people who have those clearances. My own experience, I found in the Federal Government you have hundreds, perhaps thousands of people that have security clearances of various types. And there's a discipline that goes with that in the departments. That same kind of discipline can be utilized and implemented by officials at the State and local level. I would

say since in the Federal Government there's much more classified information that goes through offices, that at the local level this will be more of a novelty and therefore I would suspect at the local level there would be even greater attention to the need to safeguard this kind of classified information.

Police departments every day have all kinds of information that requires a great deal of security about organized crime, about narcotics rings and so on. They seem to be able to handle this. I would say that they would be able to handle to this kind of information likewise.

Mr. OTTER. If I could get both of you to respond to this. Would the distribution of security knowledge include—go down as far as let's say—and I don't mean down, that's the wrong word to use—but would it include the county sheriffs? Would it include the 44 county sheriffs in Idaho?

Mr. KEATING. It really depends on the nature of the information, certainly rural California, as an example, that counties really provide the law enforcement. Municipalities do not have law enforcement. Those individuals are well trained and they are well educated and they certainly ought to be in a position, as the Attorney General said, on a need to know basis to provide assurance to the public and a response and avoidance piece to their law enforcement duties.

Congressman, we're struggling with this now in my State, I'm sure Idaho, perhaps Massachusetts and Connecticut are as well, you know, are you going to make terrorism a crime. What is terrorism? Is that a status crime? And then are you going to provide the public the information they need to know, the media the information they need to know or are you going to put a cloak over everything or in effect make everything secret or everything subject to exclusion from open records. We're struggling with that right now. The legislature is in session as we speak. We're attempting to find that proper balance. There are some who want to overdo and basically take everything out of the public circulation. Others would under-do and not provide very much protection at all.

So I mean we're trying to walk that very difficult straight and narrow.

But I think what's most important is to be able to have the FBI call the sheriff and say we have a problem. Here is what we're looking for. You need to go out there and help us man the line, if you will. Police sheriffs, State police and what have you. So that kind of information is crucially important.

Now, more arcane information, you know, should a sheriff have knowledge of the intricacies of a nuclear power plant or the intricacies of a pipeline? Perhaps not. I'm not sure that is particularly relevant. That information would perhaps not be helpful on the Internet and could be accessible, available to somebody who could do us harm. But law enforcement needs to know what is the threat. If you have a red threat or a green threat or yellow threat, whatever the threat may be, you need to be able to hand that off like a baton from Federal officer to State or local officer and say go get 'em. You have to have that seamless information. And those individuals need to have the access to the information. They need to have the security clearance to get it.

Mr. OTTER. Attorney General.

Mr. MEESE. I think it would depend in terms of sheriff. Reality would be is this principal the chief executive officer of a law enforcement agency. And this varies from State to State, even within States. In Virginia, for example, many sheriffs have complete law enforcement authority. Other sheriffs have only responsibility for detention in the service of court orders and they're county police departments. So I think the definition of the people that would need it are they are the chief executive officers of a law enforcement agency.

Mr. OTTER. The discussion that you had with the ranking member earlier made me think of the Idaho Constitution which of course is a duplicate, if you will, of the Federal Constitution. And actually the highest ranking Constitutional officer in the county is the sheriff and can only be arrested by one person and that happens to be the coroner.

I would just ask you to reflect on one more thing. One of the greatest advances or I guess I should say deterrents is disinformation. Is there any part of the dimension of our national security in which we're purposefully—we're contemplating giving out disinformation in terms of our security and in terms of our strategy for that security?

Mr. MEESE. Well, I guess if we were to say that there was would itself be self-defeating then for any such disinformation. But I know of no such effort on the part of the U.S. Government and certainly I think it would be wrong to provide disinformation to public officials who have a duty to carry out particular responsibilities. But I think that we have enough trouble in the government generally just getting the right information let alone disinformation.

Mr. OTTER. I would only conclude—Mr. Chairman, I thank you for the flexibility you have given me in time here. I would only conclude that our first line of defense for our communities are going to be the individuals within those communities. And to the extent that we can get the citizens of this country, 283 million citizen soldiers out there all prepared to defend themselves, their families and then their communities, it would probably bring a little more purpose to the mandate that we were given with Flight 93 and the folks that took the airplane down in Pennsylvania. And I would hope that we always make that a generous portion of any national policy that we have.

Mr. KEATING. May I say something along that line. I had the opportunity before I came here to speak to a large Red Cross gathering in Milwaukee. The point I made to them, and I would encourage the Congress as you look at funding State plans, in effect that's what your doing, to encourage that municipalities be a part of that, that they sit on that board. You can say cities of 100,000 and more have to have a representative, whatever the suggestion might be, but also the nonprofit community. Because the Red Cross, all these people they show up. If they have no knowledge, if they are potentially affected by a very serious physical challenge by showing up, by providing meals, by being there heroically as they do day by day, the Salvation Army as well, they need to know these things. They need to be a part of the mix in discussing a response, not particularly the response piece but they must—the health piece has to

consider the 501(c)(3) community as well because they're going to be there with most of the assets. They're going to be there timely. They're going to be the very first people off the boat, if you will, will be those 501(c)(3) folks. They need to be at the table to know what it is they can expect if they get involved.

Mr. SHAYS. Mr. Meese, I know you need to leave soon. Do you have 5 more minutes here? Let me say to you that I believe and I think a lot of other Members do as well that any disinformation program would be deadly because not only do public officials need the truth but our bosses do. If they're not told the truth, they're not going to be able to tell us the right things to do. And our bosses are being basically the general public. They need to know the truth to tell their elected officials what they want done. And so I just shudder when I think that there was any possibility of a disinformation program.

We know in the early 1950's President Eisenhower had to deal with a new assessment of a threat and develop a new strategy along with Congress. And he brought everybody into the White House and into the Sun Room and it began to be basically the solarium project in which we developed a new threat, our ally, now our enemy, wanting to overtake us politically, economically, militarily, and the cold war began.

We're kind of at that point right now. Where I am getting a little nervous is we basically have a very competent person—not basically we do—in the Governor but he is an appointee of the President not answerable to Congress. And that's a fact. But he is in charge of doing something we need to ask questions about. What is the threat, what is our strategy, and how do we deal with it. All three commissions Bremer, Hart-Rudman, and Gilmore Commission said know the threat, have a strategy and then deal with it.

I guess what I want to ask you do you think it's taking us too long to assess the threat. We've already started to take actions before we got the threat assessed. And who does Congress go to ask about these questions.

Mr. MEESE. Mr. Chairman, I think this is a very profound question that has Constitutional ramifications. I understand the reasons why a member of the White House staff, a member of the President's official family, is not—cannot—is not appropriate that they testify. I think there are, however, may be some way to reconcile this just as there is in matters relating to the budget where the Office of Management and Budget, which is also within the executive office of the President, the Director of OMB does in fact testify before Congress. And I think is a matter that might well be discussed with the President as to how to place someone, whether it's Governor Ridge or someone immediately as a spokesman for him that could testify to Congress.

The other alternative, of course, would be to invite Congress to the White House for briefings there. I think there's no question in my mind that it's important that the Office of Homeland Security share information with the Congress so that the Congress, as the very direct representatives of the people, can know what's going on and obviously can deal with matters such as the budget, legislation, which are their piece of responsibility in terms of homeland security.

I think that—so I think that this is a soluble problem that should probably be raised with the White House to see what kind of a solution can be gained. I know during the time I served in the White House there were many occasions where it was necessary to give information to the Congress such as in the Operation Grenada, which was a very sensitive operation where Members of Congress were brought to the White House so that information could be given to them. So I think there are ways of solving this. I agree with the chairman that kind of two-way communication is very necessary.

Mr. SHAYS. Thank you. Mr. Keating, any comment? Governor, I'm sorry.

Mr. KEATING. I think the most information is the better. You all determine where the money is spent and how it is spent. And to have a dialog, a conversation between the executive and legislative branches I think is essential in order to be able to be truly prepared as a people. So I would certainly agree with what the Attorney General said.

Mr. SHAYS. Thank you. You both are excellent public servants. You serve our country well, continue to do. We appreciate you honoring our committee with our presence. And thank you very much.

We'll go to the next panel. Our next panel is comprised of four individuals. Ambassador L. Paul Bremer, who is Chief Executive Officer of the Marsh Crisis Consulting Co. He was chairman of the National Commission on Terrorism and co-chairman of the Heritage Foundation Report, Defending the American Homeland.

Mr. Randall J. Larsen is the Director of ANSER Institute for Homeland Security and previously a colonel in the U.S. Air Force. Colonel Larsen has been a frequent guest on Larry King, discussing counterterrorism issues, and other shows as well.

We also have Mr. Joseph Cirincione, who is the Director of the Nonproliferation Project of the Carnegie Endowment for International Peace and a frequent contributor to newspaper opinion editorial sections.

And Mr. Henry L. Hinton is the Managing Director of the Defense Capabilities and Management Office, General Accounting Office and has appeared before the subcommittee on numerous occasions.

Mr. Hinton, we're going to swear in some of the other people as well, but is there anyone else who needs to be by your side?

Mr. HINTON. No, sir.

Mr. SHAYS. Let me ask to you stand. Let me swear you in and we'll begin with the testimony.

[Witnesses sworn.]

Mr. SHAYS. Thank you. I appreciate this panel listening to the first panel. Some of the questions and comments of the first panel you may want to make mention of in your statements. We are fortunate to have a co-chairman on both panels, so we appreciate that, and appreciate all of you being here.

Ambassador Bremer, I give you special deference because you were a former resident of New Canaan, Connecticut, and also I might say the first Ambassador on Terrorism for the State Department. Sadly that wasn't continued, was it?

Mr. BREMER. Actually I was the Ambassador for Counterterrorism.

Mr. SHAYS. Counterterrorism, not terrorism. Excuse me. You always make me speechless. When you speak, would you use your mic.

Mr. BREMER. Sorry.

Mr. SHAYS. Go for it.

STATEMENTS OF AMBASSADOR L. PAUL BREMER III, CHAIRMAN, NATIONAL COMMISSION ON TERRORISM, MARSH CRISIS CONSULTING; RANDALL J. LARSEN, DIRECTOR, ANSER INSTITUTE FOR HOMELAND SECURITY; JOSEPH CIRINCIONE, DIRECTOR, NONPROLIFERATION PROJECT, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE; AND HENRY L. HINTON, MANAGING DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, GENERAL ACCOUNTING OFFICE

Mr. BREMER. Thank you, Mr. Chairman, for the opportunity to be here. You mentioned a very important point in your last comment to the Attorney General, which is that we are at a flex point in American national security policy, very similar to the position we were in in the period 1945 to 1947, when we had to find a new organizing principle for American foreign policy.

In those days, as you pointed out, the organizing principle was to defeat and to contain and eventually defeat Soviet communism. That's a fight that took 50 years. The President has in his speech September 20th, in his State of the Union Address and in his statement yesterday in the White House made clear we're in a similar position now and that the new threat now is terrorism.

And it's there for basically two reasons: One, because we're facing a new kind of terrorism where terrorists have moved away from a restraint in the number of people they kill to mass casualty terrorism most recently on September 11th and, second, because of the America's geopolitical situation. We dominate the world as no Nation in recorded history has dominated the world. This creates opportunities but also obviously creates resentments against America.

The lesson of the Gulf War was that America is essentially not defeatable by conventional weapons. So people who resent and hate us are forced to consider moving to unconventional or asymmetric warfare using weapons of mass destruction or using terrorism. That is why we are faced in fact with a different situation today than we were on September 10th.

And as the President correctly identified in his State of the Union address, we face a nexus, a nexus between terrorist groups who wish us ill, between States which support terrorism, and between States which have access to weapons of mass destruction. And in most cases, also weapons that have access to ballistic missile technology which poses a particular threat to our country, as the Attorney General pointed out.

Now, this leaves us with a multi-faceted challenge. We've got to have new thinking across the board. We need to be able to change the culture of the way certain parts of our bureaucracy think, the FBI, the CIA. We need to have new means of communications be-

tween the Federal, State and local officials, as the Heritage Foundation study which I co-chaired showed, and we're going to have to understand there are no quick fixes. This is going to be a very long struggle.

I think the most important message that the President has given, which I support fully is that we have to change our entire strategy. Mr. Chairman, in the last decade our strategy was basically to wait for terrorists to attack and then to respond. Wait and respond. The stakes are now so high that we have to shift to a strategy which I call detect and prevent. The President said yesterday in the Rose Garden there are no margins for errors, there is no chance to learn from our mistakes. And he is absolutely right. The stakes are simply too high to get it wrong. We have to move from an emphasis on deterrence to an emphasis on prevention. We have to do things differently.

For example, in the Heritage Foundation we should be getting aircraft manifests before a plane takes off, not after it takes off. We need longer notice before cargo ships and cargos arrive at our ports. I'm glad to see that Congress is in the process of making that recommendation come into effect.

Everyone needs to be involved in protecting the homeland, Federal, State and local officials as we said, the private sector and, as Governor Keating pointed out as well, nonprofit sector.

The public itself needs to be involved. I was pleased to see that one of the recommendations of the Gilmore commission on which I served is being put into effect with the establishment of a domestic alerting system similar to the military DEFCON system, Defense Condition system, one of our major recommendations. Homeland defense does not begin at the border and it doesn't end at the border. As the Attorney General pointed out, we need to be concerned about how visas are issued. I'm pleased to see that the Congress is in the process of encouraging the establishment of a single lookout system, lookout data base so that everybody involved in border security can be looking at the same system.

And, of course, we've had the establishment of the Office of Homeland Security under Governor Ridge. I have, as you know, Mr. Chairman, supported the establishment of the office and believe Governor Ridge is doing a heroic job trying to get his hands around the multi-headed, hydra-headed bureaucracy.

I think it's only fair to point out that all of the commissions which you cited at the beginning, Mr. Chairman, also noted that Congress is not well organized on counterterrorism. There are some two dozen committees up here, that's before September 11th, I hate to think how many there are now, which assert some jurisdiction in one form or another. I'm pleased that the Speaker in this Chamber has at least established a Subcommittee on Counterterrorism to the House Intelligence Committee, which is at least a first step in trying to pull together this Chamber's approach to terrorism. But as you rightly criticize the Federal Government's lack of organization, from time to time I think Congress should look in the mirror as well. Congress is not very well-organized either.

I think the most urgent thing that I would like to focus on today, and I'll be very brief, is to counter the threat of biological terrorism. It is important to get a nationwide health surveillance system

in place. Again, steps are being taken in that direction. It's very, very important to accelerate research for drugs and vaccines against bioterrorism.

Now that the human genome sequence is available on the Internet, the nightmare is that some microbiologist somewhere will create a virus we've never heard of for which there are no vaccines.

I'm pleased to say that the National Academy of Sciences has established a commission that is looking urgently at how the scientific community in the United States can be brought to bear on the problem of focusing research on these biological-chemical-radiological threats. I'm serving on that commission. We hope to have a report to Congress and the President in the next couple of months.

This is going to be a long and difficult fight and every American life will be touched in some way by the battle. As the President said yesterday, there are more dangers and more sacrifices lie ahead. And he is surely right.

Thank you.

Mr. SHAYS. You were right, you were very mercifully brief but very precise. Mr. Larsen.

Mr. LARSEN. Thank you, sir. I'll be quick. Several things I want to discuss. First of all, I agree with Ambassador Bremer on many things he said. He's also been studying this for a long time. I've been looking at it since 1994, the idea of new thinking and new cultures as he mentioned.

I was asked to talk about how we've done in the first 6 months. I think Governor Ridge's office has done a marvelous job in his top priorities of training and equipping first responders. Bio defense, I agree with the Ambassador, I've been studying that for many years. Bio threat concerns me more than any other that we could face from external threats. Protecting our borders, information sharing, which was discussed earlier, is incredibly important, and the alert and warning system which will be announced today.

However, if we could have that first slide up there, please. The executive order that was signed by the President on the 8th of October creating Governor Ridge's office, I think this is some of the cold war thinking that we're going to have to progress beyond. This is exactly what we needed on 8th of October. We did not know what attack was going to come on the 9th of October, whether it was going to be larger and far worse. We needed something to unite us to work together on. If you take the word "prevent" out of there, it looks like a framework that would be used by FEMA to respond to a natural disaster.

One of the things we have to understand is when Hurricane Andrew hit Miami it was no smarter from Hurricane Hugo's experience in Charleston. The thinking enemies we are dealing with are smarter now once they have seen our reaction to the anthrax attack on the Hart Building and how slow we were to respond.

This is not the framework we need for the long term to build a national strategy that you talked about so often, Mr. Chairman. This is a great tactical and operational strategy.

If I could have the next slide. This is a concept we've been working on since about 1999, when we first developed this at the National War College to look at. We began with deterrence over there.

You sat here during the Dark Winter exercise when we were here in July. Deterrence, prevention, and preemption are the most important things and we talked about that. You'll see that Governor Ridge has virtually no—on my next slide you'll see that he has no real coverage of that.

Deterrence is far more difficult than during the cold war. Deterrence is either based on punishment or denial. In the cold war it was all punishment because we knew civil defense was pretty much a placebo that didn't work. Now deterrence is much more based on denial. So we talk about public health infrastructure and consequence management, yes, that's going to save lives but it also may help us deter it.

Prevention are defensive things, everything from aerospace defense, maritime defense, border controls. When I showed this to former Speaker of the House Tom Foley, he said in prevention you should include a Marshall like program for those parts of the world that tend to breed terrorism.

Preemption used to be something that was a four-letter word in the cold war because it was tied to the first use of nuclear weapons. Something we wouldn't do. I think we need to rethink preemption quite a bit. When we have seen what small actors could do to our Nation, unfortunately there's a fine line between preemption and aggression. So it's something we have to look at carefully, but I think it's something we need to consider.

Crisis and consequence management, that's FBI, lead Federal agency, consequence management FEMA, I'll jump over those. Attribution is an important element in this strategic cycle. We still don't know, the FBI Director last week said he doesn't know if it was a domestic or international source that sent that letter to Senator Daschle's office and the other letter. Until we can do the scientific work we need to help us with attribution for biological or cyber attacks and even nuclear attacks, we have very little chance of an effective response and re-establishing deterrence.

Now who's in charge of attribution? Clearly the FBI. Their budget last year was $3 billion. They don't have the science capability that our national laboratories do, civilian and DOD. That is the linchpin to this entire cycle. Once we figure out who did this attack to us when it happens, then we can properly respond. I use the respond there because if it's domestic we'll prosecute. If it's an attack from an external power we'll retaliate, as we did in Afghanistan.

That's not for revenge, that's for two purposes: One to eliminate the capability to cause further harm, and No. 2, to reestablish deterrence.

Now if you'll just go quickly to the next slide. The shaded area up there on the left, that is a busy slide, but just look at the shaded area. It's kind of hard to see up there. But you'll see Governor Ridge's responsibilities are for crisis management and consequence management, one little segment in prevention. That executive order, all it defines prevention as is preventing bad things and bad people from crossing borders. Prevention to me is much larger than that. I brief this concept to senior people in Governor Ridge's office, DOD CIA, a lot of folks up here on the Hill. They seem to like this idea of a strategic cycle. I think it's something you

should consider when we talk about building a national strategy, a threat assessment of what we look at.

Just two more quick slides here to show how complex this is. People ask me how is Governor Ridge doing. I say well, first of all, you have to understand he has the most complex challenge any Federal official has had. You take those 7 mission areas, you lay them across the top of that, then the down left side the most likely threats we're going to face. If you look at who the Federal Government is responsible for chemical consequence management, a total group of people that are completely different than cyber prevention. Who is in charge of all that? But this is a rather simplistic chart. If you go to the last, this is what it really looks like. Because you got to put Federal, State, local and the private organizations in there. That is the job we have given Governor Ridge. I'm not sure he has all the authority to do it that he needs. And particularly I think there should be one Federal official in charge of that entire strategic cycle.

The next thing I want to mention, I'll sum up quickly here, a lot of money is being spent on training. I think that's very important that we do that. I haven't seen many proposals yet for education. In many respects, Mr. Chairman, I think we're sitting right here similar to where we were in 1952 and with regard to the cold war.

In 1952 Herman Kahn hadn't started writing, Henry Kissinger hadn't started writing. There was no discipline known as national security studies at our great institutions. We need to develop an academic discipline called homeland security studies. So, yes, let's spend the money to train the first responders, but I'm talking about educating people from the State legislature level on up that are going to have to make decisions not just in crisis but do I fund a new sewer system or do I do something that is going to have to do with homeland security.

I think that's very important. I see Senator Frist mentioned that in his speech yesterday down in Florida. He said people are more important than technology in this, as General Schwarzkopf said after the Gulf War.

I have a few more comments, but I'll end them there because I'm over my time.

[The prepared statement of Mr. Larsen follows:]

Prepared Statement

House Committee on Government Reform

Subcommittee on National Security, Veterans Affairs, and International Relations

Colonel Randall J. Larsen (USAF, Ret.)

Director, ANSER Institute for Homeland Security

March 12, 2002

Introduction

Thank you, Mr. Chairman, for the privilege and opportunity to testify before the Committee. Americans face grave threats to our homeland both today and for decades into the future. Biological, nuclear, radiological, cyber, chemical, and even enhanced conventional weapons could be employed by our enemies against a wide range of targets. While there is a long list of potential weapons and targets, my greatest fear from an external threat is a large-scale attack with a contagious pathogen on one or more cities. On the other hand, the threat I fear most from a domestic source is uncontrolled spending--government spending that is neither guided by a detailed threat assessment nor a national strategy.

The 9-11 terrorist attacks and the subsequent anthrax-laced letters confronted the nation with urgent threats to the homeland. We have had to meet these immediate, short-term threats while developing the concepts, policies, strategies, and institutions that will produce homeland security for the long-term. To do both simultaneously is both difficult and necessary.

The Bush administration has met the initial homeland security challenge. I support the vast majority of immediate and short-term programs that have been introduced during the past six months. Because of my particular interests in the biological threat, I must say I am pleased with the

leadership and actions of many within the public health community such as Dr. D.A. Henderson and Mr. Jerry Hauer from Health and Human Services, Dr. Anthony Fauci from the National Institute of Health, and Dr. Robert Kadlec from the Office of Homeland Security. Our nation is indeed fortunate to have such leaders during time of crisis.

However, our focus at the ANSER Institute for Homeland Security is on the long-range challenges, including strategies, policies and the organization of America's national security institutions. While this will require a sustained effort that encompasses all levels of government and the private sector, we must understand that only the Federal government can lead this effort.

Purpose

The first step required to ensure long-term security of our homeland is a detailed and integrated threat assessment. I know that the committee Chairman has long been a leading proponent of this idea, and will therefore waste no words herein, other than to say I fully endorse and support the Chairman's recommendation.

Therefore, my testimony focuses on two important dimensions of developing homeland security for the long-term: a strategic framework for analysis which will facilitate both strategy development and resource allocation, and the requirement for an extensive executive education program in addition to the various training programs currently available for first responders. Finally, I offer one specific recommendation for a research and development program that could provide this nation with the best hope for effective defense against large-scale biological attacks in the 21st century: preclinical detection.

Recommended Framework

A strategic framework for analysis is required to develop a national strategy and determine proper resource allocations. On October 8, 2001, the Bush administration issued Executive Order 13228 which outlined six homeland security missions: detect, prepare, prevent, protect, respond, and recover. This operational framework was appropriate for the initial and immediate actions required in early October 2001. No one knew whether the next attack would happen tomorrow, and if it would be more deadly and more wide-spread than those of 9-11. We do not know this even today;

consequently, much of Governor Ridge's attention must remain focused on the immediate and near-term. However, this framework is not sufficient for developing a strategic approach to homeland security. Therefore, I recommend the following framework that is the product of eight years study of homeland security.

My study of the biological threat to the American homeland began while serving as a National Defense Research Fellow at the Mathew B. Ridgway Center for Strategic and International Studies in 1994. Several years later, while serving as the Chairman, Department of Military Strategy and Operations, at the National War College, I developed a strategic framework for the study of homeland security. Assisting in this effort was Colonel Dave McIntyre, the Dean of Academics at the National War College, and Dr. Ruth David, the former Deputy Director for Science and Technology at the Central Intelligence Agency. Today, Dr. McIntyre serves as my deputy, Dr. David is the President and Chief Executive Officer of ANSER (a nonprofit, public-service research institute), and this strategic framework is the intellectual foundation of the Institute for Homeland Security. It contains seven elements: deterrence, prevention, preemption, crisis management, consequence management, attribution, and response.

The differences between the framework identified in Executive Order 13228 and the framework recommended in this statement are more than just semantics. Deterrence, preemption, and response must be critical elements of our nation's homeland security posture and declared strategy. It is imperative that we think of homeland security as an integrated cycle instead of as a set of discrete, unrelated missions. This is the framework that can best ensure the proper development of long-range strategies, policies, resource allocations and reorganization efforts. Integration and coordination would be far simpler if all Federal agencies adopted this framework.

Deterrence must be a central element of any homeland security strategy. Our nation must have the policies and posture that deters our enemies from attacking our homeland. Deterrence is based on two elements: punishment and denial. The increased threat from non-state actors who might employ nuclear, chemical, cyber, or biological weapons demands a shift in how we practice deterrence. Throughout the Cold War, nuclear deterrence was based on mutual assured destruction—the ability to deliver incalculable punishment under any circumstances. Given the nature of homeland security threats, we must increase our ability to deter enemies by denying them the effects they seek. This will be done through methods, institutions, and programs that have not been considered elements of deterrence—for example, the public health system as a deterrent to biological terrorism. Resource allocations should reflect this new reality.

There will likely be times when our deterrent efforts fail, perhaps if only for the fact that our enemies might be undeterrable. In those cases, our nation will have to rely on its prevention capabilities. **Prevention** incorporates a wide group of active and passive measures that mitigate or even stop an attack or its effects; all of these activities are principally defensive. Our nation's prevention activities include border controls, aerospace, maritime and land defenses, arms control

treaties, and many law enforcement measures. It might even include political and military aid to address some of the conditions that give rise to terrorist organizations.

Our nation must also possess the capabilities, and associated policies, that allow us to preempt attacks on our homeland. **Preemption** is a policy that is fraught with political and military risks. In the Cold War, preemption would have meant the first use of nuclear weapons, possibly resulting in a global nuclear war. Further, aggressors have cloaked their initiation of war with claims that they were only preempting an attack on their homeland. However, preemption in the homeland security context does not have to call for the initiation of nuclear war or occupation of another nation's territory. It will require the selective use of military force and law enforcement, in concert with our allies, to preempt terrorists before they can carry out attacks. Preemption options can span the range from a JDAM delivered by a B-2 bomber to an arrest by U.S. law enforcement officials working with allies. This is a capability our nation must possess.

Crisis management is the investigation and law enforcement response to attacks on the homeland. The lead federal agency is the Federal Bureau of Investigation. However, many other state, local, and even private-sector actors have important crisis management roles to play, as evidenced by the September 11th attacks. Undoubtedly, Mayor Rudy Giuliani was the single most important crisis manager on that day. His leadership and courage calmed a city and a nation while focusing our efforts on the tasks at hand. Successful crisis management requires increased coordination and information exchange among all levels of government. We must move from the Cold War paradigm of "need to know" to the 21st century requirement of "need to share."

Consequence management is the effort to mitigate the consequences of attacks on the homeland. This includes a wide range of activities, carried out by Federal, state, and local governments, as well as the private sector. The Federal Emergency Management Agency serves as the lead federal agency due to its established role in natural disasters. Biological and cyber attacks blur the distinction between crisis and consequence management because they are the only two types of weapons that self-replicate. Furthermore, they recognize no domestic or international boundaries. The consequence management mission is a largely local event, led by local officials with Federal support when requested. However, biological and major cyber attacks are different and will require Federal leadership as demonstrated in the DARK WINTER exercise.

Attribution occupies an important place in the homeland security strategic cycle. Our nation's enemies are likely to disguise their identity, either because of they are non-state actors like Al Qaeda or because they employ especially heinous weapons. We witnessed the problem of attribution throughout the 1990's in a series of terrorist attacks, as well as last year with the anthrax letters. Improving our nation's attribution capabilities will demand greater scientific methods and technologies, as well as greater integration of the relevant law enforcement and intelligence efforts. The importance of attribution will continue to grow throughout the 21st century as non-state actors, even individuals, increase their potential to cause catastrophic destruction and disruption. Nothing is more important than removing the anonymity that provides security for terrorists. Prior to the recent anthrax attacks, the FBI had virtually no forensic capabilities for investigating biological attacks. Robust attribution capabilities will require a major research and development effort coupled with the full integration of the resources in Justice Department, the Intelligence Community, and the

Department of Defense. This does not exist today. Without attribution, there can be no response.

Response has two goals in the homeland security strategic cycle. The first is to eliminate the current threat, and the possibility of future attacks by that specific actor. This might be achieved through the arrest and prosecution of the terrorists or other coercive actions, such as the use of military force or covert actions. Certainly, the nature of the response would depend on a range of factors, not the least being whether the attacker is a domestic or international actor. The Bush administration's actions after 9-11 illustrate the potential range of response options. Secondly, the ultimate goal of any response must be the reestablishment of deterrence. If the purpose of war is to establish a better peace, then the peace we seek is deterrence.

The Advantages of an Integrated Strategy

Our nation's homeland security in the 21st century will depend on the capacity to perform all the missions of this strategic cycle. We cannot afford to prepare for these missions once a threat is imminent. Further, it is only through the integration and coordination of the efforts across these missions that our nation can gain the greatest benefits from all of these homeland security efforts.

Regarding bioterrorism, it is important to understand that public health has both consequence management *and* deterrent functions. Deterrence through denial was not a practical policy for coping with the nuclear threat during the Cold War. In the Cold War, nuclear deterrence was based almost entirely on the threat of overwhelming nuclear retaliation. Today, attribution difficulties will make it difficult to punish those who perpetrate a biological attack. We must understand that improved mitigation capabilities, or denial of intended consequences, offers significant deterrent opportunities. Managing the consequences of a biological attack is a national imperative.

Allow me to illustrate this important point. As some of you know, the ANSER Institute for Homeland Security was one of the co-sponsors of the DARK WINTER exercise that simulated a terrorist smallpox attack on the United States. The exercise revealed the challenges that biological terrorism presents for our nation. In my view, DARK WINTER's most important lesson is that the consequences of an attack are so horrific that we must focus on deterrence, first and foremost. Again, a key element of that deterrence is denial of the enemy's goals. Thus, deterrence must play a central role in any bio-terrorism or homeland security strategy. For biological terrorism, the most effective deterrent may very well be a robust public health system that includes early detection; new vaccines, antibiotics, and anti-viral drugs; and training, education and realistic exercises.

The Threat of Uncontrolled Spending

Currently, our nation's homeland security posture represents the "stovepipes" between the different governmental and private sector institutions that have homeland security responsibilities. This must be overcome so that each element of the homeland security community understands its role in the big picture. The homeland security strategic framework is the foundation for the development

of long-term strategy, policy, and resource allocation.

The success of these efforts will depend, in large part, on how resources are allocated across the homeland security missions and various programs. Defending our homeland will require enormous expenditures. However, we must not spend ourselves into bankruptcy. Increased funding for programs that reinforce the existing stovepipes between institutions will have limited value for our nation. Without a single integrated national homeland security strategy, we are likely to spend our limited resources in a highly inefficient and therefore ineffective manner. *At some point, the threat of uncontrolled, uncoordinated spending could very well become as much of a threat to our security as the weapons of our enemies.*

Developing homeland security for the long-term will require allocating resources across the missions and funding programs that facilitate cooperation across the homeland security institutions. This must be achieved, of course, in the most reasoned manner possible. When President Dwight D. Eisenhower formulated his Cold War national security strategy, he decided that "the basic objective of our national security policies: maintaining the security of the United States *and* the vitality of its fundamental values and institutions." We would do well to follow this advice when formulating a long-term approach for homeland security.

Role of Education

Additionally, long-term homeland security will require increased exchange of ideas between the institutions and professions that have homeland security responsibilities. Homeland security encompasses a broad group of professions, many of which have little familiarity or experience working with the others. They lack a common method, terminology, perspective, culture, or objective. As we have witnessed countless times, these present an unnecessary obstacle to cooperation and effectiveness. They prevent our nation from getting the full benefits from our homeland security efforts.

The most effective way to address this problem is to develop educational programs for senior leaders with homeland security responsibilities. These programs would expand their understanding of the scope of homeland security and place their role in a larger context. Such programs would build upon, not supplant, their own professional training and education. Workshops and exercises have already demonstrated their value in exchanging ideas across the homeland security community. Our nation has an established system for educating national security professionals from "first responders" (soldiers, sailors, airmen and Marines) to national leaders. A similar educational system for homeland security professionals would provide great value to the nation for the long term.

Preclinical Detection

Finally, I would like to propose an idea that should receive immediate and long-term funding for research and development. Virtually all biowarfare experts agree that early detection is the key to successful mitigation. Various public and private organizations are busy "selling" technological solutions. Most efforts focus on either environmental sampling or rapid diagnosis of symptoms.

While environmental sampling may be of use in protecting key facilities or top government officials, it is not a realistic approach to protecting America's cities. Likewise, awaiting the onset of symptoms and relying on rapid diagnosis and response of medical and public health officials gives significant advantage to the attacker. It is the area between these two events--the incubation period of a pathogen--particularly a contagious pathogen that provides us with the greatest opportunity for successful mitigation.

For instance, smallpox has an incubation period of 7-21 days, averaging 12-14 days. With current technology, an attack would not be discovered for at least a week, probably longer. There is no current test available that can determine if an individual has been exposed to smallpox or any other pathogen. (Nasal swabs can be used if we know there has been attack; however, even this does not provide proof that the pathogen has entered the body in sufficient quantity to cause the disease.) With current technology, pathogens remain undetectable after entering the body until symptoms appear. However, some in the scientific community believe that preclinical detection (also called post-exposure, pre-symptomatic detection) is possible. Similar to the breathalyzer test we currently give suspected "drunken drivers", we could sample certain groups that routinely move through our major cities, such as postal workers, police officers, airport screeners, or taxi drivers.

This sampling would provide a cost-effective and operationally feasible system that could provide early warning. An additional benefit to this system would be to determine who should receive treatment, ranging from antibiotics, to antiviral drugs or vaccines (in the case of smallpox). In the recent anthrax attack, close to 32,000 individuals received antibiotic treatment, but it is quite possible that no more than a few hundred were actually exposed. This system would be highly effective in allowing officials to manage scarce resources and in dealing with the "worried well."

The system required for preclinical detection could use one promising technology under development, called the "Zebra chip." It will primarily be funded by the private sector to identify common diseases. The Federal government should partner with the private sector to fund the

research on identification of those diseases that the commercial sector is not likely to fund themselves, such as smallpox, anthrax, tularemia and other likely bioweapons. The second key to this system requires a breakthrough in the science of preclinical detection. This would not only be a significant achievement for the war against bioterrorism, but also in the war against naturally occurring diseases. Early detection is critical for both man-made and naturally occurring diseases.

I am neither a microbiologist nor a public health officer. But as a national security strategist who has studied the threat of biological warfare for many years, I know of no other technology that offers more potential promise to both mitigate and deter biological attacks on the American homeland.

Summary

My testimony has focused on three important elements of long-term homeland security: a strategic framework, education, and a specific area of research and development that could offer great promise. None of these three recommendations offers quick fixes. It will likely take years for us to develop the concepts, policies, strategies, institutions, and technologies to meet the homeland security threats of the 21st century. We should recall our experience in the early days of World War II. When America was attacked in 1941, we had no central intelligence organization, no Joint Chiefs of Staff, no Chairman of the Joint Chiefs of Staff, no Joint Staff, no Department of Defense, no Secretary of Defense, and no National Security Council. Furthermore, many of the technologies that helped us win that war did not exist in 1941.

Today we are in a similar situation. The best way to ensure success in this war will be to build upon a proper foundation, such as the strategic framework for homeland security discussed in this statement. We must educate a new generation of national leaders in the study of homeland security--just as we did during the Cold War--when the academic discipline of national security studies was created. Finally, we must utilize our technological edge to keep us ahead of terrorists and others who would do us harm.

I am confident that we can meet these new challenges, just as we did in World War II and the Cold War. This concludes my prepared remarks.

Executive Order 13228:
Homeland Security Framework

Detect

Prepare

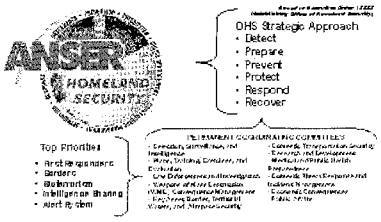
Prevent

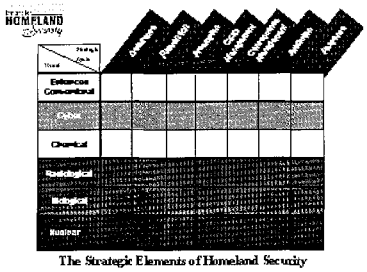
Protect

Respond

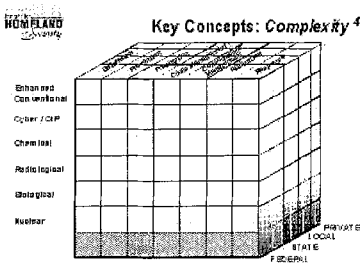
Recover

Office of Homeland Security Priorities





The Strategic Elements of Homeland Security



The Strategic Dimensions of Homeland Security

Mr. SHAYS. Mr. Cirincione.

Mr. CIRINCIONE. Thank you very much, Congressman. It's a pleasure to testify here today.

I spent 10 years in the professional staff of the House Armed Services Committee and this committee. From 1991 to 1994 I served on this subcommittee. It's easier being on the other side, I'll tell you that right now.

I am Director of the Nonproliferation Project at the Carnegie Endowment, and as such I was the author of the study that was referred to in the previous panel.

Some may have interpreted Mr. Meese's remarks to indicate that he had some question about the integrity of that analysis. I had the opportunity to speak with him just as he left and he assured me that was not his intent.

I did develop an analysis that indicates that the ballistic missile threat to the United States is actually decreasing. I invite comment and improvements on that analysis.

What I'm here to talk about today is the way we've been doing our national threat assessments. It's my belief that part of the reason the United States was so unprepared for the attacks of September 11th is that for the past few years the way our political process has handled the national threat assessments it's been given has consistently pointed us in the wrong direction. In part, this is a result of some of the partisan political warfare that was so prevalent in Washington over the past few years.

As examples of this I can point to the two studies that are most widely known as independent threat assessments. Those were both chaired by Donald Rumsfeld as it turns out. The first was the report of the commission to assess the ballistic missile threat to the United States which warned that the United States faced a threat by missiles that could be fielded by a hostile State with little or no warning.

In January 2001, the report of the commission to assess U.S. national security, space management and organization warned just as ominously that we faced a Pearl Harbor in space unless we immediately deployed a new generation of sensors, satellites and weapons.

Together these reports fortified a particular national security vision favored by some conservatives and heavily influenced the political debate of threat assessments and budgetary priorities.

Now we've all made mistakes in the past. Let me start by acknowledging our mistakes; that is, proliferation experts. We have made serious mistakes over the past few years. As a person who spends most of his professional career tracking the spread of nuclear, chemical, and biological weapons I think we have overemphasized this danger. That is, we thought the main danger to the United States was going to come by people developing the kinds of weapons that we did during the cold war. And we overlooked the kinds of attacks that occurred on September 11th. These terrorists didn't study physics or biology. They studied flight manuals. They stole what they needed and they turned our own technological marvels against us.

Similarly, whoever perpetrated the October anthrax attacks didn't do the kind of biological attack we thought we would experi-

ence. They either didn't know or didn't care that a sophisticated dispersal mechanism was needed to maximize casualties. They did a cheap but extremely effective biological attack that we were frankly unprepared for.

As a Nation, as experts, we have to redefine what we mean by mass destruction. I would say we now have to expand that definition of weapons of mass destruction to include the kinds of attacks in our critical infrastructure that we experienced on September 11th. We have to reassess our assessments. Are we getting the kind of national threat assessments that we need to get and we have to reorient. I strongly agree with Chairman Shays' comment that short-sighted attachments to the status quo only increase the likelihood and lethality of the next attack.

Very often we have gotten the warnings but we have ignored them. And some of the gentlemen that are here today have been making those warnings. As I point out in my written testimony, we were repeatedly warned that we faced a danger, an imminent danger of a terrorist attack.

One of the people that I spend a lot of time paying attention to is the head of the Defense Intelligence Agency, Vice Admiral Thomas Wilson. I have his testimony from a year ago, from January 2001. He detailed eight dangers that he feared in the next 12 to 24 months. So this is February 2001. The top of his list, a major terrorist attack against the U.S. interests either here or abroad, perhaps with a weapon designed to produce mass casualties. His second item, worsening conditions in the Middle East. He goes on to detail eight other—a total of eight challenges, four of which in fact turned out to have occurred in those next 12 months.

He also identified a threat of an expanded military conflict between India and Pakistan over Kashmir, something that did flare up in November and December of this year and thankfully has receded. He also identified intensifying disagreements with Russia over U.S. policy options, something that did flare up but thanks to the skillful diplomacy of President Bush and the wise strategic reorientation toward the West of President Putin that danger is now gone.

Anybody who is detailing eight dangers and four of them turn out to be right is somebody I would like to listen to. The problem is we didn't listen to this, because of, frankly, political considerations. Congress and the executive branch emphasized the threats that were most convenient to our political agendas. So we spent a lot of time and attention on ballistic missile threats. We spent $8 billion a year on ballistic missile threat. Is that where we should be putting our money? Is that the most urgent threat?

I would argue that it is not, that we have to find a way to depoliticize our threat assessments to come up with a national consensus on what the true threats are. I would encourage this committee to see if we can't devise a way to get a global comprehensive threat assessment that is nonpartisan, nonbiased, removed from the particular political agendas of the moment that can help guide our budgets, our diplomacy and our policy.

Thank you very much.

[The prepared statement of Mr. Cirincione follows:]

Testimony of

Joseph Cirincione

Director, Non-Proliferation Project

Carnegie Endowment for International Peace

Washington, D.C.

Before the Subcommittee on National Security,

Veterans Affairs, and International Relations

Committee on Government Reform

House of Representative

March 12, 2002

I deeply appreciate the opportunity to testify before the Subcommittee. I would like to offer a few observations on how our nation could better prepare for future attacks on the American homeland.

A major reason why the United States was so unprepared for terrorist attacks is that our national threat assessments for the past few years have consistently pointed policy-makers in the wrong direction. Partisan political warfare over the past decade distorted intelligence and defense assessments, and fundamentally misled and misdirected national security resources.

The two best known threat assessments compiled before September 11 are those prepared by two commissions chaired by current Secretary of Defense Donald Rumsfeld. The first in 1998, *Report of the Commission to Assess the Ballistic Missile Threat to the United States*, warned that the United States faced an urgent threat of attack by ballistic missiles that could be fielded by a hostile state "with little or no warning." The second, in January 2001, *Report of the Commission to Assess United States National Security Space Management and Organization*, warned just as ominously that we risked a "Pearl Harbor" in space unless we immediately launched an expansive and expensive effort to deploy new generations of sensors, satellites and weapons in space. Together, the reports fortified a national security vision favored by some conservatives and heavily influenced political

debate, threat assessments and budgetary priorities over the past three years.

Accordingly, until September 11 the top national security priority had been the deployment of a national missile defense system. Budgeted at over $8 billion per year, missile defense is by far the single most expensive weapons program in the defense budget. Last year, by comparison, $1.7 billion was allocated for combating weapons of mass destruction terrorism.

Senior officials made it their top agenda item in countless meetings with allies, Russia and China. Just a few months before September 11, five cabinet members, including National Security Advisor Condoleezza Rice, traveled to Moscow solely for the purpose of persuading the Russian leadership to acquiesce to abrogation of the Anti-Ballistic Missile Treaty. As Maureen Dowd wrote in *The New York Times* on September 5, "Why can George W. Bush think of nothing but a missile shield? Our president is caught in the grip of an obsession worthy of literature."

Ignored Warnings

It is fair to ask whether the September attacks could have been prevented if senior officials and summit meetings had addressed cooperative efforts to defend against terrorism rather than missiles. While reports on missile defense and space received overwhelming official and media attention, similar reports and warnings about asymmetrical threats and domestic terrorism were largely ignored.

Experts have warned of the dangers for years. The Commission on National Security/21st Century, chaired by former senators Gary Hart and Warren Rudman warned in February 2001 that "the United States will become increasingly vulnerable to hostile attack on the American homeland, and U.S. military superiority will not entirely protect us." Similarly in December 2001, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction said, "a terrorists attack on some level inside our borders is inevitable and the United States must be ready." The commission specifically found an urgent need to "craft a truly 'national' strategy to address the threat of domestic terrorism—conventional, cyber, chemical, biological, radiological and nuclear—from the perspective of deterrence, prevention, preparedness and response."

Numerous expert reports have warned over the past ten years that a terrorist group might try to buy or steal nuclear materials—warnings now eerily echoed in reports that al Qaeda operatives have tried to acquire uranium. In January 2001, a special commission chaired by Howard Baker and Lloyd Cutler urged the administration to triple the money spent on securing and eliminating Russia's nuclear weapons and materials. Cutler said, "Our principal conclusions are that the most urgent unmet national security threat for the United States today is the danger that weapons of mass destruction or weapons-usable material in Russia could be stolen and sold to terrorists or hostile nation-states, and used against American troops abroad, or citizens at home."

These concerns were noted in some official threat assessments. In February 2001, Admiral

Thomas Wilson, Director of the Defense Intelligence Agency, told Congress that over the next 12 to 24 months, he feared "a major terrorist attack against United States interests, either here or abroad, perhaps with a weapon designed to produce mass casualties." But the prediction was lost in a long list of other congressional concerns.

These clashing threat assessments often provoked debate between Democrats in Congress and the Republican administration. Chairman of the Senate Armed Services Committee Carl Levin summed up the divide in one such exchange:

> "I'm also concerned that we may not be putting enough emphasis on countering the most likely threats to our national security and to the security of our forces deployed around the world, those asymmetric threats, like terrorist attacks on the USS Cole, on our barracks and our embassies around the world, on the World Trade Center, including possible attacks with weapons of mass destruction and cyberthreats to our national security establishment and even to our economic infrastructure."

Deputy Secretary of Defense Paul Wolfowitz defended the assessments and budget priorities, "But when I think about it, what is different about the two [terrorism and missile defense] is, number one, we have some capability against the terrorist threat today....We have no ability to protect ourselves against ballistic missiles."

These priorities were completely wrong. Congressional inquiries would serve a valuable purpose by examining and eliminating the politicization of threat assessments that left America unprepared for the worst attacks it suffered in decades.

Has an example of how we have overestimated some threats while paying insufficient attention to others, I have attached the text of an article I wrote for *The Washington Post* Outlook section that was published on March 10, 2002.

A Much Less Explosive Trend

***The Washington Post* Sunday, March 10, 2002; Page B03**

By Joseph Cirincione

The president says the ballistic missile threat is growing and warns us how much more terrible Sept. 11 could have been if the terrorists had missiles. The CIA director says the proliferation of missile designs and technology has "raised the threat to the U.S. . . . to a critical threshold." Congress appropriates $8 billion a year to research missile defense systems -- the largest weapons program in the budget. The prevailing wisdom in Washington is that missile threats are mushrooming.

But are they? Ballistic missiles with nuclear warheads are the most dangerous weapons ever invented. Within minutes of launch they can destroy a distant city the size of Washington. However, the threat they pose now is less than in the past and is steadily declining. Today there are many fewer ballistic missiles in the world than 15 years ago, fewer nations trying to developthem, and only four potentially hostile nations trying to develop long-range versions. Moreover, the limited attack we most fear now from a rogue state would be much smaller than the nuclear holocaust we feared during the Cold War.

Of the more than 190 nations in the world, 35 of them, including the United States, have ballistic missiles. These are missiles that, like the V-2s first used by Nazi Germany, have a brief period of powered flight, then coast through space or the upper atmosphere on a ballistic trajectory that brings them back to Earth. Although the number of states with such missiles grew steadily during the Cold War, it is now decreasing. Over the past year, for example, Hungary, Poland and the Czech Republic have destroyed their small arsenals of Soviet-supplied Scud missiles; only Bahrain has joined the missile club with the purchase of some short-range missiles from the United States.

The existence of three dozen countries with ballistic missiles would still seem very dangerous but for two factors: Almost all these nations are friends of the United States, and almost all have only short-range missiles that threaten only their neighbors.

The United States is protected from most missile threats by the oceans. Almost any nation wishing to attack America from its own territory must build a missile capable of traveling thousands of miles. Fortunately, it is very difficult and expensive to do that. This is why 21 of the 35 nations possessing missiles have been able to deploy only short-range missiles, much like the V-2s, that can't go farther than 200 miles. Three others have short-range missiles capable of traveling 600 miles. Many of the missiles are old, poorly maintained and unreliable.

Of the other 10 nations besides the United States that have ballistic missiles, most only have medium-range systems that travel about 600 to 1,800 miles. That is far enough for Israel and Iran to hit each other, but not far enough for either to strike the United States.

Only China and Russia are able to attack the United States with nuclear warheads on long-range, land-based intercontinental missiles. This has not changed since Russia and China deployed their first ICBMs in 1959 and 1981 respectively. Even this threat is dwindling. Over the past 15 years, arms control agreements have cut arsenals capable of hitting the United States by 57 percent. The size of the Russian force, because of financial constraints,is expected to shrink further, from 1,022 to about 400 long-range missiles by the end of this decade; China might modernize and add to its 20 long-range missiles, but will probably deploy fewer than 40.

Not only is the American homeland less threatened by ballistic weapons; so are U.S. allies and troops in Europe. Arms control treaties with Moscow eliminated the entire class of intermediate-range ballistic missiles from the arsenal that once threatened Europe. Only three percent of the 680 missiles once in this class remain worldwide: China, with about 20 missiles, is the only nation that still possesses them.

What about the prevailing anxiety over newly emerging missile powers? The number of countries trying to develop ballistic missiles also has decreased and the nations still attempting to do so are poorer and less technologically advanced than were those trying 15 years ago. In the 1980s, we worried about missile programs in Argentina, Brazil, China, Egypt, Libya, India, Israel, Iraq, Pakistan, the Soviet Union and South Africa.In 2002, the Soviet Union is long gone; former Soviet republics Ukraine, Belarus and Kazakhstan have given up their missiles. Brazil, Argentina, Egypt and South Africa have abandoned their programs, Libya's is defunct, and Iraq's has been largely shut down. Only North Korea and Iran have started new programs.

The most significant proliferation threat today comes from the slow but steady increase in the number of states testing medium-range ballistic missiles. This development is often cited as evidence of a larger proliferation threat. Seven nations -- China, India, Iran, Israel, Pakistan, North Korea and Saudi Arabia -- now have missiles in this range. Of these, three potentially could come into conflict with the United States -- China, Iran and North Korea.

But China is the only potentially hostile nation with both ballistic missiles that can reach the United States and the nuclear warheads to put on them. North Korea might in the next 10 years develop a missile with a nuclear warhead that could reach the United States, but it does not have that capability now. Iran has neither long-range missiles nor nuclear warheads. Iran's effort to import and duplicate North Korean missiles appears in disarray after its Shahab-3 missiles blew up in two of the three tests it conducted in 1998 and 2000. We could also include Iraq in this threat mix. But Iraq's missile and nuclear ambitions are constrained by U.N. sanctions and prohibitions. It has neither nuclear warheads nor long-range missiles and it would take years for it to fully reconstruct its former programs. While theoretically possible, it appears unlikely that either Iran or Iraq will have a nuclear-armed long-range missile within the next 10 to 15 years.

Still, even if there are fewer missiles and fewer nations with missiles, if one of these three nations deployed a long-range missile by 2010, wouldn't that mean the missile threat was more acute? Not necessarily. Capability does not necessitate use. Each of these countries would almost surely be deterred from attacking the United States by the certainty that swift retaliation would follow even a failed or thwarted attack. It is also likely that the United States would preemptively destroy a missile as it was being assembled for launch.

Even our worst-case scenarios aren't as bad as they once were. If deterrence or preventive defense failed, the damage that countries such as North Korea, Iran or Iraq could inflict with one or two warheads would be a major catastrophe. But compare that to the nuclear exchange we feared 15 years ago -- in which thousands of Soviet warheads would have destroyed our country, or even the planet. The United States and NATO spent hundreds of billions of dollars, fielded dozens of military systems and endured numerous diplomatic crises precisely because we feared those missiles. We lived through decades of anxiety, from civil defense drills in classrooms to dueling deployments of Soviet SS-20s in Eastern Europe and U.S. Pershing and cruise missiles in Western Europe. In no sense can the missile threat today be considered more imminent or lethal than the threat 15, 20 or 40 years ago

.

Then why do so many people feel it is?

It may be the psychology of threat assessments. Proliferation experts invariably see the future as more threatening than the past. It is, after all, the unknown. In addition, historical revisionism has transformed the Soviet Union to an almost benign, predictable and deterrable foe, in contrast to today's supposedly unpredictable, less easily deterred rogues. This was not how the Soviet threat was viewed at the time, however.

More concretely, the estimates of the ballistic missile threat prepared by the intelligence community over the past few years have focused on Iran, Iraq and North Korea, rather than assessing the entire global picture. This approach distorts the threat. Like a fun-house mirror, it makes objects appear larger than they really are.

This is not primarily the fault of the agencies, which, in fact, have sophisticated and varied opinions on the threat. After the Republican Party won control of Congress in 1994, congressional leaders relentlessly attacked government analysts who presented balanced assessments for understating the missile threat. Congress mandated its own assessment by a hand-picked commission chaired by Donald Rumsfeld. His 1998 report warned that a ballistic missile attack could come from a hostile state "with little or no warning." This fit with preconceived positions for increased defense budgets and a crash program to field a national missile defense system. U.S. intelligence agency analysts fell in line, giving Congress the worst-case scenarios some lawmakers sought. As Richard Perle said at the beginning of the Reagan presidency, "Democracies will not sacrifice to protect their security in the absence of a sense of danger." Exaggerated views of the missile threat provided that sense of

danger

.

Sept. 11 showed us real danger. And it had nothing to do with missiles. The ballistic missile threat today is confined, limited and changing relatively slowly. There is every reason to believe that it can be addressed through diplomacy and measured military preparedness. If missile defenses prove feasible, particularly those designed to counter the more prevalent short-range missiles, they can be an important part of these efforts. But they should never dominate our policy. The sooner we restore balance to our assessments, budgets and diplomacy, the better prepared the country will be for the genuine threats we face.

Mr. SHAYS. Thank you very much.

Mr. Hinton, thank you very much as well for participating. Sometimes we put GAO as a special part of a panel. But I wanted the synergy of the four of you together, as I said before. So thank you.

Mr. HINTON. Thank you, Mr. Chairman, Mr. Kucinich, members of the committee. I appreciate the opportunity to discuss with you today our country's progress in combating terrorism to enhance homeland security. Protecting the United States and its citizens from terrorism is a national effort involving both the government and nongovernment sectors. Such broad-based efforts are inherently difficult to lead and manage. We've heard that this morning. It's been a theme. Enhancing homeland security involves all 50 States, the District of Columbia and the Territories, thousands of municipalities, more than 40 Federal agencies and countless private entities. These organizations have multiple specialized missions, distinct organizational cultures and millions of employees. Trying to effectively involve them in a single coordinated effort is a monumental undertaking.

As requested, my testimony will cover three areas: One, progress in enhancing homeland security through legislative and executive action; two, the preliminary results of our work we're doing for you, Mr. Chairman, and other Members of the House on integrating the efforts of all levels of government and the private sector into an overall homeland security strategy and; three, an approach that could be helpful in integrating governmental and private sector organizations into the Office of Homeland Security's planned national strategy.

Very briefly in response to those three objectives. One, a variety of legislative and executive branch actions to enhance homeland security were underway prior to September 11th or have been taken since that day. After the attacks the President established the Office of Homeland Security, which plans to issue its national strategy in July of this year. In the absence of a national strategy agencies have been implementing many homeland security initiatives, including planning to produce new vaccines against anthrax, and expanding the existing smallpox vaccine stockpile, providing additional planning and training for State and local disaster response and enhance aviation, seaport and border security.

Legislative actions include appropriations of about $19½ billion for 2002 and about $10 billion contained in the $40 billion emergency supplemental bill that was enacted shortly after September 11th. And for 2003 the President has requested about $38 billion for homeland security.

Our on board work, Mr. Chairman, indicates that government and nongovernment activities are looking to the Office of Homeland Security for further direction on how to better integrate their missions and more effectively contribute to the overarching homeland security effort. Without a strategy in place some Federal agencies are not sure what else they should be doing beyond their traditional missions. They also do not share a common definition of homeland security.

Even though officials at key Federal agencies believe such a definition is needed to promote a common understanding of operational

plans and requirements, to enforce budget discipline, and to avoid duplication of effort and gaps in coverage, although Federal agencies are looking for guidance, they also want to ensure that their organization's unique missions are sufficiently factored into the national strategy and implementing guidance as developed. Officials in State and local governments that we interviewed are also looking for assistance in terms of funding relief and better access to threat information, a theme that we heard this morning from the Federal Government.

Finally, private sector entities expressed a willingness to contribute to homeland security, but they are concerned about the potential for excessive Federal regulation. Once the national strategy is issued, Mr. Chairman, Federal, State and local government agencies and private organizations will need to work together to effectively implement the goals and objectives. Public/private partnerships were used to address the Y2K concerns and can be similarly used to promote implementation of the national strategy by public and private sector organizations.

These partnerships that came about in the Y2K debate were implemented through five broad efforts: One, congressional oversight of agencies to hold them accountable for demonstrating progress to heighten public awareness of the problem; two, central leadership and coordination to ensure that Federal systems were ready for the date change to coordinate efforts primarily with the States and to promote private sector and foreign government action; three, partnerships within the intergovernmental system and with private entities divided into key economic sectors address issues such as contingency planning; four, communications as we've heard this morning to share information on the status of systems, products and services and to share recommended solutions; and, last, but very importantly, human capital and budget initiatives to help ensure that the government could recruit and retain the technical expertise needed to convert systems and communicate with other partners and to fund conversion operations.

There are many parallels that are evident from the Y2K experience that can be translated to the current debate around homeland security.

Mr. Chairman, that concludes my statement. I'll be ready to take any questions you may have.

[The prepared statement of Mr. Hinton follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations
House Committee on Government Reform

For Release on Delivery
Expected at 10:00 a.m., EST
Tuesday,
March 12, 2002

HOMELAND SECURITY

Progress Made; More Direction and Partnership Sought

Statement of Henry L. Hinton, Jr.
Managing Director, Defense Capabilities and Management

GAO-02-490T

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to discuss with you today our country's progress in combating terrorism to enhance homeland security. Protecting the United States and its citizens from terrorism is a national effort involving both the government and nongovernment sectors. Such broad-based efforts are inherently difficult to lead and manage. More than 40 federal entities alone are involved in combating terrorism. Enhancing homeland security becomes even more complex because it involves all 50 states, the District of Columbia, and the territories; thousands of municipalities; and countless private entities, many of which own the infrastructure that can be attacked. These organizations have multiple, specialized missions, distinct organizational cultures, and millions of employees. Some have both international and domestic components and operations. Trying to effectively involve them in a single, coordinated effort makes a monumental undertaking.

Since September 11, our nation has taken many actions to combat terrorism and enhance homeland security. Today, it is well known that our servicemembers are conducting operations in Afghanistan in Operation Enduring Freedom. This operation covers offensive actions in the Afghanistan theater and the North Arabian Sea, and includes ground, air, and naval forces, and follow-on operations for certain support activities. Less well-known perhaps is the Department of Defense's other primary ongoing operation, Noble Eagle, which concerns the direct defense of the U.S. homeland. This operation protects civilian population centers, critical infrastructure, and special events such as the recently completed Winter Olympics held in Salt Lake City. To help provide operational forces, the department has alerted for activation just over 97,000 reserve component servicemembers and completed the call-up of more than 78,000 Reserve and National Guard augmentees.

As requested, my testimony will cover three areas. First, I will discuss progress in enhancing homeland security through legislative and executive action prior to and after September 11. Second, I will present the preliminary results of the work we are doing for you and some of your House colleagues on integrating the efforts of all levels of government and the private sector into overall homeland security efforts. Finally, I will discuss an approach that could be helpful in integrating governmental and private sector organizations into the Office of Homeland Security's planned national strategy.

My testimony is generally based on the large body of relevant work that we have completed or have ongoing.[1]

Summary

A variety of legislative and executive branch actions to enhance homeland security have been taken or were underway prior to and since September 11. After the attacks, the president issued executive order 13228 to establish the Office of Homeland Security. The office plans to issue a national strategy in July 2002. In the interim, federal agencies are implementing many homeland security initiatives, including planning to produce new vaccines against anthrax and expanding the existing smallpox vaccine stockpile; providing additional planning and training for state and local disaster response; and enhancing aviation, seaport, and border security. Legislative actions include appropriation of about $19.5 billion for fiscal year 2002 and about $9.8 billion contained in a $40 billion emergency supplemental budget shortly after the September 11 terrorist attack. For fiscal year 2003, the president has requested about $37.7 billion for homeland security.

Our ongoing work indicates that government and nongovernment activities are looking to the Office of Homeland Security for further direction on how to better integrate their missions and more effectively contribute to the overarching homeland security effort. For example, at key federal agencies we did not find a broadly accepted definition of homeland security. Having a common definition can help avoid duplication of effort and gaps in coverage by identifying agency roles and responsibilities. Although the agencies are looking for guidance, they also want to ensure that their organizations' unique missions are sufficiently factored in as that guidance is developed. At the same time, without a national strategy, some agencies were not sure what else they should be doing beyond their traditional missions. Officials in state and local governments want funding relief and better access to threat information from the federal government. Finally, private sector entities expressed a willingness to contribute to homeland security, but they are concerned about the potential for excessive federal regulation. If it is comprehensive, the national strategy should address many of these issues.

Once the national strategy is issued, the federal, state, and local government agencies and private sector organizations will need to work

[1] See the appendix for a list of selected reports and testimonies.

together to effectively implement the goals and objectives. Public-private partnerships were used to address Y2K concerns and can similarly be used to promote implementation of the national strategy by public and private sector organizations.

Improvements to Homeland Security Are in Process

Legislative and executive branch action has led to a variety of governmentwide and agency-specific initiatives, started and ongoing, to enhance homeland security. Establishment of an Office of Homeland Security and the office's planned national security strategy represent important governmentwide initiatives to address homeland security concerns. The planned production of new vaccines or expansion of existing vaccines, additional intergovernmental-planning and consequence-management efforts, and enhancements to aviation, seaport, and border security suggest progress in enhancing homeland security. Moreover, Congress appropriated about $19.5 billion in fiscal year 2002 and about another $9.8 billion contained in a $40 billion emergency supplemental budget after September 11 to help address homeland security concerns. The president has requested about $37.7 billion for fiscal year 2003 for homeland security.

Governmentwide Initiatives

In October 2001, the president established a single focal point to coordinate efforts to secure the United States from terrorist attacks—the Office of Homeland Security. This is consistent with a recommendation that we had previously made. The office is charged with broad responsibilities including, but not limited to (1) working with federal agencies, state and local governments, and private entities to develop a national strategy and to coordinate implementation of the strategy; (2) overseeing prevention, crisis-management, and consequence-management activities; (3) coordinating threat and intelligence information; (4) reviewing governmentwide budgets for homeland security as well as providing advice to agencies and the Office of Management and Budget on appropriate levels of funding; and (5) coordinating critical infrastructure protection. The office plans to issue its national strategy in July 2002. The strategy is to be "national" in scope not only by including states, localities, and private-sector entities, as well as federal agencies; but also by setting clear objectives for homeland security with performance measures to gauge progress. Also, the plan is to be supported by a crosscutting federal budget plan.

In previous work on combating terrorism,[2] we had also recommended that the Federal Bureau of Investigation work with appropriate agencies to develop a national-level threat assessment on terrorist use of weapons of mass destruction. The bureau concurred in July 1999 but never issued the assessment and has now suspended the effort. We continue to believe that the threat assessment is needed.

Production of New Vaccines

Progress has been made and efforts are continuing to enhance U.S. capability to respond to biological terrorism. Research is underway to enable the rapid identification of biological agents in a variety of settings; develop new or improved vaccines, antibiotics, and antivirals to improve treatment and vaccination for infectious diseases caused by biological agents; and develop and test emergency response equipment such as respiratory and other personal protective equipment. Another initiative includes the production of 155 million doses of smallpox vaccine to bring the total number of doses in the nation's stockpile to 286 million by the end of 2002, which is enough to protect every U.S. citizen. In addition, the National Institutes of Health plans to award a contract to accelerate development of new vaccines against anthrax.

The number of "push packages" in the National Pharmaceutical Stockpile[3] will increase from 8 to 12. Each push package has quantities of several different antidotes and antibiotics that can treat and protect persons exposed to different biological and chemical agents. The push packages are planned to have enough pharmaceuticals to treat 12 million persons for inhalation anthrax as compared to the 2 million that could be treated before the project started. Finally, Mr. Chairman, the concerns you raised prior to September 11, 2001, about accountability over medical supplies, including items from the National Pharmaceutical Stockpile, put responsible agencies on alert, and they have subsequently improved their

[2] *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks* (GAO/NSIAD-99-163, Sept. 14, 1999).

[3] The Centers for Disease Control's National Pharmaceutical Stockpile Program is to ensure the availability and rapid deployment of pharmaceuticals, antidotes, other medical supplies, and equipment to counter the effects of biological pathogens and chemical agents.

internal controls for these items so they are current, accounted for, and ready to use.[4]

Intergovernmental Planning and Consequence Management

As you know Mr. Chairman, federal, state, and local governments share a responsibility to prepare for a terrorist incident. The first responders to a terrorist incident usually belong to local governments and local emergency response organizations, which include local police and fire departments, emergency medical personnel, and public health agencies. Historically, the federal government has primarily provided leadership, training, and funding assistance.

The president's First Responder Initiative was announced in his State of the Union address of January 29, 2002. The initiative will be led by the Federal Emergency Management Agency, and its proposed fiscal year 2003 budget includes $3.5 billion to provide the first responder community with funds to conduct important planning and exercises, purchase equipment, and train their personnel. At the request of the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, House Committee on Government Reform, we have begun to examine the preparedness issues confronting state and local governments and will report back to the subcommittee later this year.

Aviation and Seaport Security

Progress has been made in addressing aviation security concerns, but significant challenges will need to be confronted later this year to meet established goals and time frames. The Congress passed the Aviation and Transportation Security Act in November 2001, which created the Transportation Security Administration with broad new responsibilities for aviation security. The administration faces the daunting challenge of creating this new organizational structure, which must implement more than two dozen specific actions by the end of 2002. All actions due to date have been completed, but formidable tasks remain. For example, the administration is required to have sufficient explosive detection systems in place to screen all checked baggage at more than 400 airports nationwide by December 31, 2002. As of January 2002, fewer than 170 of these machines had been installed. The administration estimates that about

[4] *Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement* (GAO-01-463, Mar. 30, 2001) and *Combating Terrorism: Chemical and Biological Medical Supplies Are Poorly Managed* (GAO/HEHS/AIMD-00-36, Oct. 29, 1999).

2,000 additional machines will need to be produced and installed by the end of the year. Concerns have been raised that the vendors will not be able to produce sufficient number of machines to meet the deadline. The administration continues to work to identify ways to fill the gap between the requirement and the production capability, including considering the use of noncertified equipment as an interim measure. Also, the administration needs to hire about 40,000 employees, including more than 30,000 screeners, federal air marshals, and other officials. Achieving this goal presents a big challenge because a significant number of the current screening workforce may not qualify for screening positions. Airport screeners must now be U.S. citizens and be able to speak and read English. For example, currently up to 80 percent of the personnel in these positions at Dulles International Airport in Washington, D.C., do not qualify for employment.

While not currently as high-profile as airport security, the vulnerability of major commercial seaports to criminal and terrorist activity has caused concern for many years, and the terrorist attacks on September 11, 2001, elevated those concerns again. Even prior to the attacks, this subcommittee expressed concerns about seaport security and the potential consequences of a terrorist attack on the successful deployment of our military forces. Because of these concerns, you asked us to examine the effectiveness of Department of Defense force protection measures at critical seaports located within the United States and at overseas locations, and we will issue our report to you later this year. As part of our work, some of which I can highlight today, we have observed efforts by the Coast Guard to improve seaport security since the attacks.

In order to establish a clear indication of how Coast Guard units and personnel should respond to various threat levels at seaports, the Coast Guard is developing three new maritime security levels. The first level, "new normal," will encompass a greater level of security effort in the ports, including increased emphasis on security patrols, improved awareness of all activity in and around seaports, and better information about inbound vessels and their cargo. The other two security levels will contain increasingly heightened security measures to be taken if threat conditions escalate. The Coast Guard has also initiated the "sea marshal" program, whereby armed Coast Guard teams are placed aboard select commercial vessels navigating the waters of some of our major ports. A third Coast Guard initiative underway is the development of a vulnerability assessment methodology that the Coast Guard plans to use at more than 50 major U.S. seaports to identify vulnerabilities of critical infrastructure at each port.

Congress is considering legislation to enhance seaport security. The port and maritime security legislation, which passed the Senate in December, contains a number of provisions aimed at further improving the state of seaport security. Among these provisions are establishing local port security committees, comprised of a broad range of federal, state, and local governments as well as commercial representatives; requiring vulnerability assessments at major U.S. seaports; developing comprehensive security plans for all waterfront facilities; improving collection and coordination of intelligence; improving training for maritime security professionals; making federal grants for security infrastructure improvements; and preparing a national maritime transportation security plan. Moreover, for fiscal year 2002, Congress appropriated $93.3 million to the Transportation Security Administration for port security assessment and improvements.

Border Security

The Immigration and Naturalization Service (INS) has a number of efforts underway designed to increase border security to prevent terrorists or other undesirable aliens from entering the United States. The service proposes to spend nearly $3 billion on border enforcement in fiscal year 2003, about 75 percent of its total enforcement budget of $4.1 billion. I will describe some of the service's efforts to increase security at the nation's ports of entry and between the ports, as well as to coordinate efforts with Canadian authorities to deter illegal entry into Canada or the United States.

Ports of Entry

Currently, the United States does not have a system for identifying who has overstayed their visa, nor a sufficient ability to identify and locate visitors who may pose a security threat. Consequently, INS is developing an entry and exit system to create records for aliens arriving in the United States and match them with those aliens' departure records. The Immigration and Naturalization Service Data Management Improvement Act of 2000 requires the attorney general to implement such a system at all airports and seaports by the end of 2003, at the 50 land border ports with the greatest numbers of arriving and departing aliens by the end of 2004, and at all ports by the end of 2005. The USA Patriot Act, passed in October 2001, instructs the attorney general and the secretary of state to focus on two new elements in designing an entry and exit system—the development of tamper-resistant documents readable at ports of entry, and the utilization of biometric technology. Legislation now before Congress would go further by making the use of biometrics a requirement in the proposed entry and exit system.

Implementing such a system within the mandated deadlines represents a major challenge for the INS. According to INS officials, important policy decisions significantly affecting development, cost, schedule, and operation of an entry and exit system have yet to be made. For example, it has not been decided whether arrival and departure data for Canadian citizens will be recorded in the new system. Currently, Canadian citizens are not required to present documents to enter the United States. The particular biometric identifier to be used, such as a fingerprint or facial recognition, has not been determined. Nor has a decision been made on whether a traveler's biometric would be checked only upon entry, or at departure, too.

The INS' proposed fiscal year 2003 budget states that INS seeks to spend $380 million on the proposed system in fiscal year 2003. To increase the detection and apprehension of inadmissible aliens, including terrorists, at the nation's ports of entry, the service seeks to add nearly 1,200 inspectors in fiscal year 2003 to operate more inspection lanes at land ports and air ports of entry, and examine information on arriving passengers in order to identify high-risk travelers.

Between the Ports of Entry

To deter illegal entry between the ports of entry and make our borders more secure, the INS seeks to add an additional 570 Border Patrol agents in fiscal year 2003. In response to the September 11 attack, of the 570 Border Patrol positions, INS now seeks to add 285 agents to the northern border, thereby accelerating a staffing buildup at the northern border. The remaining half will be deployed to the southwest border. This represents a departure from previous decisions to deploy most new agent positions to the southwest border. Along the northern border, the service plans on maintaining an air surveillance program capable of responding 24 hours a day 7 days a week. Plus it plans to complete the installation of 67 automated surveillance systems and begin construction of 44 new systems. In addition, the INS has signed a memorandum of agreement with the Department of Defense allowing about 700 National Guard troops and equipment, such as helicopters, to assist in border enforcement duties for up to 6 months. The agreement allows the use of the troops for such activities as assisting in surveillance, transporting Border Patrol agents, as well as managing traffic at ports of entry.

Coordination with Canada

In December 2001, the United States and Canada signed a Smart Border Declaration calling for increased coordination to create a border that facilitates the free flow of people and commerce while maintaining homeland security. The declaration calls for such actions as (1) implementing collaborative systems to identify security risks while

expediting the flow of low-risk travelers, (2) identifying persons who pose a security threat before they arrive at North American airports or seaports through collaborative approaches such as reviewing crew and passenger manifests, and (3) establishing a secure system to allow low-risk frequent travelers between the two countries to cross the border more efficiently. The INS and other U.S. and Canadian agencies are in the initial stages of working on developing plans and initiatives to implement the declaration's objectives.

Funding for Homeland Security

Congress has also acted and provided significant homeland security funds. According to documents supporting the president's fiscal year 2003 budget request, about $19.5 billion in federal funding for homeland security was enacted in fiscal year 2002. Congress added about $9.8 billion more in an emergency supplemental appropriation of $40 billion following the September 11 attacks. The funds were to be used for a variety of homeland security needs including supporting first responders, defending against biological terrorism, securing U.S. borders, enhancing aviation security, and supporting Department of Defense support to homeland security, among other things. The president has now requested about $37.7 billion for homeland security in his fiscal year 2003 budget request.

Public and Private Sectors Seek Both Direction From and Partnership With the Office of Homeland Security

Our ongoing work indicates that federal agencies, state and local governments, and the private sector are looking for guidance from the Office of Homeland Security on how to better integrate their missions and more effectively contribute to the overarching homeland security effort. In interviews with officials at more than a dozen federal agencies, we found that a broadly accepted definition of homeland security did not exist. Some of these officials believed that it was essential that the concept and related terms be defined, particularly because homeland security initiatives are crosscutting, and a clear definition promotes a common understanding of operational plans and requirements, and can help avoid duplication of effort and gaps in coverage. Common definitions promote more effective agency and intergovernmental operations and permit more accurate monitoring of homeland security expenditures at all levels of government. The Office of Homeland Security may establish such a definition. The Office of Management and Budget believes a single definition of homeland security can be used to enforce budget discipline. Although some agencies are looking to the Office of Homeland Security for guidance on how their agencies should be integrated into the overall security effort and to explain what else they should be doing beyond their traditional missions, they also want their viewpoints incorporated as this

guidance evolves. For example, an official at the Centers for Disease Control and Prevention saw the Office of Homeland Security as both providing leadership and getting "everyone to the table" to facilitate a common understanding of roles and responsibilities.

State officials told us that they also seek additional clarity on how they can best participate in the planned national strategy for homeland security. The planned national strategy should identify additional roles for state and local governments, but the National Governor's Association made clear to us that governments oppose mandated participation and prefer broad guidelines or benchmarks.

State officials were also concerned about the cost of assuming additional responsibilities, and they plan to rely on the federal government for funding assistance. The National Governors Association estimates fiscal year 2002 state budget shortfalls of between $40 billion and $50 billion, making it increasingly difficult for the states to take on expensive, new homeland security initiatives without federal assistance. As we address the state fiscal issues through grants and other tools, we must (1) consider targeting the funds to states and localities with the greatest need, (2) discourage the replacement of state and local funds with federal funds, and (3) strike a balance between accountability and flexibility.

State and local governments believe that to function as partners in homeland security they need better access to threat information. Officials at the National Emergency Management Association, which represents state and local emergency management personnel, stated that such personnel experienced problems receiving critical intelligence information and that this hampered their ability to help pre-empt terrorists before they strike. According to these officials, certain state or local emergency management personnel, emergency management directors, and certain fire and police chiefs hold security clearances granted by the Federal Emergency Management Agency; however, other federal agencies, such as the Federal Bureau of Investigation, do not recognize these clearances. Moreover, the National Governor's Association said that intelligence sharing is a problem between the federal government and the states. The association explained that most governors do not have a security clearance and, therefore, do not receive classified threat information, potentially impacting their ability to effectively use the National Guard and hampering their emergency preparedness capability. On the other hand, we were told that local Federal Bureau of Investigation offices in most states have a good relationship with the emergency management

community and at times shared sensitive information under certain circumstances.

The private sector is also concerned about costs, but in the context of new regulations to promote security. In our discussions with officials from associations representing the banking, electrical energy, and transportation sectors, they expressed the conviction that their member companies desire to fully participate as partners in homeland security programs. These associations represent major companies that own infrastructure critical to the functioning of our nation's economy. For example, the North American Electric Reliability Council is the primary point of contact with the federal government on issues relating to the security of the nation's electrical infrastructure. It has partnered with the Federal Bureau of Investigation and the Department of Energy to establish threat levels that they in turn share with utility companies within their organization. Such partnerships are essential, but the private sector may be reluctant to embrace them because of concern over new and excessive regulation, although their assets might be better protected. According to National Industrial Transportation League officials, for example, transport companies express a willingness to adopt prudent security measures such as increased security checks in loading areas and security checks for carrier drivers. However, the league is concerned that the cost of additional layers of security could cripple their ability to conduct business and felt that a line has to be drawn between security and the openness needed to conduct business.

If it is to be comprehensive, a national strategy should address many of these issues.

Y2K Style Partnerships Can Be Useful in Promoting Public-Private Participation for Homeland Security

Once the homeland security strategy is developed, participating public and private sector organizations will need to understand and prepare for their defined roles under the strategy. In that connection, Y2K-style partnerships can be helpful. While the federal government can assign roles to federal agencies under the strategy, it will need to reach consensus with the other levels of government and with the private sector on their roles.

As you know Mr. Chairman, the world was concerned about the potential for computer failures at the start of the year 2000, known as Y2K. The recognition of the interconnectedness of critical information systems led to the conclusion that a coordinated effort was needed to address the problem. Consequently, Congress, the administration, federal agencies, state and local governments, and private sector organizations collaborated

to address Y2K issues and prevent the potential disruption that could have resulted from widespread computer failure. Similarly, the homeland security strategy is intended to include federal, state, and local government agencies and private sector entities working collaboratively, as they did in addressing Y2K issues.

The Y2K task force approach may offer a model for developing the public-private partnerships necessary under a comprehensive homeland security strategy. A massive mobilization with federal government leadership was undertaken in connection with Y2K, which included partnerships with state, local, and international governments and the private sector and effective communication to address critical issues. Government actions went beyond the boundaries of individual programs or agencies and involved governmentwide oversight, interagency cooperation, and cooperation among federal, state, and local governments as well as with private sector entities and even foreign countries. These broad efforts can be grouped into the following five categories:

- Congressional oversight of agencies to hold them accountable for demonstrating progress to heighten public awareness of the problem.
- Central leadership and coordination to ensure that federal systems were ready for the date change, to coordinate efforts primarily with the states, and to promote private-sector and foreign-government action.
- Partnerships within the intergovernmental system and with the private entities, divided into key economic sectors to address such issues as contingency planning.
- Communications to share information on the status of systems, products, and services, and to share recommended solutions.
- Human capital and budget initiatives to help ensure that the government could recruit and retain the technical expertise needed to convert systems and communicate with the other partners and to fund conversion operations.

As we reported in September 2000,[5] the value of federal leadership, oversight, and partnerships was repeatedly cited as a key to success in addressing Y2K issues at a Lessons Learned summit that was broadly attended by representatives from public and private sector entities. Developing a homeland security plan may require a similar level of

[5] *Year 2000 Computing Challenge: Lessons Can Be Applied to Other Management Challenges* (GAO/AIMD-00-290, Sept. 12, 2000).

leadership, oversight, and partnerships with state and local governments, and the private sector. In addition, as in the case of Y2K efforts, Congressional oversight will be very important in connection with the design and implementation of the homeland security strategy.

Mr. Chairman, this concludes my prepared statement. I would be happy to answer any questions you or members of the subcommittee may have. Please contact me at (202) 512-4300 for more information. Raymond J. Decker, Brian. J. Lepore, Stephen L. Caldwell, Lorelei St. James, Patricia Sari-Spear, Kim Seay, William J. Rigazio, Matthew W. Ullengren, Deborah Colantonio, and Susan Woodward made key contributions to this statement.

Related GAO Products

Homeland Security

Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs (GAO-02-160T, November 7, 2001).

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts (GAO-02-208T, October 31, 2001).

Homeland Security: Need to Consider VA's Role in Strengthening Federal Preparedness (GAO-02-145T, October 15, 2001).

Homeland Security: Key Elements of a Risk Management Approach (GAO-02-150T, October 12, 2001).

Homeland Security: A Framework for Addressing the Nation's Issues (GAO-01-1158T, September 21, 2001).

Combating Terrorism

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness (GAO-02-483T, March 1, 2002).

Combating Terrorism: Considerations For Investing Resources in Chemical and Biological Preparedness (GAO-01-162T, October 17, 2001).

Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822, September 20, 2001).

Combating Terrorism: Actions Needed to Improve DOD's Antiterrorism Program Implementation and Management (GAO-01-909, September 19, 2001).

Combating Terrorism: Comments on H.R. 525 to Create a President's Council on Domestic Preparedness (GAO-01-555T, May 9, 2001).

Combating Terrorism: Observations on Options to Improve the Federal Response (GAO-01-660T, April 24, 2001).

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy (GAO-01-556T, March 27, 2001).

Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response (GAO-01-15, March 20, 2001).

Combating Terrorism: Federal Response Teams Provide Varied Capabilities: Opportunities Remain to Improve Coordination (GAO-01-14, November 30, 2000).

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training (GAO/NSIAD-00-64, March 21, 2000).

Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism (GAO/T-NSIAD-00-50, October 20, 1999).

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack (GAO/NSIAD-99-163, September 7, 1999).

Combating Terrorism: Observations on Growth in Federal Programs (GAO/T-NSIAD-99-181, June 9, 1999).

Combating Terrorism: Analysis of Potential Emergency Response Equipment and Sustainment Costs (GAO-NSIAD-99-151, June 9, 1999).

Combating Terrorism: Use of National Guard Response Teams Is Unclear (GAO/NSIAD-99-110, May 21, 1999).

Combating Terrorism: Observations on Federal Spending to Combat Terrorism (GAO/T-NSIAD/GGD-99-107, March 11, 1999).

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO-NSIAD-99-3, November 12, 1998).

Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program (GAO/T-NSIAD-99-16, October 2, 1998).

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments (GAO/NSIAD-98-74, April 9, 1998).

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, December 1, 1997).

Public Health

Bioterrorism: The Centers for Disease Control and Prevention's Role in Public Health Protection (GAO-02-235T, November 15, 2001).

Bioterrorism: Review of Public Health and Medical Preparedness (GAO-02-149T, October 10, 2001).

Bioterrorism: Public Health and Medical Preparedness (GAO-02-141T, October 10, 2001).

Bioterrorism: Coordination and Preparedness (GAO-02-129T, October 5, 2001).

Bioterrorism: Federal Research and Preparedness Activities (GAO-01-915, September 28, 2001).

Chemical and Biological Defense: Improved Risk Assessments and Inventory Management Are Needed (GAO-01-667, September 28, 2001).

West Nile Virus Outbreak: Lessons for Public Health Preparedness (GAO/HEHS-00-180, September 11, 2000).

Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks (GAO/NSIAD-99-163, September 7, 1999).

Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework (GAO/NSIAD-99-159, August 16, 1999).

Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives (GAO/T-NSIAD-99-112, March 16, 1999).

Disaster Assistance

Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures (GAO-01-837, August 31, 2001).

Federal Emergency Management Agency: Status of Achieving Key Outcomes and Addressing Major Management Challenges (GAO-01-832, July 9, 2001).

FEMA and Army Must Be Proactive in Preparing States for Emergencies (GAO-01-850, August 13, 2001).

Budget and Management

Results-Oriented Budget Practices in Federal Agencies (GAO-01-1084SP, August 2001).

Managing for Results: Federal Managers' Views on Key Management Issues Vary Widely Across Agencies (GAO-010592, May 2001).

Determining Performance and Accountability Challenges and High Risks (GAO-01-159SP, November 2000).

Managing for Results: Using the Results Act to Address Mission Fragmentation and Program Overlap (GAO/AIMD-97-156, August 29, 1997).

Government Restructuring: Identifying Potential Duplication in Federal Missions and Approaches (GAO/T—AIMD-95-161, June 7, 1995).

Government Reorganization: Issues and Principals (GAO/T-GGD/AIMD-95-166, May 17, 1995).

Grant Design

Grant Programs: Design Features Shape Flexibility, Accountability, and Performance Information (GAO/GGD-98-137, June 22, 1998).

Federal Grants: Design Improvements Could Help Federal Resources Go Further (GAO/AIMD-97-7, December 18, 1996).

Block Grants: Issues in Designing Accountability Provisions (GAO/AIMD-95-226, September 1, 1995).

Mr. SHAYS. Thank you very much. Mr. Tierney didn't participate in the first round and, with Mr. Kucinich's concurrence, we're going to go to him first.

Mr. TIERNEY. Thank you. Mr. Chairman, if it's acceptable to everyone, I'll submit my statement for the record and then just ask the questions because I have to run.

Mr. SHAYS. Sure, that would be good.

Mr. TIERNEY. I thank the witnesses for their indulgence. Somebody mentioned either, this panel or last panel, that President Bush said there was no margin for error, the stakes are too high to get it wrong, which apparently seems to be correct except when it comes to national missile defense, which is raised somewhat to the level of religion by some folks around here because apparently it now seeks to do a trial and error process of development of national missile defense. And our occasion for determining whether or not the trial has been in error won't be until we are under attack.

That concerns me greatly because I think if we properly assess the threats that are posed to us and put them in the proper priority order, then we will have time to research and test any type of national missile defense before we actually start trying to build it and potentially wasting a lot of money for false security.

Mr. Cirincione, back before 1998 most intelligence estimates indicated that the nearest threat we had of any country sending a long range ballistic missile at us was 2010 or beyond. Then along came Mr. Rumsfeld and, not surprisingly, I would guess a couple of reports came out and all of a sudden it became much more immediate. Then the CIA then bought into it, the Pentagon.

Can you explain to us what seems to have happened that people so radically changed their opinion apparently without any change in the underlying facts?

Mr. CIRINCIONE. Several things, Congressman. And in 1993, when Mr. Woolsey was Director of the CIA, he submitted a threat assessment, national intelligence estimate, they're called, NIE, on the ballistic missile threat to the United States that concluded that the United States would not face a third country developing an ICBM with a nuclear warhead for at least 15 years. In 1995, a new assessment was done that reaffirmed and went even a little further, went into greater detail, the fact that the United States would only face a ballistic missile attack from Russia or China over the next 15 years.

At that time those assessments came under harsh criticism from some Members of Congress, and there were a number of very intense hearings that criticized those assessments for underestimating the ballistic missile threat. The Congress then decided to do its own independent assessment and Congress hand-picked a commission to review the national intelligence estimate.

In 1996, that commission reported back and concluded that in fact the estimate was valid and in fact the case was stronger even than the publicly presented information. That was a commission that was headed up by Mr. Robert Gates, the former Director of the CIA under then first President Bush. That report was not made public until December 1996, after the Presidential election, but again this was now the third assessment in a row that it found that the ballistic missile threat while serious was not urgent.

The Congress then appointed another commission and this was the commission that came to be known as the Rumsfeld Commission that came back with a very different assessment in 1998, that found that there was a threat of a third country, specifically Iran, Iraq or North Korea, developing an ICBM, missiles that could hit the United States with little or no warning, that we might not know when a country was doing this and we would wake up when it was too late. That report was actually criticized by the Joint Chiefs of Staff. They did not agree with the conclusion of the Rumsfeld Commission. But nonetheless, those views and those methodologies came to be adopted by our Intelligence Community, and that produced in 1999 the first national intelligence estimate that corresponded with the Rumsfeld conclusions and found that in fact there could be a possibility of a threat from North Korea, secondarily from Iran and possibly from Iraq.

And I believe they, just to sum up, that these national intelligence estimates are wrong, that they overestimate the threat and they reach these conclusions by basically changing our standards of how we judge the threat, that they lower the standards by which we would judge a ballistic missile to be threatening the United States and seemed to indicate that there was some dramatic new threat when in fact they were assessing the programs that we had known about all along but now we're judging them in a different way.

Specifically, they changed the range from an attack on the continental United States, which had been all other assessments, to one on any part of the United States. And the difference between, for example, Seattle and the tip of the Aleutian Island chain is 5,000 miles. So it meant that a medium range missile could now be a threat to the United States.

Changed the time line and several other factors that you could go into if you would like; most of all focused on the developing missile threat from these three countries and did not do a global assessment of the overall situation with ballistic missiles which, as the report that I've submitted indicates, is actually declining and declining dramatically by most criteria.

Mr. TIERNEY. Thank you, Mr. Chairman. I know that you had a question. I yield to you whatever time I have. I have to run.

Mr. SHAYS. I would just like to have a full response to that question if you want to stay here. It could be your time if would you like. Yes, Mr. Bremer.

Mr. BREMER. I have to say that I'm not an expert on ballistic missile technology, but I also don't have the confidence of my copanelist in predicting the future. I'm a historian. Historians are students of discontinuities. I'm always very uneasy when people make straight line projections. It seems to me there are two relevant points about the ballistic missile technology.

First is we've just seen one of the most extraordinary failures of American intelligence in our history on September 11th. During the 1990's, people who didn't know what they were talking about predicted confidently that in fact the threat of terrorism was declining and in fact it was increasing. At the end of that decade we had one of the most extraordinary failures of intelligence. So anybody who stands today and says that he is confident that he knows

that we will have warnings it seems to me is ignoring the experience we've just seen in the last year on a very important issue, in this case terrorism.

Second point is more the historical point. One can of course list today the States which have ballistic missile technologies and might under some conceivable circumstances want to use that against the United States or threaten to. Attorney General Meese mentioned several of those countries in the previous panel. What one cannot say is what the world is going to look like 10 years from now. So even if you accept the original Woolsey panel assessment of 1993 that we did not face a threat for 15 years, I remind you that's only 6 years from now. I don't know how long it's going to take to develop ballistic missile technology. I know we have to develop it. I don't think it is prudent to assume that we will have warning. I think we've already seen 9 of the 15 years even by the Woolsey definition that have gone by.

So I fully support the deployment as soon as it is practicable of ballistic missile technology and, as Mr. Meese pointed out, technologies which are—would be available to not only protect America and its homeland from Hawaii to Maine but also to protect our allies and our troops stationed abroad.

I think the fact that five of the seven States which support terrorism, five of the seven have ballistic missile technology today, should be a rather sobering reminder to Members of Congress about the importance of this area.

Mr. TIERNEY. That said and having stayed for it——

Mr. SHAYS. You have 5 minutes.

Mr. TIERNEY. I do have to run. I want to make a point. I think what we're talking about is assessing threats and prioritizing them. That's the real key here. If we're going to go out on some untested system that has been nothing but failures pretty much, unless we expect we're going to have a missile sent out of the country instead of in with a beacon on it three times the size of what's there with no decoys or whatever, we're putting our priorities for what is anticipated.

What is anticipated by most accounts of reasonable people is that we will see more terrorism acts along the nature of what we have experienced so far, or things like that, well before we'll experience a long range ballistic missile that is big enough, powerful enough, accurate enough and able to carry the kind of payload to be concerned. So as we prioritize those things, that will be a little further down the line. That's what we have to spend our money on is the things that hit the top of the line first and then test the system, instead of starting to build the thing before it even gets tested.

Thank you, Mr. Chairman. Thank the witnesses.

Mr. SHAYS. The question I wrestle with, and that is why would someone send a missile when they can just put it in a suitcase.

Mr. CIRINCIONE. In fact, in the latest national intelligence estimate, this is what the intelligence agencies conclude. They conclude that it is more likely that the United States will be attacked by a weapon of mass destruction by nonmissile means; that is, by ship, plane or truck. So they do make that assessment that the nonmissile means of delivery is more likely than missile means.

Mr. SHAYS. But I wrestle with Ambassador Bremer's comments as well. Because I realize that anything I do really has impact 10 years from now. So we have to anticipate 10 years from now. So my own view based on the hearing we've had is that you continue the development but you don't—excuse me—the research and continue to try to improve the technology but then you don't yet proceed to go into production. It's kind of how I sort it out myself.

Mr. CIRINCIONE. I would agree with that, sir. I think that's a prudent course. What we're talking about here is balance and priorities. How far money goes to these efforts, how much priority, how much diplomacy, how much of our senior leader's attention goes to this particular threat as compared to all the other threats that we face.

Mr. SHAYS. Yes. Mr. Hinton.

Mr. HINTON. As you well know, one of the key recommendations we made last year was for the focal point being Governor Ridge's office that the President appointed him to to oversee the development of a national threat and risk assessment. That would bring to light all of the diffused threats that your Nation would face in the future and go through the assessment of the threat, look at the various vulnerabilities and look at the criticality assessments of our infrastructure and try to lay those out so that we could see everything and how they stack up, so that would help us direct where we need to put the resources.

We still believe that recommendation has merit. We have not seen that implemented yet. And we continue to stand by that because we think it is very important for the oversight purposes of the Congress, as you are overseeing the expenditure of all of the money that we are making available for homeland security.

Mr. SHAYS. I will give Mr. Kucinich 10 minutes and then go to Mr. Otter and I. But I will just tell you where I want to use my 10 minutes. I want to—I am going to real religion on this issue of knowing what the threat is and developing the strategy because we had too many hearings before September 11th when we were told we need to do it. And I don't—I see more the strategy being developed before we know what the threat is. I am going use as the basis of my question Ambassador Bremer's comments about—instead of the strategy of wait and respond, I guess before that is prepare, wait and respond. We need to have one that is prepare, detect and prevent.

I am going to ask it based on what threat and—but that will be my time after my two colleagues have gone. Mr. Kucinich, you have 10 minutes. We will do it in two 5-minute lots just so you see it happen.

Mr. KUCINICH. Thank you very much. I thank the witnesses. Mr. Cirincione, I wanted to thank you for your testimony. I thought your piece in The Washington Post was breakthrough.

Contrary to what we have been hearing in the last few years, it appears that the threat of intercontinental ballistic missiles has actually decreased over the last decade, rather than increased. I want to go back to that. Is that fairly stated?

Mr. CIRINCIONE. Yes, it is, sir.

Mr. KUCINICH. I took the liberty of copying the chart that accompanied your piece. I mentioned it earlier. Would you mind briefly

running through that for the benefit of the subcommittee? It is basically divided into two timeframes, the situation in 1987, the situation today; is that right?

Mr. CIRCINCIONE. Yes, it is.

Mr. KUCINICH. What does each of those rows represent?

Mr. CIRINCIONE. The hours on the end—the hours on the end represent the trend lines. What I tried to do was assemble the various criteria by which anyone would judge a ballistic missile threat, and then try to assess where those criteria were going, what was the trend line.

And, you know, I am obviously inviting others to bring in their own criteria. What other standards should we use?

Mr. KUCINICH. So when you put all of this——

Mr. SHAYS. Let me ask the gentleman to yield. Do the other panelists have a copy of this? I would like you to be able to look at this to be able to respond as well.

Thank you.

Mr. CIRINCIONE. Would you like me to go through it? What is the biggest threat that we face? Intercontinental ballistic missiles. There are only two countries in the world right now that can threaten the United States with long range land-based intercontinental ballistic missiles: Russia, which has thousands of them, and China, which has about 20.

If we go back 15 years, where were we 15 years ago? I picked 1987 because it was one of the peak years of the cold war and it was before arms control treaties started reducing the ballistic missile threat. Fifteen years ago there were 2,384 long range ballistic missiles threatening the United States. Now there are 1,042. All but 20 of those are Russia's.

Mr. KUCINICH. So the real concern, in terms of threat assessment with respect to threats to this country——

Mr. CIRINCIONE. To any part of this country.

Mr. KUCINICH. China.

Mr. CIRINCIONE. China. Russia. Those are the only countries that can hit us with an intercontinental ballistic missile currently.

Mr. KUCINICH. So based on your studies of threat assessment, have you seen any circumstances which would suggest that either China or Russia would initiate an attack on the United States, a missile attack?

Mr. CIRINCIONE. No. That is an extraordinarily unlikely event.

Mr. KUCINICH. In concert with that, how does that then fit into a newly enunciated U.S. policy of first use or first strike, which it appears some of our panelists have advocated?

Mr. CIRINCIONE. If you are referring to the recommendations of the nuclear policy review—-.

Mr. KUCINICH. I think the word is posture.

Mr. CIRINCIONE. The nuclear posture review, there are recommendations there that the United States develop a new generation of smaller, more usable nuclear weapons for a wide variety of contingencies against States that have weapons of mass destruction, or that might present us with a surprising military development.

Mr. KUCINICH. How does that square, though, with the realities of the situation?

Mr. CIRINCIONE. In this case, there is no correlation between the two facts.

Mr. KUCINICH. Elaborate. What do you mean there is no correlation? Could it be fairly stated that this policy that has been enunciated and elaborated on in the nuclear posture review has no basis in reality that we should—that the United States should take a position of advocating first strike?

Mr. CIRINCIONE. These are two slightly different areas. But there is no justification in an assessment of the threats from ballistic missiles that would warrant the United States changing its nuclear doctrine at this point.

Mr. KUCINICH. And if other—is it possible that other countries that have weapons of mass destruction right now, intercontinental ballistic missiles—you talked about China and Russia who have them right now. How would the threat assessment change if they suddenly adopted the same policy of the United States?

Mr. CIRINCIONE. Well, this is always a very good test of our policy. How would we feel if other countries announced, for example, if they were developing a new generation of smaller nuclear weapons and were intending and developing a doctrine for use? I don't mean just a rogue nation, but India, for example.

Mr. KUCINICH. How does this change the threat index?

Mr. CIRINCIONE. That would substantially increase your risks of nuclear weapons being used in combat and significantly increase the chance of other countries acquiring nuclear weapons. So it would be a more dangerous world if other countries adopted the kinds of policies that are being recommended by this policy review. I think it is unquestionable that it would lead to a more dangerous world.

Mr. KUCINICH. So those policies actually increase the threat to this country?

Mr. CIRINCIONE. I think they do, sir. That is why I think this is a dangerous set of recommendations, and I hope that the senior leadership of the administration sends this report back for revision, and that Congress gets involved in this discussion. This is a very, very dramatic change in U.S. nuclear policy. It should not be a change that is made by the——

Mr. KUCINICH. I would like to say here in this hearing, as the ranking Democrat of one of the subcommittees involved here, that I think it is urgent for Congress to get involved in this, because the whole calculus of threat assessment is being used as the basis for building missile defense systems and spending billions upon billions of dollars for homeland—so-called homeland defense. And yet at the same time, those policies enunciated in the nuclear posture review put the United States in much graver danger than the United States was in prior to those policies being enunciated.

Mr. CIRINCIONE. It does get back to the chairman's main point here, that some of those strategies and policies are being developed before a concrete threat assessment.

Mr. KUCINICH. I would like to go one step further with that. This is not a particularly partisan statement, because I challenged the Clinton administration on a number of its foreign policies. But I think that—the fact that the potential first use of nuclear weapons—and when we talk about first use, not against necessarily gov-

ernment actors, but against their people, that the fact that can be blindly discussed anywhere is the height of immorality, and whatever administration, at any time, to throw that stuff around as though it is—as though it is just casual locker room banter, snap the towel, no, you know.

I am looking here at one of the witnesses—a new strategy must be to detect and prevent attacks before they happen. Well, on one level that could be acceptable. But if you are talking about—if that is translated to nuclear first strike, just putting that out there, it is immoral. That is all. It puts the United States in a position of telling the whole world to go to hell. And that is not a way to conduct world affairs.

You know, I am just stopping the music here for a moment to focus on this, because, you know, we can talk about all of the threats that Governor Keating is familiar with, and we can talk about the Heritage Foundation's report, which has a lot of interesting information that might be of real value. But when we get into a discussion here where we are actually talking about the first use of nuclear weapons, and making that a new doctrine, people are playing with the Apocalypse, they are playing with doomsday scenarios, and it has to be stopped. It is not an acceptable part of a dialog in a civil society. It is basically insane, and it needs to be challenged. And this is just one Member of Congress here. But whatever needs to be done, needs to be done nationally and even internationally to stop this descent into this maelstrom of chaos which is brought about by loose talk of a nuclear first strike.

You know, I saw the movies about the Cuban missile crisis, and I saw the discussions that people had about their children and their grandchildren. This is just not acceptable. So if there is anybody here even remotely connected with the administration, they should just know that there is going to be efforts made to start a national movement to repudiate this first strike dementality.

I don't have anything more to say.

Mr. SHAYS. I just want to point out that the comments of first strike, we are not even quite sure where they are coming from, or any validity. I hesitate to even speak about them, because I don't give them much credibility, but I would welcome any comment that anyone else wants to make on this issue before we go on.

Mr. KUCINICH. Would the Chair yield?

Mr. SHAYS. I just want to make sure that the full panel responds.

Mr. KUCINICH. Would the Chair yield for a question?

Mr. SHAYS. Sure.

Mr. KUCINICH. I spent some time Sunday watching members of the administration on talk shows try to explain the administration's position that was stated in The Los Angeles Times story, and I didn't see anything that repudiated the United States or what sounds like very strongly United States' position with respect to first strike.

You know, they may have backpedaled about whether or not the circumstances would come up, but they basically have said there would be a reservation of the right. And I am saying, so to be very clear about what I am saying here, that it is immoral to let that kind of talk go out there, about reserving the right for a nuclear first strike, and particularly—I mean you look at these threat as-

sessments, there is no justification for it even technically, let alone getting into the morality. Thank you.

Mr. SHAYS. What I listened to was a very cautious response and no—no real acceptance that those reports were accurate, other than to say that all administrations have had to look at all options and had to respond to all options as a possibility.

Mr. KUCINICH. Well, further asking the Chair for his indulgence, no administration has been confronted with these set of circumstances, nor has an administration ringingly rejected the comprehensive test ban treaty, the antiballistic missile treaty, talked about building a national missile defense, building bunkers they have people hiding in. I mean what signal does that send to anyone? And then you also have this loose talk about a first strike. I mean we are—you know, somebody is screwing around with the end of the world here. And I think that it ought to be called for what it is.

Mr. SHAYS. I am afraid they are the terrorists that are screwing around with the end of the world.

Mr. KUCINICH. We need not copy them with our mentality.

Mr. SHAYS. OK. Let me just invite the panel to respond to any comment.

Mr. LARSEN. Yes, sir. In my statement there was discussion of preemption, but there was no discussion of first use of nuclear weapons. I think that has been a long-standing policy of the United States. But one of the things that has to be discussed is we sat in here in July and talked about the Dark Winter exercise. There are nations out there that we believe have smallpox, which in many respects could be worse than a nuclear strike on this Nation.

North Korea and Iraq are the two that I am greatly concerned about that can cause significantly more loss of life. People I talked to at CDC and Johns Hopkins who have studied this for years tell me it could take this Nation beyond the point of recovery. That is a serious threat to our national security. It is not the highest probability, just like when we talked about national missile defense, is that the highest probability? No, but what are the consequences? I think we have to look at it.

The Gilmore Commission looked at low probability—I mean high probability, low consequence truck bombs. I don't lose a lot of sleep over those. Those are personal tragedies, but those are not threats to our national survival. I think reevaluating some of our issues such as preemption, as I had talked about in my statement, had nothing to do with nuclear weapons; that we need to send a very clear message to those who brought about September 11th attacks on this country and those out there who have capabilities to bring even more severe attacks, that the United States takes this very seriously, and we will respond as necessary to protect our Nation.

Mr. KUCINICH. Do you advocate that the non-state actors, that we respond to them by attacking the States from which they come?

Mr. LARSEN. I think we should attack the actors. Thirty-two years in the military as an Air Force pilot. I dislike nuclear weapons probably more than you do. They are terribly—they are a terrible weapon. You know, the idea of dropping a nuclear weapon on Baghdad is preposterous, and kill 2 million people. I will agree with you on that point. But I tell you what. I want to make it very

clear to anyone who thinks that they will launch further attacks on the United States that we don't take anything off the table, and if you attack our Nation with something that could threaten the very survival of this government, we should take nothing off the table when we talk and think about that response. And you were talking about, oh, we are building bunkers out here in the mountains. Those were built in the Eisenhower administration. That program has been around—I worked in that program——

Mr. KUCINICH. Did we have a separate administration set up?

Mr. LARSEN. We have no separate administration today. There are different levels of alert, just like we have—you mentioned the force protection levels, Alpha, Bravo, Charlie and Delta. At times of higher threat, and I think we are in times of higher threat right now, I am happy to know that there are some folks out there. Whenever we have——

Mr. KUCINICH. Congress would have been happy to know, too.

Mr. LARSEN. Whenever we have a State of the Union address, we don't put the whole leadership team in one building.

Mr. SHAYS. Let me give the time to Mr. Otter, but just say that this committee has no doubt about the reliability of information that has come to us that said terrorists have chemical, biological, potentially radioactive material, and has sought to get nuclear weapons. And we basically have heard testimony that says we are in the race with terrorists to shut them down before they shut us down. But I am pretty clear about one thing, the fact that we are concerned about the potential of a nuclear attack on the United States. It won't be by missile, it will be by suitcase or truck or something else. It is real. And we tell the American people the truth and then they respond by telling us what they want to do. That is in fact the truth. And I just want to make this point. It would be absolutely inexcusable for this administration not to anticipate that possibility and act on it.

Mr. KUCINICH. Well, let me ask the Chair a question then. I am not going to dispute your scenario with respect to a suitcase, but I heard seven nations named in the nuclear posture review now. They weren't talking about suitcases.

Mr. SHAYS. I agree with you. But I am just responding to your whole point of why we have a government, somewhat a shadow government in exile. Let me give Mr. Otter 10 minutes.

Mr. OTTER. Thank you, Mr. Chairman. I hadn't intended to continue with this sort of discussion, but I guess I will because the Rumsfeld Report, I think, brought a lot of things to light.

Now one of the previous questioners mentioned the greatest key to this whole discussion is the question of assessment. And I think the greatest danger to this whole discussion and this hearing that we are having today is to focus ourself so much on one potential threat as to ignore at our peril the rest of them.

We did focus on a missile defense, obviously to the extent of ignoring potential terrorist threats, and those did not come without warning. You know, when you think back in the previous administration, when the al Qaeda organization led a strike against the World Trade Center, also against the Korban Towers, two embassies in Africa, and then against the USS Cole, and I would ask you and I would ask the ranking member, I suspect that is it worse to

warn about potential threats and make necessary assessments and prepare for those than it is to let those four attacks against this country go on except for to—over an 8-year period, except to bomb an aspirin factory in the Sudan and deny those people an opportunity to get over a headache.

No, I think it is much more dangerous to focus our assessment on just one area to the exclusion of the other. And let me go on record as saying that I do not believe it is immoral for this country to prepare for its survival. And if that survival includes assessments of other countries' abilities to attack us, I think we need to know that.

But having said all of that, I guess my question then would go to—relative to those assessments or relative to those attacks that came over the last 8 years, is there any reason to believe that those won't continue? Is there any reason to believe that perhaps those targets will come closer and closer to the Western Hemisphere? And if there is, instead of attacking the embassies in Africa, perhaps we need to have more assessments of the attacks that are possible on our own homeland. I think that is where this discussion really ought to go.

And if we fail to respond in kind, as we did in those four instances during the last 8 years, can't we just expect to continue to be chipped away at to a point beyond irritation, and a reoccurrence of September 11th? If you will, panelists, respond to that. Mr. Ambassador.

Mr. BREMER. The consensus of most people who look at the terrorist threat in the government, out of the government, here on the Hill, is that what we saw on September 11th was the logical if horrible extension of a trend that was visible throughout the 1990's.

I know of no one who thinks that trend will diminish. Most of the analysis—and I think my commission was the first one to point out this problem in June 2000, when we pointed out that we thought there would be mass casualty, mass destruction attacks in the United States on the homeland, and we reported in particular to the dangers we associated with the possibility of chemical and biological, particularly biological attacks.

I have been involved one way or the other, for my sins, in counterterrorism now for almost 20 years, and I don't know of anybody who disagrees with that assessment. So I think it is prudent to expect that we will continue to see mass casualty attempts in the United States, and that it is the only prudent and, indeed, politically defensible thing for the administration in power to do, to do everything that it possibly can to prevent that from happening.

Mr. OTTER. Mr. Larsen.

Mr. LARSEN. I think our No. 1 priority, as I said in my statement, should be on deterrence. And we are seeing now, much different than in the cold war, but in this new era, the role that consequence management and crisis management plays in deterrence. We still don't know who sent those letters to Senator Daschle or to the news offices. Our enemies understand that. Whether that was some domestic terrorist, we don't know. But the international enemies we are most concerned about here, they understand how poorly we responded. We don't know who did it.

I think the most important thing is reestablishing that deterrence and the—the priorities that you spend—that we spend in the next couple of years are going to do that. What money is in the current budget for attribution?

Mr. OTTER. Mr. Cirincione.

Mr. CIRINCIONE. Thank you. I think the war in Afghanistan, which I strongly support, is a very powerful deterrent. Perhaps al Qaeda thought that they could get away with this. Perhaps they thought that they could provoke the United States and it would result in U.S. involvement in the Middle East that would trigger the Jihad that they sought. They were sadly mistaken. I think any terrorist group that thinks that mass casualties in the United States are somehow going to accomplish their purpose now has to think at least twice about that.

As to the threats we face in the near term, I again defer to an international expert on this, the testimony of Vice Admiral Thomas Wilson, the director of the Defense Intelligence Agency. This February he lists again his top concerns, and right at the top is still a major terrorist attack against U.S. interests here or abroad. Second on his list is escalating violence in the Middle East. He goes on to worry about a war between India and Pakistan, widespread violence against U.S. citizens and interests in Colombia, and other factors, including the dangers of ballistic missile attack. It is a very comprehensive assessment.

He also goes out of his way to emphasize some of the contributing factors to global instabilities, such as demographics and economic dislocations. He talks about resources shortages in many parts of the developing world. The danger—I think where we get into trouble is not that we don't listen to those assessments, but we then pick and choose the threats that we want to respond to. That is a problem. We are clearly having a problem as a Congress, as an executive branch, as a Nation, prioritizing the threats that we face, understanding how to allocate the resources. And my simple message is that I think we misallocated our resources in the past.

We have to correct that imbalance. We have to put our money where our threat assessments are.

Mr. OTTER. Mr. Hinton.

Mr. HINTON. Mr. Otter, our work has largely focused on the process, if you will, and I don't know if I can add any more than what I said earlier, which was picked up in the letter of—the bipartisan letter that went from this committee over to the President seeking a threat-and-risk assessment in this whole area to try to take stock of what the threats are and to come up with a balanced portfolio against those. So I think that is the process that needs to unfold. That has been the subject of the recommendation and our reports where we are looking to Governor Ridge to oversee that process, that will provide that information to help you all in your oversight capacity.

Mr. OTTER. Much has been said about the cold war, and the result of how the cold war came about. I happen to be a student, not a disciple of, but I happen to be a student of the notion that when the Manhattan Project was put together, had equal enthusiasm been in place, an equal study, an equal deliberation on what would

happen if they were successful, if that had paralleled the efforts of Oppenheimer and the rest of the folks to make that major weapon of mass destruction, and we had known, and that assessment been made then, 1945 would have seen the total control under one government. That one government would have been the government that invented it, and they would have had the assessment that if anybody else gets their hands on this stuff, this knowledge, we could be in for a 50-year cold war, which is exactly what happened.

So we need to study these things, not only—and deliberate them in their total vision, in our total vision of assessments of danger to this country, but also I think we need to assess at the same time is what happens if we are successful.

I thank you, Mr. Chairman. I yield back the balance of my time.

Mr. SHAYS. Thank you. I have a number of questions. I want to get right to it. I was kind of thrown for somewhat of a loop, Mr. Bremer, when you talked about 1947. And I am realizing that there must have been two parts to getting our act together, under Truman putting the Pentagon together, basically building it, creating this force structure, and then the strategic must have been what happened in the Solarium Project. But I don't feel that we can wait 5 years to resolve this. I am getting very, very nervous that—we continue to talk about strategy before we have this kind of assessment of the threat.

I want to—maybe I get some comfort in you kind of making what seems complex seem kind of simple to me. I want you to elaborate a bit on the wait-and-respond versus the detect-and-prevent. What is our strategic strategy? We had to be prepared, correct, but it was basically—it was a deterrent, we waited and we responded.

Talk to me a little about detecting and preventing. That is a strategy, right?

Mr. BREMER. Well, it is a posture or a strategy. I think that obviously it is a bit—it does somewhat oversimplify to argue that all we did was wait and respond, because before September 11th, we also had programs to try to detect what terrorists were up to and to disrupt their plans before they could attack. But as the Bremer Commission pointed out, as the Gilmore Commission pointed out, as a number of other studies have shown, over the last decade our intelligence abilities have deteriorated because the intelligence agencies had adopted a sort of—or had acquired a risk-averse culture and we were not out aggressively enough going after terrorists because our general posture was the terrorists would attack and we would then try to figure out how to respond.

That was certainly the case, as Mr. Otter just pointed out, during the four major incidents that he referred to in the last decade.

What I am saying is that the threat posed by terrorists today and their new motives is such that we simply cannot afford, it is not morally or political acceptable to say to the American people, I am going to wait now for the terrorists to get their hands on this bad stuff, because we are talking about not 3,000 people being killed or 30,000 or even 300,000. It could be 3 million people. If it is the case of smallpox, as Colonel Hansen pointed out, we could be talking about tens of millions of people.

So the stakes are so high now the government cannot get the strategy wrong and the government cannot get the organization of

the Federal Government wrong. We don't have that margin. We don't have 5 years, as you pointed out.

Mr. SHAYS. It strikes me, though, that one of the key things that this President has done—and I think most of his success is, you hold the country responsible that allows the terrorist activity to grow and prosper in that country. And the reason I am struck by, from all of our hearings, is that basically cottage industries can create weapons of mass destruction within a border and wipe out humanity as we know it, as relates to biological.

What I am also struck with, though, it seems to me that what—as we sort out this threat and we develop a strategy, and I open it up to any comments from any of the panelists, that we may have to act unilaterally if in fact our strategy is to detect and prevent, we are not going to wait to—I mean there was this great cartoon one time showing Soviet tanks in Washington, and Congress was meeting, and we—you know, we finally decided to declare clear war against the Soviet Union in this scenario.

It strikes me that we can't wait, if we are going to detect and prevent, and that may require us to act unilaterally. And I will throw it open to any—I will start with you, Mr. Larsen, and then go to you, Mr. Bremer.

Mr. LARSEN. Yes, sir. I think after a truly major attack on the United States, there would be no debate whether we would act unilaterally or wait for some sort of coalition. Perhaps we should look at that first. The line between unilateral operations and leadership is sometimes very thin. I remember January 10, 1991, polls in the United States, even here, domestically was not in a favor of starting the war in Iraq. President Bush started it, thought it was the right thing to do. Three days after the air war began, all of a sudden the American people, like 75 percent, said, yeah, it was the right thing to do. That was leadership.

I think when we see some of the problems, like with the biological warfare convention—I wish we had a better treaty, arms control regime for biological weapons. They scare me more than anything else. But I don't think we should sign up to something that won't work. We had the most intrusive inspection regime going on in Iraq——

Mr. SHAYS. Let me go to the next, if I could. Mr. Cirincione.

Mr. CIRINCIONE. I think there are a number of circumstances where the United States will have no choice but to act unilaterally, particularly in situations such as were just described. I think that should be, unless it is time-urgent, that should be our last option. It is always better when the United States acts in concert with their allies and friends. The 1991 Persian Gulf War is an excellent example of that. That is why Vice President Cheney is out in the region again.

Mr. SHAYS. I put one caveat, though. There was basically an agreement in order to get that unification, that we weren't going to go into Bagdad. And this—this White House isn't going to—I am pretty comfortable in saying that, because I just remember in the dialog with the President, the former President, getting this Peace Corps volunteer to vote for war, he was saying, you know, we have an understanding, we are going to Baghdad. That was no secret. We didn't.

I mean, at least that is the way I always assumed it as I dialogd with the White House on this.

Mr. CIRINCIONE. There are a number of things that we probably should have done differently at that end of that war. Whether going into Baghdad would have solved the problem is unclear. But you could go into lots of things. For example, allowing Iraq to keep flying helicopters. Allowing it to keep building short-range ballistic missiles, not having a no-holds-barred inspection regime. There is a whole lot of things that we should have done differently.

Mr. SHAYS. Mr. Hinton, and then Mr. Bremer.

Mr. HINTON. Chairman Shays, that is a policy realm for which I don't feel qualified to answer that.

Mr. SHAYS. Well, you are qualified, but you are wise not to answer it.

Mr. BREMER. I don't think there is any question we have to be—the President has to be able to act unilaterally. Of course, it is better to have some friends along with you. As Winston Churchill said, the only thing worse than fighting with your allies is fighting without them. But there will be times when people won't come along with us and we will have to go along on our own.

Mr. CIRINCIONE. But when that happens, it should give us pause. We should think about why it is that no one else would agree with us, and maybe we should be rethinking our policy or our priorities.

Mr. SHAYS. Continue.

Mr. CIRINCIONE. Well, the case of Iraq is much in the news. You know, Iraq doesn't show up on most threat priority lists. It isn't in Admiral Wilson's list. Is it a danger? Yes. Would we all be better off if Saddam Hussein were not in power? Yes. Should it be our No. 1 priority? Should we subordinate everything else to that effort?

Mr. SHAYS. I am nodding my head and saying yes, because I don't know what reports you are looking at, but the basic information I get that isn't classified is three to 5 years he has nuclear weapons. This is a regime where basically heads are in pickle jars and a regime that has used chemical weapons to destroy 30,000 people in almost a day's work. So it shows up on my radar screen.

Mr. CIRINCIONE. I think we can separate regime change from acquisition of weapons of mass destruction. It is not necessarily so that we have to remove Saddam Hussein in order to prevent those programs from advancing, nor is it necessarily so that if we do, that the next regime would not pursue those capabilities. And that is part of the reason I think why the United States is trying its best to explore options through the United Nations of reestablishing the inspection regime. That may be ruled out. Iraq may make that impossible. He may give us no other choice but to once again engage in military action.

But that is why it should be a last choice, not the first choice.

Mr. SHAYS. When we try to determine the assessment of threat, I am struck by the fact that the threat is so different and has so many parts compared to this monolithic attack potentially from the Soviet Union. Is threat assessment, going back to the 1950's, much easier than threat assessment now, or it is basically the same process and it shouldn't be any more difficult?

Mr. CIRINCIONE. Let me just start this process. It is much more difficult now. There is no question about it. There is a little bit of

historical revisionism going on where we now remember the Soviet Union as this almost benign predictable deterrable foe. That is not how we saw the Soviet Union at the time. And you, sir, got involved in many hearings where we started off with a very concrete threat assessment of a Warsaw Pact invasion through the Folder Gap.

Mr. SHAYS. There are bomb shelters all over my district.

Mr. CIRINCIONE. Sir, we all did duck-and-cover drills. This was very scary times. We engaged in numerous diplomatic crises, we spent hundreds of billions of dollars to deter the Soviet Union attacks. Now we have a less concrete, more diffuse, somewhat less predictable threat, and it requires a lot more analysis and many more tools. If you just look at Admiral Wilson's testimony, he talks a lot about the underlying forces that generate global instabilities and how we have to deal with them, and it is a much more complicated political, military, economic, diplomatic issue than a straightforward military threat assessment.

Mr. SHAYS. The bottom line, deterrence doesn't mean much, it strikes me.

Mr. BREMER. I agree that the threat assessment is more difficult. I think one of the problems, Mr. Chairman, that we all have to grapple with, in some ways we are all still thinking of this in cold war terms as if threats were quantifiable, you know, how many SS–20's does the Soviet Union have? Where are they deployed? What is the order of battle for the Red Army? These are all very tidy things, difficult to get your hands on it, but once you do get your hands on it, you can do the threat assessment.

As my colleague said, the threat is so diffuse now, it comes from so many directions, and it is potentially in many ways even greater than it was at the height of the cold war. We have to, I think, not—I think you would make a mistake, it seems to me, in Congress to say we need a very precise threat assessment before we can do anything. You are not going to get that. The threat is so different.

America's vulnerabilities are essentially infinite. You cannot start with the vulnerability analysis, because with the country of 283 million spread across the continent and halfway across an ocean, our vulnerabilities are essentially infinite. So, of course, you have to have some sense of the threat in order to determine priorities, which is the theme that the ranking member has made and others have made here. Absolutely correct. But let's not get ourselves into the mindset that it is going to be the way it was in the cold war, that a threat assessment is sort of almost a mathematical thing. It is not going to be that easy.

Mr. SHAYS. Before I give the floor to Mr. Kucinich, though, don't you need to know what the threat is before you develop a strategy?

Mr. BREMER. I agree. I am saying let's be careful when we get to the issue of quantifying the threat.

Mr. SHAYS. But we still need to know the threat to develop a strategy.

Mr. CIRINCIONE. I think it is quantifiable. I think it is knowable. It is not completely unpredictable.

Mr. LARSEN. It was much more capabilities we looked at in the cold war, our intelligence community, and they are still focused on

that, counting missiles and armor divisions. Now it is more intent that we are worried about.

Mr. HINTON. Chairman Shays, I would like to add I agree, too, that the threat is more complex, it is diffuse. But key to this, I think, is understanding all of the complexities around the different threats out there before you come up with the strategy.

Mr. SHAYS. Mr. Kucinich, would you like the floor back?

Mr. KUCINICH. Yes. The Chair raised a very good point here, first know the threat before you look at the strategy, because otherwise we end up in, you know, Alice in Nuclear Land. You know, first, the strategy, then the threat.

And that seems to be some of the case of what is going on here, Mr. Chairman. I want to call to the committee's attention an article from January 11, 2002 in The Washington Post, "U.S. Alters Estimate of Threats, Non-Missile Attacks Likelier, CIA Says." And the first paragraph of the article says, "The United States is more likely to suffer a nuclear, chemical or biological attack from terrorists using ships, trucks or airplanes than one by a foreign country using long range missiles, according to a new U.S. intelligence estimate."

Mr. SHAYS. Doesn't everyone, everyone, basically agree with that point in the short run?

Mr. CIRINCIONE. Yes, I do.

Mr. KUCINICH. Well, I am glad that there is concurrence among members of the panel. However, what we are seeing raised here with the administration is what Mr. Cirincione has said publicly is the elimination of the line between nuclear weapons and chemical and biological weapons. And we are also seeing a United States which is telling countries, as Mr. Cirincione has said, that changing the policy—that if they did not acquire nuclear weapons, we would not attack them with nuclear weapons. That policy is being abandoned. The concern that I have is that we are being, for some reason, pushed into a discussion about survival.

And, Mr. Cirincione, I mean anything in these threat assessments that you have seen, would they suggest that the very survival of the United States is at stake at this moment?

Mr. CIRINCIONE. No, sir, there is not, which is why it is a mistake to conclude that just because the threats are more difficult to analyze that therefore they are greater. I do not believe we are under—they are greater threats to the United States now than there was 15 years ago. Fifteen years ago we were talking about national survival. Five thousand Soviet nuclear warheads would have destroyed the country, in fact, the planet. We do not face that magnitude of a threat, thank goodness, today.

Mr. KUCINICH. Any of the panelists want to disagree with that, that the very survival of the United States as we know it is at risk at this very moment?

Mr. BREMER. I disagree.

Mr. KUCINICH. Do you want to explain?

Mr. BREMER. Well, I went through it rather at some length in my opening statement. I think it is now clear that terrorist groups, the ones we are most concerned about, have made it clear they have a motive of killing as many Americans as possible. Those groups

have tried to get and may have gotten hands on weapons of mass destruction.

Terrorists states, of which there are seven, five of them have got nuclear, chemical, biological programs and ballistic missile technologies. Some of those states could very well, and have already have close relations with some of the terrorist groups and could either make that kind of material available to them or use it themselves.

The use of a biological, a well-planned biological attack on the United States would absolutely threaten the survival of this country, no question about it.

Mr. KUCINICH. Mr. Cirincione.

Mr. CIRINCIONE. That is certainly a worst-case scenario.

Mr. BREMER. So was a nuclear attack by 5,000 Soviet missiles which you just admitted was a threat 15 years ago. That was the worst case? Was there something worse than that?

Mr. CIRINCIONE. No, there wasn't.

Mr. BREMER. Case made. If you want to look at worst-case scenarios? , that is it.

Mr. CIRINCIONE. In fact, Mr. Bremer, I think there is a remote chance that there could be a biological weapons attack that could kill millions of Americans. That is a terrible scenario. Previously we feared that kind of attack from states, and particularly from the Soviet Union, which had one of the largest biological capabilities in the world. They could have done that. Even so, even—granted that this is still a danger, I—I believe it was a much greater danger 15 years ago when those biological weapons existed in state hands with excellent delivery vehicles ready to be deployed.

What we are now worried about now is whether a terrorist group would do that. Terrorists do—are trying to acquire biological weapons. But so far they have been unsuccessful in developing or possessing a usable biological weapon. Does Iraq have biological weapons? Absolutely. Will they launch a biological weapons attack against the United States? It is possible. That is something that we have to worry about.

Mr. KUCINICH. Do they have the capability of intercontinental ballistic missile technology?

Mr. CIRINCIONE. No, they don't. They would have to bring it over on a ship, a plane, or smuggle it in a truck.

Mr. SHAYS. Would the gentleman yield a second?

Mr. KUCINICH. Sure.

Mr. SHAYS. I have some sympathy about the immediacy of whether we need to have a missile defense system. And on that I—I have some—but I just want to say to you, we have had witnesses before us, doctors of noted medical journals, and one of the last questions we asked, unprovoked, was, is there anything you want to say before we close?

He said my biggest fear is that basically a small group of biological specialists will basically create a biological agent that has no antidote, an altered biological agent that will wipe out humanity as we know it. And there was—there is a basic recognition, this is more than just a possibility. And the thing is, there is no restraint on them because there is no government that says we are not going

to do it because we don't want to go into oblivion. There is no deterrence.

So all of a sudden you just left me way off. I can't tell you how strongly I agree with—everything we have heard in our 25 hearings backs up what Dr. Bremer says. So you are kind of on one side here. I would love to have you come back again. But good grief.

Mr. CIRINCIONE. Is it possible? Surely it is possible. It is a question of how likely such a threat is. And there have been some very well-funded, very determined terrorist organizations, particularly Aum Shinrikyo, trying to do this, and they have failed to do it. It is a lot harder than most people think. Is it possible? Yes. Is it likely? I don't think so.

Mr. SHAYS. I am going to invite you back when we have some of those doctors here to respond. So I would love to get this hearing ended. I would love to give you an opportunity to close out.

Mr. KUCINICH. I would like to just—to kind of wrap up this discussion. We have—on this I spent a lot of time talking about the attempts to buildup a national missile defense system and the money that is being spent on that.

The Carnegie Endowment for the National Peace again in their bulletin on March 4, 2002 talks about how in January 2001 a special commission chaired by Howard Baker and Lloyd Cutler urged the administration to trim the money spent on securing and eliminating Russia's nuclear weapons and materials.

Cutler said, "our principal conclusions are that the most urgent unmet national security threats for the United States today is the danger that weapons of mass destruction or weapons-usable material in Russia could be stolen and sold to terrorist or hostile nation states and used against American troops abroad or citizens at home."

So it would seem that our money would be well spent in addressing trying to control the nuclear weapons and materials out of Russia. Furthermore, I think it would be important at some point for this committee to bring people from the administration in to go over this question about the prerogative for first use, because that has to be based on some kind of threat assessment, Mr. Chairman. And I have heard testimony here about the threat assessment with respect to China and Russia and the ICBMs. But the first-strike policy would not be consistent with that threat assessment with respect to ICBMs, and I just wonder why so many people are pushed into this survival mode with respect to ICBMs when others have testimony that there is other security problems that confront this Nation.

Mr. SHAYS. I understand the gentleman's concern. I figured it was a slow news day and it was a newspaper that got a story that would could have basically written any year in the last 20 years in terms of what we require in the military to do.

But I am going to call this hearing to a close. I think there have been some really important elements that you all have brought out, and I think every one of you has made a very fine contribution, and I thank you very, very much.

The hearing is closed.

[Whereupon, at 12:45 p.m., the subcommittee was adjourned.]

COMBATING TERRORISM: PROTECTING THE UNITED STATES, PART II

THURSDAY, MARCH 21, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:35 p.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Putnam, Weldon, Kucinich, Clay, and Watson.

Staff present: Lawrence J. Halloran, staff director and counsel; Dr. R. Nicholas Palarino, senior policy advisor; Kristine McElroy and Thomas Costa, professional staff member; Sherrill Gardner, detailee-fellow; Jason M Chung, clerk; David Rapallo, minority counsel; and Earley Green, minority assistant clerk.

Mr. SHAYS. I would like to call this hearing to order and to welcome our guests, and obviously, to welcome our witnesses.

For more than 10 years, we have been at war with transnational terrorists, but were unwilling to acknowledge and confront the unnatural menace inexorably creeping toward our shores. Today, while United States and coalition forces pursue the armies of terror abroad, we remain avoidably vulnerable to the next terrorist attack at home. Six months after lethal terrorism came to our shore through the skies and through the mail, we lacked the real time threat assessment, national strategy and organizational reforms long acknowledged as prerequisites to true homeland security.

Without doubt, the task is enormous. We are a mobile open society of more than 286 million souls living within 7,000 miles of open land borders and 4,000 miles of unguarded coastline. Public safety and public health systems are not well integrated. Critical transportation and information systems are susceptible to disruption. Intelligence sharing is stilted. Military capabilities have not yet been fully transformed to meet symmetrical threats.

Where to begin? It is a question of priorities. Until valid threats are culled from innumerable vulnerabilities, until a strategy is crafted to meet these threats and until governments are organized to implement the strategy, time and money will be wasted and lives put at risk as we lurch from crisis to crisis, or succumb to bureaucratic infighting and inertia.

Last week we heard testimony from a distinguished panel of experts who recommended a renewed sense of urgency to propel and

focus homeland security efforts. That momentum and steady guidance are supposed to be supplied by the Office of Homeland Security referred to as OHS, but there are indications that staff level coordination mechanism may not be strong enough to prevail in pitched turf warfare against entrenched interests in the agencies and in the Congress.

While we appreciate the briefing that we hoped to have this afternoon by Admiral Abbot, OHS deputy director, private discussions alone cannot answer questions so critical to public health and safety. So today we will hear from the Federal departments and agencies charged with key initiatives to protect the American people from terrorism. Their efforts, individually and collectively, have made the homeland more secure, particularly since September 11th, but the low-hanging fruit of homeland security has now been harvested. Unprecedented levels of coordination and cooperation will be required to reach the loftier but essential objective of a threat-based, strategically sound organizationally effective homeland security program. The question we ask our witnesses to answer, are we moving a pace toward that objective? We look forward to their testimony.

[The prepared statement of Hon. Christopher Shays follows:]

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
J.L. MICA, FLORIDA
JAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS

Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
CROC.NS@mail.house.gov
http://www.house.gov/reform/ns/

Statement of Rep. Christopher Shays
March 21, 2002

For more than ten years, we have been at war with transnational terrorists, but were unwilling to acknowledge or confront the unnatural menace inexorably creeping toward our shores. Today, while U.S. and coalition forces pursue the armies of terror abroad, we remain avoidably vulnerable to the next terrorist attack at home. Six months after lethal terrorism came to our soil through the skies and through the mail, we lack the real-time threat assessment, national strategy and organizational reforms long acknowledged as prerequisites to true homeland security.

Without doubt, the task is enormous. We are a mobile, open society of more than 286 million souls living within 7000 miles of open land borders and 4000 miles of unguarded coastline. Public safety and public health systems are not well integrated. Critical transportation and information systems are susceptible to disruption. Intelligence sharing is stilted. Military capabilities have not yet been fully transformed to meet asymmetrical threats.

Where to begin? It is a question of priorities. Until valid threats are culled from innumerable vulnerabilities, until a strategy is crafted to meet those threats, and until governments are organized to implement the strategy, time and money will be wasted, and lives put at risk, as we lurch from crisis to crisis or succumb to bureaucratic infighting and inertia.

Last week, we heard testimony from a distinguished panel of experts who recommended a renewed sense of urgency to propel and focus homeland security efforts. That momentum and steady guidance are supposed to be supplied by the Office of Homeland Security (OHS). But there are indications that staff-level coordination

mechanism may not be strong enough to prevail in pitched turf warfare against entrenched interests in the agencies and in the Congress. While we appreciate the briefing provided this afternoon by Admiral Abbot, OHS Deputy Director, private discussions alone cannot answer questions so critical to public health and safety.

So today we will also hear from the federal departments and agencies charged with key initiatives to protect the American people from terrorism. Their efforts, individually and collectively, have made the homeland more secure, particularly since September 11th. But the low-hanging fruit of homeland security has now been harvested. Unprecedented levels of coordination and cooperation will be required to reach the loftier, but essential, objective of a threat-based, strategically sound, organizationally effective homeland security program.

The question we asked our witnesses to answer: Are we moving apace toward that objective? We look forward to their testimony.

Mr. SHAYS. At this time, I recognize the distinguished gentleman from Ohio, the ranking member, Mr. Kucinich.

Mr. KUCINICH. I want to thank the Chair, and I look forward to our working to have a cooperative relationship on this committee. Now, despite doubling funding for homeland defense, despite asking Congress to provide $38 billion next year, unfortunately, we don't have the director here to come to the Hill and testify about this program. The Office unfortunately has ignored repeated recommendations from numerous sources, including the General Accounting Office, and even from this committee, to conduct a comprehensive assessment of the threats which may face this country.

This subcommittee has heard over and over again that to craft a coherent strategy to fight terrorism, the administration must begin with one job, conducting a comprehensive assessment of all the threats our country may face. The Office must gather intelligence from sources throughout government agencies, must evaluate the many different threats to this country side by side, and must place them in some sort of priority order. Otherwise, how do we know whether the $38 billion of taxpayers' money is being used productively? How do we know that an additional $358 billion in defense spending requested by the President will be geared toward programs which really do protect the American people?

The President's budget calls for 8 billion to be spent on missile defense in the year 2003, and 38 billion over the next 5 years, despite the fact that experts, including U.S. intelligence and military officials have concluded that the threat of a rogue state launching a missile at the United States is an unlikely scenario. Who decided that in this funding? What threat assessments were examined? This sort of analysis is important.

Mr. Chairman, we joined together in writing to President Bush last October when the head of Homeland Security was first appointed. Chairman Burton and Ranking Member Waxman also joined with us. This was an urgent call from all of us based on our many, many hearings on terrorism, recommending that the Office of Homeland Security determine what the threats are and prioritize them in a logical fashion.

As we said, this is the first step toward crafting a strategy toward allocating our budget resources properly. We have been informed that this office refuses to take the step. In fact, they are skipping the step altogether, plunging into writing a national strategy to be released sometime this summer. The Chair has said it, don't you need to know what the threat is before you develop a strategy? Of course you do. We all know that. GAO and the experts know that, but the Office of Homeland Security has not acknowledged it. But maybe that will change today.

So we must ask if the office is not basing strategy on a comprehensive assessment of the threat, then on what is it basing its decisions? I want to say I do have a lot of confidence in Governor Ridge. He is a fine public servant, someone who loves this country. He has served the people of Pennsylvania well, and I think he will serve this country well. I am confident that he can provide validated information, and I am confident that he can provide the intelligence. I am confident that he can provide analytical assessment. I am confident that he can provide well-crafted priorities.

Unfortunately, the Office of Homeland Security hasn't produced any of these yet. But I do have a lot of confidence and trust in Governor Ridge's intentions and in his ability.

Now, earlier this week the White House press secretary defended the administration's decision to keep the head of Homeland Security from testifying in public. He said, "this is an important line to draw and the President has drawn it." But it wasn't a line that was drawn when we saw the new alert system brought forward, and of course Congress has had no opportunity to bring questions to that. So I think we in this committee try to be careful not to let politics obstruct the pursuit of this Nation's security. Last year we heard from Joseph Sirinconi of the Carnegie Endowment for National Peace. He gave us some good advice. He said we need to find a way to depoliticize our threat assessments to come up with a national consensus on what the true threats are, and I would encourage this committee to see if it can't devise a way to get a global comprehensive threat assessment that is nonpartisan, nonbiased, removed from political agendas of the moment. This can help guide our budget, our diplomacy, and our policy.

Mr. Chairman, I think this is right on target. I want to thank the Chair for having this hearing and indicate to you I am pleased to be here and pleased that this is a public process. Thank you.

Mr. SHAYS. I thank the gentleman. At this time, the Chair recognizes Mr. Putnam.

Mr. PUTNAM. Thank you, Mr. Chairman. I also want to thank you for conducting this hearing, and I want to thank you for your leadership on all of the issues surrounding homeland security and terrorism and the threat assessment that this Nation has undergone and needs to continue to undergo, both prior to and since September the 11th. No other subcommittee has shown the leadership that you have shown as chairman of this subcommittee on these issues. No other subcommittee chairman has been as open or as bipartisan as you have been in searching for answers.

As the ranking member alluded to, there have been a number of joint letters, a number of hearings where under your leadership, you have gone out of your way to reach out to both sides that we may get to the truth. Unfortunately today the political agenda was in the driver's seat, and the political agenda was the message and not the truth and not the search for the best ways for us to secure our homeland security.

I am very troubled that we have been given an opportunity to hear from the Office of Homeland Security, and because of the political agenda and because of political high jinks, we are now at least two more weeks removed from having any information. I too am troubled by the reluctance of the Office to provide testimony to Congress. I would like to have more information about how the threat assessments are being made. I would like to have more information on how the budget requests were arrived at, but unfortunately, I don't have that opportunity now because the political agenda trumped the search for the truth today, and more importantly and more disappointing to me, Mr. Chairman, is that in the greater political game, and all of us are elected to Congress, none of us are naive when it comes to politics, but in the greater political

game, the most open, fair and bipartisan chairman in the Congress was trampled in the stampede, and that is what I regret the most.

So I look forward to the hearing that remains. I look forward to the testimony of this panel and the truth that hopefully is yet to come. Thank you.

Mr. SHAYS. Thank you. At this time I would like to recognize the gentlelady from California, Diane Watson.

Ms. WATSON. Thank you so much. Mr. Chairman, I too am here to gain as much information as we can relative to our plan, our design and our strategy for freeing this country from terrorism, sneak attacks, and securing the safety of our Members. However until we are fully informed, we cannot see the whole picture. It is regrettable that our administration chooses to not take us along and keep us as well informed as possible but there are other ways to seek the truth of the matter and I trust that under your leadership of the committee we will become knowledgeable. We all need to be partners in our national security.

I wish Governor Ridge well. I know he suffers from lack of resources and maybe lack of communication, but I do think communicating to us that which can be made public will not be a threat. I understand there are certain things that needed to be kept away so that our enemies don't know what we are planning but I think there is a broad overview that could be presented to us.

So I am hoping as a result of our hearing that we can make a positive impact on the administration and have somebody come and tell us what the plans are. We that appropriate need to understand and need to be part of that general planning. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much and thank you for that very articulate statement.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman. Mr. Chairman, we gather today to review the progress of goals and challenges made by the executive branch and its departments to develop a comprehensive threat and risk assessment plan. I think it is very important to state at the onset that from our constituents' point of view they do not want their Members of Congress to make this briefing and investigation a partisan fight that ostensibly erodes to name calling and finger pointing.

All of us are in this together. No one can escape or dispute the reality that there are vulnerabilities in our domestic assessment because of a lack of defined methodology. Like the constituents we represent, there are many political, religious and social persuasions present here today, all coming together to plan for a safer America through an agreed approach to homeland security. However, I am deeply troubled by the administration's ongoing over effort to thwart Congress from being a part of the solution.

Mr. Chairman, how will we, as Members of Congress, be able to give an accounting to our constituents of the moneys that are being requested by various Federal agencies without a comprehensive risk assessment plan in place? What methods will Federal agencies use to prioritize counter measures? How large is the domestic threat? And where will the next threat come from? How much time

will elapse before these questions can be answered? What or whom is being evaluated?

Like many Americans, I eagerly await Director Ridge's proposed national strategy in July. Supposedly, it will set clear objectives with performance measures supported by a crosscutting Federal budget plan according to the GAO. As the administration works to formulate its plan to be presented to the American people, I would suggest that a more expanded approach to its planning effort occur first. All future planning regarding domestic security should include Federal, State and local stakeholders.

I would also suggest, as Senator Lieberman has suggested in the March 19 letter to Director Ridge, that the following components be addressed in a comprehensive homeland security plan, methods to improve communications among the agencies and between the public and private sectors, methods to better coordinate response efforts among all responsible entities, methods to improve the resolution of conflicts between competing agencies and an improved comprehensive national strategy that identifies the homeland security responsibilities of all relative public entities. Then after careful consultation with other stakeholders, goals should be realistically set, threats identified and priorities proposed. And Mr. Chairman, I ask unanimous consent to submit my statement.

Mr. SHAYS. Thank you very much. Does anybody else seek recognition, any other statements before we begin? At this time, let me just deal with—I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and that the record be remain opened for 3 days for that purpose. Without objection so ordered. I ask further unanimous consent that all witnesses be permitted to include their written statements in the record and without objection, so ordered.

At this time, let me acknowledge the presence of our witnesses, and then afterwards, I will ask them to stand and swear you all in. We have Mr. Peter Verga, special assistant for Homeland Security Office of the Secretary of Defense. We have Mr. Stephen McHale, Deputy Under Secretary for Transportation Security, Transportation Security Administration, Department of Transportation. We have Dr. William Raub, deputy director, Office of Public Health Preparedness, Department of Health and Human Services; Mr. Kenneth 0. Burris, director of Region IV, Atlanta, Federal Emergency Management Agency; Mr. James Caruso, Deputy Assistant Director for Counterterrorism, Federal bureau of investigation; and Mr. Joseph R. Green, Deputy Executive Associate Commissioner for Field Operations, U.S. Immigration and Naturalization Service.

I would just point out that before I ask you to stand, we realize it is a large panel, I'm still going to invite you to speak for 5 minutes plus. You have that range between 5 to 10. You don't want to get close to 10, but we want you to say what you need to say, and then we will seek to ask you questions. I consider this a very important hearing, and I welcome you here, and I think we can learn a lot in this process, and at this time I would ask you to stand and I will swear you in.

Before I begin is there anyone else whom you may seek to ask advice from? If so, I would ask them to stand as well. Is there anyone else in your office? OK.

[Witnesses sworn.]

Mr. SHAYS. Note for the record that all of our witnesses have responded in the affirmative, and I'm making the assumption we are going to go in the order in which I called. Are we lined up that way? Let's see. We're going to start with you, Mr. Verga, and we'll need to hear you and there's a clock in front of you, just so you know—is it working? Five minutes and then it will get to red and you'll see the red and you will know you've got less than 5 minutes to conclude.

Mr. VERGA. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you.

STATEMENTS OF PETER VERGA, SPECIAL ASSISTANT FOR HOMELAND SECURITY OFFICE OF THE SECRETARY OF DEFENSE; STEPHEN MCHALE, DEPUTY, UNDER SECRETARY, TRANSPORTATION SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF TRANSPORTATION; WILLIAM RAUB, DEPUTY DIRECTOR, OFFICE OF PUBLIC HEALTH PREPAREDNESS, DEPARTMENT OF HEALTH AND HUMAN SERVICES; KENNETH O. BURRIS, DIRECTOR OF REGION IV, ATLANTA, FEDERAL EMERGENCY MANAGEMENT AGENCY; JAMES CARUSO, DEPUTY ASSISTANT DIRECTOR FOR COUNTER TERRORISM, FEDERAL BUREAU OF INVESTIGATION; AND JOSEPH R. GREEN, DEPUTY EXECUTIVE ASSOCIATE COMMISSIONER FOR FIELD OPERATIONS, U.S. IMMIGRATION AND NATURALIZATION SERVICE

Mr. VERGA. Mr. Chairman, members of the subcommittee, thank you very much for the opportunity to speak with you to the Department of Defense activities with respect to homeland security. I will outline the Department's organizing approach to oversee and conduct homeland defense missions and how DOD assists and coordinates with the Office of Homeland Security.

Mr. SHAYS. I'm going to make a request. I can hear you because you, but just lower the mic a little bit. You have a cool mic there as well that goes somewhere else, and I want to make sure they can hear you as well.

Mr. VERGA. At the direction of the Secretary of Defense, the Department is developing organizations that will oversee policy and conduct operational missions related to homeland defense and support to civil authorities. Secretary of the Army White has been managing day-to-day execution of homeland defense activities on a temporary basis in his capacity as interim executive agent for Homeland Security. The Deputy Secretary of Defense, Paul Wolfowitz, is leading the effort within the Office of Secretary, to establish an office at an appropriate level to provide policy guidance for and oversight of the Department's homeland defense and civil support activities, and to work with the Office of Homeland Security.

The Deputy Secretary is scheduled to propose organizational options to the Secretary not later than May 1st of this year. This office will ensure internal coordination of DOD policy direction and

provide oversight for military activities in support of homeland defense and civil support. It will also provide a focused, coherent interface with the Office of Homeland Security and other agencies of government on these matters. The schedule calls for the new office to be established by June 30th of this year, subject, of course, to any necessary legislation.

Second, the Department is considering a revision of the unified command plan which is the plan that establishes U.S. unified commands and assigns to them geographic areas of responsibilities and missions or functional responsibilities. The objective of this revision is unity of command in the conduct of homeland defense missions.

The chairman of the Joint Chiefs of Staff has proposed to the Secretary the creation of a new combatant command, U.S. Northern Command. This command would be assigned the mission of defending the United States against external threats and providing support to civil authorities. Under the proposal, Northern Command would assume responsibility for security cooperation with Canada and Mexico as well. If approved by the President, the proposal is to activate the command on October 1st of this year. At the same time, the Deputy Secretary is overseeing preparation of a report mandated in the fiscal year 2002 National Defense Authorization Act.

The Congress has asked the Department, among other things, to describe its supporting organization within the Office of the Secretary to address combating terrorism, homeland security, and sharing of intelligence information on these activities with other agencies. That report is due at the end of June of this year.

Previously, the Quadrennial Defense Review recognized that the highest priority for the U.S. military is the defense of the U.S. homeland. The Department of Defense is, of course, a key agent for protecting U.S. sovereignty, territory and the domestic population and critical defense infrastructures against external threats and aggression. In addition to its homeland defense role, the Department is asked, from time to time, to support a lead Federal agency such as the Federal Emergency Management Agency in responding to domestic emergencies such as a major hurricane. The Department stands ready and willing to assist civil authorities in crisis situations.

Beyond such emergency situations and other extraordinary circumstances, the Department of Defense support to U.S. civil authorities should be called for only when DOD involvement is appropriate and where a clear end date for the DOD mission is defined. The Secretary has also stressed the requirement for other agencies to reimburse the Department of Defense for civil support missions. An example of this support is what we are doing with the Treasury and Justice Departments to augment the border security activities on the northern and southern borders.

To ensure the Department's readiness for homeland defense and civil support missions, DOD components also engage in emergency preparedness, that is, those planning activities undertaken to ensure DOD processes and procedures and resources are in place to support the President and the Secretary of Defense in a national security emergency. These include planning related to cognitive op-

erations during crisis and protection of civil critical defense infrastructure.

For the first time since World War II, the Department has been engaged in the direct defense of the American homeland. Operation Noble Eagle commenced immediately after the September 11th attacks. It includes combat air patrols over various domestic locations, other expanded air operations, and command and control of active component forces. The security of U.S. domestic air space is, of course, a major concern. Other support to civil authorities in the United States includes National Guard's security augmentation at commercial airports, the support to the Olympics, and the support to the Super Bowl.

As long as terrorist networks continue to recruit new members, plan and execute attacks against U.S. national interests or seek weapons of mass destruction, our forces and Department must remain engaged. Our goals are to thwart terrorist operations, disrupt their plans, destroy their networks, and deter others who might consider such attacks on our Nation. In the coming year, U.S. military forces likely will be called upon to act either unilaterally or in concert with others to address terrorist threats in a number of countries. Our forces will be prepared to do this. Thank you very much.

Mr. SHAYS. Thank you very much.

[The prepared statement of Mr. Verga follows:]

FOR OFFICIAL USE ONLY UNTIL RELEASED BY

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

STATEMENT OF

MR. PETER VERGA

SPECIAL ASSISTANT FOR HOMELAND SECURITY

BEFORE THE 107TH CONGRESS

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

MARCH 21, 2002

FOR OFFICIAL USE ONLY UNTIL RELEASED BY

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

Statement of Mr. Peter Verga

Special Assistant for Homeland Security

Before the House Committee on Government Reform,

Subcommittee on National Security, Veterans Affairs, and International Relations

March 21, 2002

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to speak with you about Department of Defense activities with respect to homeland security. I will outline the Department's approach to organizing itself to oversee and conduct of homeland defense missions and how DoD assists and coordinates with the Office of Homeland Security.

Emerging DoD Organizational Constructs for Homeland Defense and Civil Support

At the direction of the Secretary of Defense, the Department is developing organizations that will oversee policy and conduct operational missions related to homeland defense and support to civil authorities.

Secretary of the Army White has been managing day-to-day execution of homeland defense activities on a temporary basis in his capacity as "Interim Executive Agent for Homeland Security." The Deputy Secretary of Defense is leading the effort within the Office of the Secretary of Defense (OSD) to establish an office to provide policy guidance for and oversight of the Department's homeland defense and civil support activities and to work with the Office of Homeland Security. The Deputy Secretary is scheduled to propose organizational options to the Secretary not later than 1 May 2002. This organization will ensure internal coordination of DoD policy direction and provide oversight for military activities in support of homeland defense and civil support. It will also provide a focused, coherent interface with the Office of Homeland

Security and other agencies of the government. The schedule calls for the new office to be established by 30 June 2002, subject to any necessary legislation.

Second, the Department is considering a revision to the Unified Command Plan (UCP). The objective is unity of command in the conduct of homeland defense missions. The UCP establishes U.S. Unified Commands and assigns to them geographic areas of responsibilities and missions or functional responsibilities. The Chairman has proposed to the Secretary the creation of a new combatant command, U.S. Northern Command. It would be assigned the mission of defending the United States against external threats and providing support to civil authorities. Under the proposal, Northern Command would assume responsibility for security cooperation with Canada and Mexico. The proposal is to activate the command on October 1, 2002.

At the same time, the Deputy Secretary is overseeing preparation of a report mandated by the FY 2002 National Defense Authorization Act. The Congress has asked the Department to describe its supporting organization within the Office of the Secretary of Defense to address combating terrorism, homeland security, and sharing of intelligence information on these activities with other agencies. That report is due at the end of June 2002.

The Department's Role in Homeland Defense, Civil Support, and Emergency Preparedness

The Quadrennial Defense Review recognized that the highest priority for the U.S. military is the defense of the U.S. homeland. The Department of Defense is a key agent for protecting U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression.

In addition to its homeland defense role, the Department may be asked, from time-to-time, to support a Lead Federal Agency, such as FEMA or the Justice Department, in

responding to domestic emergencies and for designated law enforcement and other activities. The Department stands ready and willing to assist civil authorities in crisis situations. The Secretary of Defense and Governor Ridge have agreed that, beyond such emergency situations, Department of Defense support to U.S. civil authorities should be called for only where DoD involvement is appropriate and where a clear end state for DoD's mission is defined. The Secretary has also stressed the requirement for other agencies to reimburse the Department of Defense for civil support missions.

To ensure the Department's readiness for homeland defense and civil support missions, DoD Components also engage in emergency preparedness—those planning activities undertaken to ensure DoD processes, procedures, and resources are in place to support the Secretary of Defense and the President in a designated National Security Emergency. These include planning related to continuity of operations during crises and protection of critical defense infrastructure.

Domestic Department of Defense Operations in Support of the Global War on Terrorism

The direct defense of the American homeland, Operation NOBLE EAGLE, commenced immediately after the 11 September attacks. Activities the Department carries out under Operation NOBLE EAGLE include the combat air patrols over key domestic locations, expanded air operations, and command and control of active component forces, including US Navy ships with anti-aircraft systems to enhance the security of US domestic airspace. NOBLE EAGLE also entails Coast Guard inspections of cargo vessels and patrols in defense of major seaports. Other measures taken in support of civil authorities here in the United States include:

- Army National Guard augmentation of security at over 400 commercial airports throughout the country, peaking to a total of almost 9,000 personnel over the 2001/2002 holiday season.

- DoD support for the Olympics and the Super Bowl. For instance, over 4,000 National Guard troops were deployed to augment security at the Olympic Games in Salt Lake City, and US Air Force aircraft, under the auspices of the North American Air Defense Command, provided air defense.

- Army National Guard augmentation of US Customs Service, Border Patrol, and Immigration and Nationalization Service personnel along our nation's northern and southern borders.

The use of military personnel to augment border security has been an area of particular concern to the Secretary of Defense, the President, and Congress.

The Department of Defense received three requests for assistance in monitoring and securing the northern and southern borders: one from the Department of Treasury, and two from the Department of Justice, including the Immigration and Naturalization Service. The Secretary of Defense agreed to support these requests, and the Department of Defense finalized Memoranda of Agreement with the Department of Treasury and Immigration and Naturalization Service that specify the type, duration, nature, and funding for requested support. Accordingly, DoD is detailing 626 personnel to assist the U.S. Customs Service at Ports of Entry in 12 Border States as well as an additional 108 support personnel (734 DoD personnel total). The Department is also detailing 710 personnel to assist the Immigration and Nationalization Service at Ports of Entry in 9 Border States and an additional 114 support personnel (824 DoD personnel total). Finally, DoD is providing 83 personnel and 6 helicopters—16 personnel to support Sector Intelligence Centers in 8 northern Border Sectors and 67 personnel along with the helicopters to support 6 northern Border Sectors—to assist the U.S. Border Patrol.

DoD personnel have already joined their Federal agency counterparts in their temporary border security missions.

Protecting US Forces and Installations

The events of the past six months have further strengthened the Secretary's already strong determination and resolve to protect the Department's personnel and installations at home and abroad. Threat and force protection levels are constantly evaluated, commanders are empowered with increased resources and flexibility to respond to changes in the threat, and exercising and training for chemical and biological attacks has increased markedly. Since September 11, the Army has completed a security infrastructure assessment at each of its installations to determine the incremental and total costs for structural and procedural enhancements for access control packages and equipment, critical mission essential areas, and weapons of mass destruction preparedness. In that same timeframe, the Department has mobilized over 31,000 National Guard and Reserve Security Forces to support force protection at domestic and overseas military bases. The Department is also finalizing new DoD guidance on Installation Emergency Preparedness, which, among other things, encourages interaction with local communities—to include planning, exercises, and interoperability of equipment—and leverages joint military-civilian response capabilities through Memoranda of Agreement. This guidance also extends to our DoD installations abroad.

The Department's Counterterrorism Priorities

Defensive measures alone cannot deter terrorist incidents. At home, the domestic law enforcement community is responsible for countering terrorist threats; the Department of Defense stands ready to provide assets and capabilities in support of civil authorities, consistent with U.S. law. The Department's counterterrorist focus is on bringing the fight to the terrorists abroad through the prosecution of the global War on Terrorism.

As long as terrorist networks continue to recruit new members, plan and execute attacks against U.S. national interests and seek out weapons of mass destruction, our

forces and Departmental assets will remain engaged. Our goals are to thwart terrorist operations, disrupt their plans, destroy their networks, and deter others who might consider such attacks on our nation. In the coming year, U.S. military forces will likely be called upon to act unilaterally or in concert with others to address terrorist threats in a number of countries. Our forces will, as they have in the past, undergo the most advanced, diverse training possible. US military personnel will constantly exercise—often with foreign counterparts—to maintain relevant counterterrorist proficiency and develop new skills.

Supporting the Office of Homeland Security

As we move forward with improving the Department's organization for homeland defense and civil support missions, it is critical to coordinate our activities with those of the Office of Homeland Security (OHS). Secretary White, his staff, and I speak regularly with Gov. Ridge and his Deputy, Admiral Abbott. In addition, the Department of Defense is represented on the Homeland Security Council's eleven different inter-agency committees, and their subordinate working groups, which cover issues ranging from bioterrorism to border security to a national threat advisory system.

Mr. Chairman, that concludes my prepared statement. I will try to answer any questions that you or other members of the Subcommittee have for me.

Mr. SHAYS. Mr. McHale.

Mr. MCHALE. Thank you, Mr. Chairman. Chairman Shays, Congressman Kucinich, and members of the subcommittee, I am pleased to appear before you today on behalf of Secretary Mineta and Under Secretary John Magaw, to discuss the Department of Transportation's progress in improving security for airports and seaports as well as other parts of the transportation infrastructure. The Aviation and Transportation Security Act established tight deadlines for the Transportation Security Administration to implement the enhanced aviation security measures. We have met all of the law's deadlines to date and are on track to meet all of the remaining deadlines. Going forward, we will be using a wide variety of innovative approaches to check baggage screening using explosive detection technology, improved ways to run the passenger screening process, and innovative procurement and recruitment strategies using all of the tools that Congress has given us.

On February 17 the TSA took over all civil aviation security functions performed by the FAA and responsibility from the airlines for passenger and baggage screening. TSA is using private screening companies until Federal security screeners can be hired, trained and assigned to all U.S. airport security screening check points. We have hired the first of tens of thousands of new employees to screen passengers and baggage at 429 airports nationwide, and we fully expect to be able to certify to Congress on November 19th of this year that we have complied with the Act's requirement to carry out all passenger and baggage screening using Federal personnel.

Our Federal security directors will be strong front line managers who will bring Federal authority directly to the point of service, the airport. An area of port security following September 11th, the Coast Guard refocused resources to protect high consequence targets in the marine environment including port facilities, critical bridges, and other infrastructure. In addition, Secretary Mineta established the National Infrastructure Security Committee [NISC], a coordinated interagency effort to address transportation security. An analysis of our transportation system in the aftermath of the events of September 11th clearly laid bare the susceptibility of container shipments as delivery system for terrorist weapons.

The Department, through TSA and the Coast Guard, in cooperation with the Customs Service, is making every effort to ensure that the security of cargo including containerized cargo as it moves throughout America's seaports and the intermodal transportation system.

The struggle against terrorism is a truly national struggle. Federal, State and local government agencies, as well as the private sector, must work seamlessly together. TSA and all of DOT's modal administrations are engaged in extensive outreach campaigns to all of the transportation industry. We are also working with law enforcement and intelligence officials at all levels to protect and defend against future terrorist attacks and to effectively manage incidents whenever and wherever they should occur.

In meeting our transportation security mission and helping us coordinate other intelligence needs, we will rely on the new Transportation Security Oversight Board, which met for the first time in

January. That board is composed of representatives from a number of Federal agencies, including the intelligence community. In addition, TSA is working coordination with the Office of Homeland Security on a regular basis as it develops national homeland security strategy. The TSA, on behalf of DOT, is charged with security for all modes of transportation and a focus on aviation must not slow the TSA's pace in addressing the security needs of other transportation modes. Across every mode we must continue to develop measures to increase the protection of critical transportation assets, addressing cargo as well as passenger transportation. We will maintain a commitment to measure performance relentlessly, building a security organization that provides world class transportation security and world class customer service.

Thank you, Mr. Chairman and I will be happy to answer any questions that you or the subcommittee may have.

Mr. SHAYS. Thank you.

[The prepared statement of Mr. McHale follows:]

Stephen J. McHale
Deputy Under Secretary of Transportation
for Security

before the

Subcommittee on National Security, Veterans Affairs
and International Relations
Committee on Government Reform
U.S. House of Representatives

March 21, 2002

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before you today on behalf of the Transportation Security Administration (TSA), which is charged with ensuring the security of air travel and other modes of transportation across the United States in accordance with the Aviation and Transportation Security Act (ATSA).

Today I would like to discuss the Department of Transportation and its progress in improving security at airports and seaports; its efforts to coordinate with Federal, State, and local agencies, including the Office of Homeland Security; priorities for additional counterterrorism efforts; and additional steps that need immediate attention to protect against future terrorist attacks.

Progress of Improvements in Security at Airports and Seaports

I would like to begin by describing the Department's progress to date on enhancing security at our nation's airports and then discuss our seaports.

Airport Security

The ATSA established tight deadlines for the TSA to achieve certain milestones on the road to enhanced aviation security. As you know, we met all 30-day deadlines. We published qualifications for federal screeners, submitted a report to Congress on general aviation security, and published claims procedures for reimbursement of direct security-related costs for airport operators and certain vendors.

Among the action items with 60-day deadlines that were completed on January 18th, the requirement to establish a system for screening all checked baggage was the most important and most challenging. The law requires that explosives detection systems (EDS) be used to screen checked bags at those airports where EDS are located. Alternative means for checked baggage screening are authorized for use at those airports where EDS is currently unavailable. These include measures and procedures passengers can see like greater use of explosives trace detection devices on checked baggage and articles like shoes, more use of explosives detection canine teams, and physical inspection of checked bags. Procedures are also being used to match passengers with their bags as allowed by the Act.

We released our screener training plan, which was written with input from leading government and private sector training experts. We also issued interim final rules to implement the $2.50 Passenger Security Fee on airline tickets sold on or after February 1, as well as the Aviation Security Infrastructure Fee, which will paid by air carriers to help finance TSA operations. In addition, U.S. and foreign air carriers have begun to electronically transmit passenger and crew manifests to the U.S. Customs Service prior to arrival, and the Federal Aviation Administration (FAA) issued its guidelines for flight crews who face threats onboard an aircraft.

On February 17, the Under Secretary of Transportation for Security took over all civil aviation security functions performed by the FAA. The TSA assumed many airline screening company contracts in the interim until Federal security screeners can be hired, trained and assigned to all U.S. airport security

screening checkpoints. TSA also published a rule requiring certain aircraft operators using aircraft weighing 12,500 pounds or more to implement a security program that includes criminal history records checks on their flightcrews and restricted access to the flight deck. These security regulations apply to both all-cargo and small scheduled and charter passenger aircraft not already covered by a security program, and will take effect on June 24, 2002.

Explosives detection equipment is a vital part of our baggage screening program. Every available explosives detection system and device will be continuously used. The Computer-Assisted Passenger Prescreening System (CAPPS) analyzes data voluntarily provided by passengers to airlines during commercial transactions. The information is used by CAPPS to screen out passengers for whom additional security procedures are unnecessary. In addition, bags in airport terminals will be subject to inspection by certified explosives detection canine teams. A certain amount of randomness is built into all of our security systems to make full use of the system as well as to hinder the planning of those intent upon attacking it.

Seaport Security

An analysis of our transportation system in the aftermath of the events of September 11 clearly laid bare the susceptibility of container shipments as a delivery system for an enemy's weapons. Prior to September 11th, DOT's primary concern was the efficient movement of these containers through the transportation system. The advent of just-in-time business processes and the use of the transportation system as a rolling inventory tied the transportation system even more integrally into the economic vitality of this country.

We have taken a number of critical steps since September 11:

- The Coast Guard has refocused resources to protect high consequence targets in the marine environment, including critical bridges, port facilities and other infrastructure.
- The Coast Guard has issued an emergency regulation requiring 96-hour advance notices of arrival for ships arriving in U.S. ports, and expects to make that regulation permanent by the summer of 2002.
- The Coast Guard Intelligence Coordination Center, working with the Office of Naval Intelligence, has been tracking inbound high-interest vessels and providing intelligence on the people, cargoes and vessels to operational commanders and interested agencies.
- The Coast Guard has deployed personnel as Sea Marshals and small boat escorts to ensure positive control of vessels containing critical cargoes and in sensitive areas.
- The Maritime Administration has been meeting with members of the maritime industry to examine and address security issues and make recommendations regarding legislation and policy changes.
- The Maritime Administration has heightened security at its Ready Reserve Force fleet sites and outport locations as well as activated one ship to assist in Operation Enduring Freedom.
- The Maritime Administration, Research and Special Programs Administration, Credential Direct Action Group and TSA are working to examine ways that advanced technologies, including smart card, biometrics and public key infrastructure can be used throughout the maritime and related industries in order to accurately identify employees working in security-sensitive areas.
- The Research and Special Programs Administration has issued a Multimodal Cargo Container Transportation and Security Broad Agency Announcement (BAA), which is open for 12 months,

seeking innovative concepts or new applications of proven technology, methods, or processes for reducing the risk and vulnerability of cargo container transportation systems to terrorist actions.

- The St. Lawrence Seaway Development Corporation has been working closely with its Canadian counterpart and the Coast Guard to heighten security on the St. Lawrence River and ensure the protection of ocean access to our Great Lakes ports.

In addition to the U.S. Coast Guard's quick response to guard the security of American ports and waterways, on February 28, 2002, Secretary Mineta announced the implementation of the Port Security Grants Program, from which TSA will distribute $92.3 million in grant money to seaports to finance port security assessments and the cost of enhancing facility and operational security at critical national seaports.

Secretary Mineta also established the National Infrastructure Security Committee (NISC), a coordinated interagency effort to address transportation security. Through several direct action groups, the NISC was tasked with evaluating transportation infrastructure vulnerabilities, security protocols, and processes and recommending changes to improve security.

From the direct action group process, other groups have been formed to tackle very specific security issues. Among these is the Container Working Group – established through the NISC in December. The Container Working group is co-chaired with the U.S. Customs Service and includes representatives from the Departments of Defense, Energy, Commerce, Justice, Agriculture, Health and Human Services (FDA) and others. The group has oversight from the Office of Homeland Security.

In order to address individual aspects of container security, four subgroups of the Container Working Group are studying information systems, security technologies, business practices, and international affairs. On the front lines of container security is the U.S. Customs Service, as well as other federal agencies. The Container Working Group is studying technologies and business practices that will enable Customs and others to prevent high-risk containers from entering the United States or to ensure that they are properly inspected before they pose a threat to the United States. Although the Customs Service utilizes a thoughtful risk-based selection method, preventing a container from being used as a weapon requires a more complex strategy, enhancing the non-intrusive inspection technology and information used for selection. The new Customs Container Security Initiative builds upon previous work with our international trading partners to improve container security throughout the world's global supply chain.

Coordination with the Office of Homeland Security and Federal, State, and Local Agencies

The struggle against terrorism is a truly national struggle. Federal, State, and local government agencies, as well as the private sector must work seamlessly together. Having the right system of communication - content, process, and infrastructure - is critical to bridging the existing gaps between the Federal, State, and local governments, as well as the private sector. Effective communications systems will greatly assist our officials at all levels to protect and defend against future terrorist attacks, and to effectively manage incidents whenever they should occur.

To help meet these needs, the Administration implemented a uniform national threat advisory system to inform Federal agencies, State and local officials, as well as the private sector, of terrorist threats and appropriate protective actions. The President's Budget for fiscal year 2003 supports this effort by funding the development and implementation of secure information systems to streamline the dissemination of critical homeland security information.

In meeting its transportation security mission, TSA plans to place heavy reliance on the new Transportation Security Oversight Board composed of representatives from the Departments of Justice, Defense, and Treasury, the Central Intelligence Agency, the National Security Council, and the Office of Homeland Security. In addition, TSA separately is working in coordination with the Office of Homeland Security on a regular basis as it works to roll out its security program.

We also are working with the States, airport authorities, and local governments as TSA transitions to a fully Federal workforce of screeners and law enforcement personnel. In addition, we will be working with States and localities on the ground at airports through the newly appointed Federal Security Directors. These FSDs are the strong front-line managers who will bring Federal authority directly to the point of service, the airport. Secretary Mineta swore in the first contingent of FSDs on March 13.

In addition, TSA is working with the States, airport authorities, and local agencies as it rolls out pilot programs to test its security procedures. For instance, TSA is working with the State of Maryland to use Baltimore-Washington International Airport as a site to study airport security operations, test TSA deployment techniques and technology, and begin to train senior managers for TSA.

Establishment of Priorities for Additional Counterterrorism Efforts

Congress has, in large part, given the Department specific guidance on its security priorities for transportation. From the date of enactment of the ATSA, the Secretary has focused our efforts intensively on complying with or exceeding the deadlines established in the new law. As Secretary Mineta has stated, we consider the law's tight deadlines as promises made to the American people, and we will do everything possible to keep these promises. Secretary Mineta has given those of us in DOT a simple mandate with regard to these deadlines: let's figure out how to meet them, because they are not negotiable.

TSA has hired the first of tens of thousands of new employees to screen passengers and baggage at 429 airports nationwide, so that we can certify to Congress on November 19 of this year that we have complied with the Act's requirement to carry out all passenger screening with Federal personnel. We also are working to ensure that all checked baggage is screened by explosives detection technology by December 31, 2002.

Cargo screening in all modes of transportation is another area that is integral to transportation security and that requires our focused attention as we choose among competing demands for available funds. Air cargo, in particular, is a critical part of the commercial supply chain and an important contributor to the economics of the civil aviation system. As TSA moves forward in meeting its legislative mandate to protect the entire airplane and its associated processes, air cargo security on passenger aircraft has taken on a heightened level of focus. This focus includes new approaches as well as accelerating the efforts and prototypes that FAA had been pursuing prior to the creation of TSA.

Another area that the Department recognizes as crucial in our fight against terrorism is the protection of our critical infrastructure, including our cyber infrastructure. DOT is coordinating with the major components of the transportation sector to ensure the protection of the nation's critical infrastructure. This effort includes working with the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce to assess critical physical and technological assets and their interdependencies on other components of the critical infrastructure such as telecommunications.

In addition, a major effort to upgrade the Department's information technology security program is underway. This will include installing new security devices, monthly vulnerability testing of the infrastructure, and the implementation of better intrusion detection capabilities. We have also significantly increased the training of executives and staff as well as computer support personnel on security requirements. TSA will, of course, have a major role in this intradepartmental effort.

Additional Steps to Protect the U.S. from Future Attacks.

September 11 taught us that our enemies are willing to die to attack us, and that means that we must successfully screen all baggage and cargo on a passenger flight. Screening all checked baggage and cargo is therefore among our highest priorities. We are looking at a wide variety of innovative approaches using technology, different ways to run the check-in process, and procurement strategies that can get us to that goal.

The TSA, on behalf of DOT, is charged with security for all modes of transportation, and a focus on aviation must not slow the TSA's pace in addressing the security needs of other transportation modes. Across every mode, we must continue to develop measures to increase the protection of critical transportation assets, addressing cargo as well as passenger transportation. We will maintain a commitment to measure performance relentlessly, building a security organization that provides world-class security, and world-class customer service, to those who travel.

The new security system will be robust and redundant, and we will be relentless in our search for improvements. It is better today than yesterday; and it will be better still tomorrow.

This concludes my statement. I will be glad to answer any questions.

Mr. SHAYS. Doctor, I've learned that if you give 10 minutes, you usually get five and when you give five you usually get 10.

Mr. RAUB. I'll try to keep of the pattern, Mr. Chairman.

Mr. SHAYS. OK. You have 10 minutes.

Mr. RAUB. Thank you, sir, and members of the subcommittee. I welcome this opportunity to apprise this subcommittee about the activities of the Department of Health and Human Services related to protecting the United States from terrorist attacks. I have a short oral statement and with your permission, Mr. Chairman, I'll submit my written statement for the record.

Mr. SHAYS. Thank you.

Mr. RAUB. Mr. Chairman, your letter of February 28 to Secretary Thompson listed six topics to be addressed during this hearing. I will address each briefly. First is coordination with the Office of Homeland Security, or OHS. HHS coordinates its antiterrorism activities closely with OHS. Secretary Thompson, Deputy Secretary Allen, and Dr. D.A. Henderson, director of the recently created Office of Public Health Preparedness, are in frequent contact with OHS Director Ridge and his senior multidepartment activities, as well as specific HHS initiatives. Deputy Director Allen participates routinely as a member of the Office of Homeland Security's deputies committee, which is the primary senior level mechanism for interdepartmental communication and coordination.

Several other HHS senior staff participate in more specialized interdepartmental groups called policy coordinating committees that support the work of the deputies committee. Second is the establishment of HHS program priorities. The priorities for the use of HHS counterterrorism funds are the result of the confluence of the priorities articulated by the President in his budget request and the priorities specified by the Congress in the regular, and supplemental appropriations for fiscal year 2002.

In general, HHS is directing its investments toward enhanced preparedness for bioterrorism, other outbreaks of infectious disease and other public health threats and emergencies with antibioterrorism enhancements at the local, State and national levels as job No. 1. Guided by this strategic framework, HHS's primary emphasis areas are as follows: One, enhancing State and local preparedness; two, improving HHS response assets to support municipalities and States as needed; third, developing and procuring safer and more effective vaccines against smallpox and anthrax; fourth, developing better diagnostic tests, drugs and vaccines for the microorganisms most likely to be used by terrorists; and fifth, reinforcing and augmenting border coverage of all imported products, particularly foods through increased inspectional and laboratory resources and coordination with the U.S. Customs Service.

HHS is striving for measurable achievements in all of these areas. For example, recently awarded cooperative agreements to enhance the terrorism related capabilities of health departments and hospitals feature particular critical benchmarks, critical capacities and other specific objectives that the States and other eligible entities are expected to achieve. Third is coordination with other agencies. HHS has had a long-standing role with respect to the Federal response plan, working closely with the Federal emergency

management agency, the Department of Justice and other agencies as appropriate.

In particular, under the Federal response plan, HHS is the lead agency within the Federal Government for addressing the medical and public health consequences of all manner of mass casualty events, whether terrorist induced, accidental or naturally occurring. This responsibility is codified as emergency support function No. 8. HHS also is working to coordinate planning, training and consequence management actions at the State and local levels.

The recently awarded cooperative agreements to enhance the terrorism relevant capabilities of health departments and hospitals across the Nation emphasize statewide and regional planning, training of health professionals and other responders, and medical and public health preparedness in response to mass casualty events. As work under the cooperative agreements progress, HHS will collaborate with its State and municipal partners in identifying exemplary practices in these and other preparedness areas and promoting common approaches wherever appropriate.

The fourth topic was private sector feedback. The private sector seems able and eager to help advance the HHS priorities. In the vaccine development area for example, representatives of the pharmaceutical industry have stressed that to the extent that the Federal Government can provide its vaccine requirements and assure upfront that the requisite funds will be available, the industry will meet the challenge.

Thanks to the President's leadership and congressional appropriations for fiscal year 2002, this currently is the case for the HHS effort to develop and acquire a sufficient quantity of a new smallpox vaccine to protect the entire U.S. population. HHS is hopeful for a similar scenario to be realized for a new anthrax vaccine if the advanced development work during fiscal year 2002 is successful and if the President's request for $250 million for anthrax vaccine acquisition in fiscal year 2003 is approved by the Congress.

The fifth topic is other actions to facilitate the development of new medical products. HHS-funded research, primarily through the National Institutes of Health, is attempting to produce new knowledge that will enable the development of new or improved antiterrorism capabilities. Foremost among these is the rapidly expanding array of studies in microbial genomics. By sequencing the genomes of the various species and strains of the microbes most likely to be used by terrorists and by performing comparative analyses of these genomes and their protein products, scientists hope to achieve fresh leads for the development of new or improved diagnostic devices, drugs and vaccines.

Moreover, such research often referred to as comparative microbial genomics and proteomics, also may yield new insights into the genetic basis for why different species of microbes or even different strains of the same species differ from one another, often substantially, in either their virulence or their susceptibility to antibiotics. The results of such research not only could spur advanced development and commercialization of new diagnostic, therapeutic and prophylactic products, but also could enable more informed preventative and therapeutic strategies using existing products.

Finally, with respect to other necessary steps, HHS recognizes that much remains to be done to ensure our Nation is adequately prepared for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies.

For example, a robust infrastructure for infectious disease surveillance will require continuous improvement over the next several years. Moreover, the development and commercialization of new diagnostics, drugs and vaccines almost inevitably are complex scientific and technical endeavors and rarely proceed on a predictable course or time line. Nevertheless, despite these formidable challenges and uncertainties, HHS believes that its fundamental antiterrorism strategy is sound and notes that it is already yielding solid incremental enhancement in local, State and national capabilities to ensure homeland security. The major challenge at present is to invest in enhanced local, State, and national capabilities as rapidly yet responsibly as possible. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much.

[The prepared statement of Mr. Raub follows:]

Testimony
Before the Committee on Government Reform
Subcommittee on National Security, Veterans Affairs and International Relations
United States House of Representatives

Combating Terrorism - Protecting The United States: The Role of HHS's Office of Public Health Preparedness

Statement of
William F. Raub, Ph.D.
Deputy Director,
Office of Public Health Preparedness
Department of Health and Human Services

For Release on Delivery
Expected at 1:00 pm
on Thursday, March 21, 2002

Good morning, Mr. Chairman and members of the Subcommittee. I am William F. Raub, Deputy Director of the Office of Public Health Preparedness, Department of Health and Human Services (HHS). I welcome this opportunity to apprise the Subcommittee about HHS activities related to protecting the United States from terrorist attacks.

THE OFFICE OF PUBLIC HEALTH PREPAREDNESS

In the wake of the terrorist attacks in September and October, 2001, Secretary Thompson acted to strengthen HHS anti-terrorism programs by creating the Office of Public Health Preparedness (OPHP) within the Office of the Secretary and recruiting as its first Director Dr. Donald A. Henderson, an internationally acclaimed leader in public health. OPHP directs and coordinates HHS preparedness and response activities related to bioterrorism and other public health emergencies. The HHS program includes enhancement of state and local preparedness; development and maintenance of critical federal government response assets (such as the National Pharmaceutical Stockpile and the National Disaster Medical System); research and development toward new vaccines, diagnostics, and drugs; and liaison with key organizations outside HHS (such as the White House Office of Homeland Security and the academic and industrial communities).

TOPICS FOR WHICH THE SUBCOMMITTEE REQUESTED COMMENTS

The Chairman's letter of February 28 to Secretary Thompson listed six topics to be addressed during this hearing. The remainder of this statement comprises HHS' comments on those topics.

1. "the extent to which the Department of Health and Human Services (HHS) coordinates with, and provides input to the Office of Homeland Defense in their development of a national strategy to counterterrorism."

HHS coordinates its anti-terrorism activities closely with the Office of Homeland Security (OHS). Secretary Thompson and Dr. Henderson are in frequent contact with OHS Director Ridge regarding multi-Department activities as well as specific HHS initiatives. For example, Dr. Henderson recently briefed OHS staff about HHS awards of more than $1 billion via cooperative agreements to all 50 States, 4 selected major municipalities (the District of Columbia, Los Angeles County, Chicago, and New York City), and the 5 U.S. territories to foster state and local preparedness for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies. In addition, the Deputy Director of HHS, Claude Allen, participates routinely as a member of the Office of Homeland Security's Deputies Committee, which is the primary senior-level mechanism for inter-Departmental communication and coordination. Also, several other HHS senior staff participate in more specialized inter-Departmental groups, called Policy Coordinating Committees, that support the work of the Deputies Committee.

2. " how your agency establishes priorities for the additional counter terrorism funds received, and measurable achievements"

Priorities for the use of HHS counterterrorism funds are the result of the confluence of the priorities articulated by the President in his budget requests and the priorities specified by the Congress in the regular and supplemental appropriations for fiscal year 2002. In general, HHS is directing its investments toward enhanced preparedness for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies, with anti-bioterrorism enhancements at local, state, and national levels as job number one.

Guided by this strategic framework, HHS' primary emphasis areas are as follows: (a) enhancing state and local preparedness; (b) improving HHS response assets to support municipalities and states as needed; (c) developing and procuring safer and more effective vaccines against smallpox and anthrax; (d) developing better diagnostic tests, drugs, and vaccines for the microorganisms most likely to be used by terrorists, and (e) reinforcing and augmenting border coverage of all imported products particularly foods through increased inspectional and laboratory resources and coordination with the U.S. Customs Service. Within the first category, state and local preparedness, the HHS focus is on improving the capabilities of state health departments, local health departments, hospitals, and Metropolitan Medical Response Systems to respond to terrorist-related events, including our ability to communicate at all levels among responders and to the public during a public health emergency. Within the second category, HHS response assets, the HHS focus is on improving the infectious disease surveillance and broader emergency response capabilities of the Centers for Disease Control and Prevention, augmenting the size and scope of materials within the National Pharmaceutical Stockpile and

ensuring rapid deployment of these materials as needed; and on further developing the National Disaster Medical System.

HHS is striving for measurable achievements in all these areas. For example, the recently awarded cooperative agreements to enhance the terrorism-related capabilities of health departments and hospitals feature particular "critical benchmarks," "critical capacities," and other specific objectives that the States and other eligible entities are expected to achieve. In a similar vein, HHS has outlined specific objectives for its further investments in the National Pharmaceutical Stockpile, the National Disaster Medical System, and smallpox vaccine development and acquisition. The Department would be pleased to provide additional information on these activities as the Subcommittee may desire.

3. "agency efforts to coordinate the planning, training, and consequence management actions among federal, state, and local agencies"

HHS has had a longstanding role with respect to the Federal Response Plan — working closely with the Federal Emergency Management Agency, the Department of Justice, and other agencies as appropriate. In particular, under the Federal Response Plan, HHS is the lead agency within the federal government for addressing the medical and public health consequences of all manner of mass casualty events whether terrorist-induced, accidental, or naturally occurring. This responsibility is codified as Emergency Support Function #8.

HHS is also working to coordinate planning, training, and consequence management actions at the State and local levels. The recently awarded cooperative agreements to enhance the terrorism-relevant capabilities of health departments and hospitals across the nation emphasize state-wide and regional planning, training of health professionals and other responders, and medical and public health preparedness and response to mass casualty events. As work under the cooperative agreements progresses, HHS will collaborate with its state and municipal partners in identifying exemplary practices in these and other preparedness areas and promoting common approaches wherever appropriate. For example, in striving to help states and municipalities strengthen their information technology capabilities, HHS will place a high priority on achieving interoperability of communications systems and databases.

4. "your feedback from the private sector about the role they will play in addressing the priorities you have identified"

The private sector seems able and eager to help advance the HHS priorities. In the vaccine development area, representatives of the pharmaceutical industry have stressed that, to the extent that the federal government can prescribe its vaccine requirements and assure up front that the requisite funds will be available, the industry will meet the challenge. Thanks to the President's leadership and Congressional appropriations for fiscal year 2002, this currently is the case for the HHS effort to develop and acquire a sufficient quantity of a new smallpox vaccine to protect the

entire U.S. population. HHS is hopeful for a similar scenario to be realized for a new anthrax vaccine, if the advanced development work during fiscal year 2002 is successful and if the President's request for $250 million for anthrax vaccine acquisition in fiscal year 2003 is approved by the Congress.

The private sector also is active in other pertinent areas. Development of new or improved multi-spectrum antibiotics is a high priority for the pharmaceutical industry. Many companies, large and small, are attempting to develop rapid diagnostic tests and devices for microbes likely to be used by terrorists. Still other companies, large and small, are pursuing new information technologies and systems that may prove valuable for infectious disease surveillance and hospital response to mass casualty events.

For the purpose of providing the private sector with a single Department of Health and Human Services point of contact and maximizing the opportunities for public private partnerships, Secretary Thompson established the *Council on Private Sector Initiatives to Improve the Security, Safety, and Quality of Health Care.* The Council is triaging requests from individuals and firms seeking review of their ideas or products and forwarding information to the appropriate agencies and offices. This system ensures that DHHS responds systematically and consistently to private sector requests.

The food industry has actively engaged in strengthening security measures at food processing facilities, restaurants, and retail establishments through establishment of the Alliance for Food Security. In January of this year, the Food and Drug Administration published food security guidance for the domestic and imported food industries. The guidance provides a checklist of potential preventive measures that these firms can take to reduce the risk that food under their control will be subject to tampering, criminal, or terrorist action.

5. "other actions to facilitate the production of new therapeutic medicines and vaccines against the toxins and agents sought by terrorists"

HHS-funded research, primarily through the National Institutes of Health, is attempting to produce new knowledge that will enable the development of new or improved anti-bioterrorism capabilities. Foremost among these efforts is the rapidly expanding array of studies in microbial genomics. By sequencing the genomes of the various species and strains of the microbes most likely to be used by terrorists and by performing comparative analysis of these genomes and their protein products, scientists hope to achieve fresh leads for the development of new or improved diagnostic devices, drugs, and vaccines. Moreover, such research (often referred to as comparative microbial genomics and proteomics) also may yield new insights into the genetic basis for why different species of microbes (or even different strains of the same species) differ from one another, often substantially, in either their virulence or their susceptibility to antibiotics. The results of such research not only could spur advanced development and

commercialization of new diagnostic, therapeutic, and prophylactic products but also could enable more informed preventative and therapeutic strategies using existing products.

6. "additional steps which need immediate attention to protect United States citizens from terrorist attacks"

HHS recognizes that much remains to be done to ensure our nation is adequately prepared for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies. For example, a robust infrastructure for infectious disease surveillance will require continuous improvement over the next several years. Moreover, the development and commercialization of new diagnostics, drugs, and vaccines almost inevitably are complex scientific and technical endeavors and rarely proceed on a predictable course or time line. Nevertheless, despite these formidable challenges and uncertainties, HHS believes that its fundamental anti-terrorism strategy is sound and notes that it is already yielding solid incremental enhancements in local, state, and national capabilities to ensure homeland security. The major challenge at present is to invest in enhanced local, state, and national capabilities as rapidly yet responsibly as possible. HHS is prepared to stay the course. Our Nation's security demands nothing less.

Mr. SHAYS. Mr. Burris, you're next. Just refresh me, your district is Atlanta, but how many States does it include?

Mr. BURRIS. The 8 southeastern States from Mississippi over to North Carolina, Tennessee and Kentucky.

Mr. SHAYS. Great. Thank you very much.

Mr. BURRIS. Yes, sir. Good afternoon, Mr. Chairman and members of the subcommittee. On behalf of Director Allbaugh, I'd like to extend his regrets for being unable to be here today, but I'm more than happy to be here to discuss FEMA's efforts in homeland security. December 2000, the Gilmore Commission issued its second report, stressing the importance of giving States and local first responders a single point of contact for Federal assistance in training, exercises and equipment. The third Gilmore Commission report included recommendations to address the lack of coordination including proposals to consolidate the Federal grant program information and application process as well as to include the first responder community in participating in Federal preparedness programs.

These findings and recommendations have been echoed in numerous other commission reports and GAO reports as well, and by first responder community and State and local officials. FEMA's role in responding to terrorist attacks was well established before September 11th. On May 8, 2001, the President tasked Director Allbaugh with creating the Office of National Preparedness within FEMA. The mission of the Office of National Preparedness is to coordinate and facilitate Federal efforts to assist State and local first responders as well as emergency management organizations with planning, equipment, training, and exercises.

The goal is to build and sustain their capability to respond to any emergency or disaster, including a terrorist incident, weapon of mass destruction or any other natural or man-made hazard. By creating the Office of Homeland Security, the President took an important first step to improve the Nation's capabilities to respond to and to coordinate Federal programs and activities aimed at combating terrorism.

FEMA works closely with the Office of Homeland Security, as well as other Federal agencies, to identify and develop the most effective ways to build and enhance the overall domestic capability for response to terrorist attack. In January, the President took another important step to support the efforts of first responders to prepare for incidences of terrorism. The First Responder Initiative, which would include $3.5 billion distributed to State and local jurisdictions, will give them the critically needed funds to plan, purchase equipment, train and exercise personnel to respond to a terrorist incident.

These grants to be administered by our Office of National Preparedness will be based on lessons learned by the first responder community of September 11th. These lessons will be incorporated as national standards for the interoperability and compatibility of training, exercises, equipment and mutual aid. The grants coupled with these standards will balance the need for both flexibility that is sought for by States and local government and the accountability at the State and local level. FEMA's Office of National Preparedness will work with other Federal agencies and the States to co-

ordinate terrorism-related first responder programs in order to simplify and unify the national response system. FEMA is well prepared and equipped to respond to terrorist events.

Our goal is to ensure that the Federal Government and its partners provide support to disaster victim, first responders, and local government. We are positioned to move forward in these initiatives in a meaningful way and look forward to working with our other Federal partners, State and local partners in helping our Nation prepare for the future. It's critical that we require—this requires a commitment of all of our partners working together to ensure its success and if by doing so we can accomplish the greatest achievement of all for our country and that's a Nation prepared.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you, Mr. Burris.

[The prepared statement of Mr. Burris follows:]

STATEMENT OF

KENNETH O. BURRIS JR.
REGION IV DIRECTOR

FEDERAL EMERGENCY MANAGEMENT AGENCY

BEFORE THE

GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

U.S. HOUSE OF REPRESENTATIVES

MARCH 21, 2002

Introduction

Good morning, Mr. Chairman and Members of the Subcommittee. I am Ken Burris Federal Emergency Management Agency (FEMA) Region IV Director. Director Allbaugh regrets that he is unable to be here with you today. It is a pleasure for me to represent him at this very important hearing on combating terrorism.

FEMA is the Federal Agency responsible for coordinating our nation's efforts to mitigate against, prepare for, respond to, and recover from all hazards. Our success depends on our ability to organize and lead a community of local, State, and Federal agencies, volunteer organizations, private sector entities and the first responder community. We know whom to bring to the table when a disaster strikes in order to ensure the most effective management of the response and recovery effort. We provide management expertise and financial resources to help State and local governments when they are overwhelmed by disasters.

The Federal Response Plan (FRP) forms the heart of our management framework and lays out the process by which interagency groups work together to respond as a cohesive team to all types of disasters. This team is made up of 26 Federal departments and agencies, and the American Red Cross, and is organized into 12 emergency support functions based on the authorities and expertise of the members and the needs of our counterparts at the State and local level.

Since 1992, in all manner of horrific natural disasters like the Northridge Earthquake and Hurricane Floyd and also in response to the Oklahoma City bombing and the terrorist attacks of September 11, 2001, the FRP has proven to be an effective and efficient framework for managing all phases of disasters and emergencies. The FRP is successful because it builds upon existing professional disciplines, expertise, delivery systems, and relationships among the participating agencies. FEMA has strong ties to emergency management organizations - fire service, law enforcement and emergency medical communities - and we routinely plan, train, exercise, and operate together to remain prepared to respond and recover from all hazards.

We learn from every disaster experience and incorporate these lessons wherever possible into our planning and processes to improve the next disaster response. For example, an assessment of the Oklahoma City bombing led to the full realization of the FEMA Urban Search & Rescue teams as well as the processes for monitoring the long-term health of first responders. The World Trade Center and Pentagon disaster responses are no different. We have learned from both. We recognize that better personal protective equipment is needed for our first responders and that training and exercises, better communications and improved interoperability of the equipment, and enhanced medical response capabilities and mutual aid agreements are also needed. We are committed to ensuring that those needs are met.

Meeting The Challenge Ahead – Office of National Preparedness

Although the challenge of meeting these needs may represent an expansion of our duties, in many respects, FEMA's role in responding to terrorist attacks was identified well before September 11th. On May 8, 2001, the President tasked Director Allbaugh with creating the Office of National Preparedness (ONP) within FEMA to "coordinate all Federal programs dealing with weapons of mass destruction consequence management" and "work closely with state and local governments to ensure their planning, training, and equipment needs are met."

ONP: Mission and Activities in Support of Homeland Security

Following the September 11 attacks, the President appointed Governor Ridge to head the newly established Office of Homeland Security (OHS) with the charge to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." In carrying out this activity, the OHS was tasked to "coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States." Since that time, FEMA has been working closely with Governor Ridge and OHS and other agencies to identify and develop the most effective ways to quickly build and enhance the overall domestic capability to respond to terrorist attacks. In consultation with OHS, FEMA will provide critical support for homeland security initiatives, particularly in the area of local and State capability building. FEMA will also have a significant role supporting the development of the national strategy, participating in interagency forums and working groups, including the Homeland Security Council and Policy Coordinating Committees, and contributing to the interagency budget strategy and formulation process.

The Office of National Preparedness' (ONP) mission is to provide leadership in the coordination and facilitation of all Federal efforts to assist State and local first responders (including fire, medical and law enforcement) and emergency management organizations with planning, training, equipment and exercises necessary to build and sustain capability to respond to any emergency or disaster, including a terrorist incident involving a weapon of mass destruction and other natural or manmade hazards.

FEMA has made or in the process of making the following changes to support this expanded mission to support the Office of Homeland Security:

- Realigned preparedness activities from the Readiness, Response and Recovery Directorate to ONP;
- Realigned all training activities into the U.S. Fire Administration to allow greater coordination between training for emergency managers and training for firefighters;
- Moved the authority for credentialing, training and deploying Urban Search and Rescue teams from the Readiness, Response and Recovery Directorate to the U.S. Fire Administration.

ONP Organization

The ONP is organized in FEMA Headquarters under a Director (reporting directly to the FEMA Director) and supported by a Management Services Unit and four Divisions to carry out key its functions to coordinate and implement Federal programs and activities aimed at building and sustaining the national preparedness capability. The divisions and their functional responsibilities include the following:

- **Administration Division** – Provide financial and support services, and management of the grant assistance activities for local and State capability building efforts.
- **Program Coordination Division** – Ensure development of a coordinated national capability involving Federal, State, and local governments, to include citizen participation in the overall efforts to effectively deal with the consequences of terrorist acts and other incidents within the United States.
- **Technological Services Division** – Improve the capabilities of communities to manage technological hazard emergencies and leverage this capability to enhance the capability for dealing with terrorist attacks.
- **Assessment and Exercise Division** – Provide guidance, exercises, and assessments and evaluate progress in meeting National goals for development of a domestic consequence management capability.

We continue to work with all 55 states, and territories, the District of Columbia, and Federally recognized Indian Tribes and Alaskan Native Villages to implement our grant programs to assist State, Tribal, and local government to enhance their capabilities to respond to all types of hazards and emergencies including terrorist incidents and natural disasters.

First Responder Initiative

In his FY'03 Budget proposal, the President has requested that FEMA receive $3.5 billion to administer the First Responder Initiative. Grants based on this initiative will give the first responder community critically needed funds to prepare for a terrorist incident. The ONP will be responsible for administering these First Responder grants.

Some of the goals established by ONP for the First Responder Initiative are as follows:

- Provide States and localities with the proper balance of guidance and flexibility so that the funds are used in the local areas where they are needed most;
- Establish a consolidated, simple, and quick method for disbursing Federal assistance to States and localities;
- Foster mutual aid across the nation so that the entire local, State, Federal and volunteer network can operate together seamlessly;
- Create an evaluation process to make sure that all programs are producing results and to direct the allocation of future resources, and;
- Involve all Americans in programs to make their homes, communities, States and nation safer and stronger.

In achieving these objectives, FEMA will implement a procedure designed to speed the flow of resources to the States and localities. Federal funds will then be used to support State and local governments in four key areas:

- **Planning.** Providing support to State and local governments in developing comprehensive plans to prepare for and respond to a terrorist incident.
- **Equipment.** Allowing State and local agencies to purchase a wide range of equipment needed to respond effectively to a terrorist attack, including better, more interoperable communications equipment.
- **Training.** Provide training to first responders to respond to terrorist incidents and operate in contaminated environments.
- **Exercises.** Develop a coordinated, regular exercise program to improve response capabilities, practice mutual aid, and assess operational improvements and deficiencies.

The First Responder Initiative builds upon existing capabilities at the Federal, State, and local level by providing needed resources to improve our response capabilities and strengthen our preparedness as a nation.

The Role of the U.S. Fire Administration

Our nation's firefighters will continue to bear an increasing portion of the burden for homeland security, responding to a variety of emergent issues including terrorism. The U.S. Fire Administration (USFA) will provide the Office of National Preparedness with essential support through its unique focus on training programs within the Federal Government. These programs are included in the Agency's mission-related preparedness and mitigation strategies.

In addition, the Assistance to Firefighters Grant Program remains an important element in supporting the most pressing needs of at-risk communities and fire service providers in reducing the loss of life and property from fire, including loss of life and injury to firefighters. As a result of the last year's appropriations, this Grant Program received $150 million that must be obligated by September 30th of the current fiscal year. An additional $210 million was received in the Emergency Supplemental that is expendable until September 30th, 2003. We expect most of the supplemental appropriation will be obligated in FY 2002 with almost all of the remainder obligated in the first quarter of FY 2003. FEMA is happy to report that our on-line application system is up and running as of March 1, 2002.

Transfer of the Office for Domestic Preparedness to FEMA

The President's budget request also seeks to consolidate our nation's preparedness efforts under one Federal agency; the President has requested that the Office for Domestic Preparedness (ODP) be transferred from the Department of Justice to FEMA. With this proposal the President has shown true leadership in his willingness to address a long-standing problem – the need for central coordination among the myriad of Federal programs dealing with terrorism preparedness.

Some forty Federal Departments and Agencies have been involved in the overall effort to build the national capability for preparedness and response to the consequences of terrorist incidents. Many of these activities have been primarily focused on the development or enhancement of

Federal capabilities to deal with terrorist incidents, including plans, personnel and physical security upgrades, and specialized resources such as protection and detection technology and response teams. Other Federal programs and activities are focused on building the local and State first responder and emergency management capabilities, to include the provision of resources and funding to support planning, training, exercises and equipment acquisition.

Various independent studies and commissions have recognized the problems inherent in this uncoordinated approach. Several recommendations by the Gilmore Commission, for example, stress the importance of giving states and first responders a single point of contact for Federal assistance for training, exercises and equipment. In its second report issued in December 2000, the Commission found that the "organization of the Federal government's programs for combating terrorism is fragmented, uncoordinated, and politically unaccountable." The Commission's third report issued seven key recommendations regarding state and local response capabilities. These seven recommendations included consolidating Federal grant program information and application procedures.

These findings and recommendations have been echoed in numerous other Commissions and reports, by the first responder community, and by state and local governments.

In the post-9/11 environment, we can ill afford to wage turf battles that in effect protect the inefficiencies of the status quo. We must instead focus on the merits of a proposal that seeks to address duplication, shore up gaps, eliminate confusion and reduce complication.

Citizen Corps

In order to help Americans strengthen their communities, President Bush tasked FEMA with overseeing Citizen Corps. This initiative is part of the overall effort of Freedom Corps, whose mission is to assist individuals and communities with implementing Homeland Security Programs in their areas. Since September 11, 2001, Americans are more aware than ever of the threat of terrorist acts on home soil. In the days following the attacks we saw immediate and selfless volunteering, generous monetary gifts, blood donations, and an outpouring of support and patriotism across America. Sustaining that spirit of volunteerism and unity is crucial to defending the homeland.

Citizen Corp's broad network of volunteer efforts will harness the power of the American people by relying on their individual skills and interests to prepare local communities to effectively prevent and respond to the threats of terrorism, crime, or any kind of disaster.

Citizen Corps will build upon existing crime prevention, natural disaster preparedness, and public health response networks. Citizen Corps will initially consist of participants in the following five programs: the Volunteers in Police Service Program; an expanded Neighborhood Watch Program; the Medical Reserve Corps; Community Emergency Response Teams (CERT), and the Terrorism Information and Prevention System (TIPS). FEMA has the responsibility for approving additional programs to be affiliated with Citizen Corps in the future.

Finally, Citizen Corps will bring together local government, law enforcement, educational institutions, the private sector, faith-based groups and volunteers into a cohesive community resource. The Federal role is to provide general information, to develop training standards and materials, and to identify volunteer programs and initiatives that support the goals of the Citizen Corps.

Moving Forward

In addition to the President's plan to provide greater assistance to First Responders, FEMA and ONP are currently implementing a number of other homeland security initiatives. These include:

- **Training Course Review**. The ONP is preparing a *Report to Congress on Terrorism and Emergency Preparedness and Training* that will include a complete accounting of all FEMA and Federal emergency and terrorism preparedness training programs and activities. The NDPO's *Compendium of Federal Terrorism Training* will be used as a baseline, supplemented by visits to a representative group of 10 cities to determine the effectiveness of the courses, unmet training needs, and the applicability of private sector training models.

- **Mutual Aid.** In conjunction with the First Responder Initiative, FEMA will work to foster mutual aid arrangements within States and between and among States so that the entire local, State, Tribal, Federal and volunteer network can operate seamlessly together. In building capacity, existing and new assets will be leveraged to the maximum extent by focusing on resource typing for teams, accreditation of individuals with using standardized certifications and qualifications, equipment interoperability and communications interoperability.

- **National Exercise Program**. The ONP will establish annual national exercise objectives, a multi-year strategic exercise program, and a national corrective action program. This will include development of an integrated exercise schedule.

- **Assessments of FEMA Regional Office Capabilities**. FEMA is in the process of reviewing the capabilities of our Regional Offices to respond to a terrorist attack.

- **Costing Methodology to Support State and Local First Responders**. The ONP is updating a methodology for better estimating the costs of building a viable local and State responder capability, to include developing plans, acquiring equipment, undertaking training, and conducting exercises to respond to terrorist attacks. The information will be used by FEMA to support the Office of Homeland Security in its effort to develop the National Homeland Security Strategy.

All of these activities will strengthen the nation's capability to respond to a terrorist incident.

Conclusion

Operationally, FEMA is well prepared and equipped to respond to an act of terrorism. Following a manmade or natural disaster FEMA will ensure that the Federal government and its partners provide needed support to disaster victims, first responders, and local governments. I look forward to working with each of you on this critical matter, as it will require a commitment from all of us to ensure its continued success.

Thank you, Mr. Chairman. I would be happy to answer any questions you have.

Mr. SHAYS. Mr. Caruso.

Mr. CARUSO. Mr. Chairman, thank you very much, members of this subcommittee. With your permission, I would enter my written statement into the record and just make a few points.

Mr. SHAYS. You can do that even without my permission.

Mr. CARUSO. The United States faces a serious threat. The No. 1——

Mr. SHAYS. Could you move your mic just a little close closer to you. Thank you.

Mr. CARUSO. We face a serious threat. The No. 1 threat is radical international jihad movement, and the No. 1 group within that movement is al Qaeda. We place at the doorstep of al Qaeda the following brutal horrendous attacks on American interests, both at home and abroad now: East Africa bombings of August 1998 we place at that doorstep; the bombing of USS Cole in October 2000 we place at the al Qaeda doorstep; and the September 11th attacks in New York and Washington against our country we place at the doorstep of al Qaeda.

The primary tactic of the radical international Jihad movement is attacks of large scale, high profile, and high casualty. A second category of international terrorists more clearly defined in some respects would be Palestinian Hamas, Hezbollah and other organizations. Director Mueller has changed the mission of the FBI. When he briefs the President, which is on a daily basis, the President of the United States does not ask Director Mueller how many people have you arrested today and how many people have you investigated today and prosecuted?

He asks what have you done in the past 24 hours and what will you do in the next 24 hours to prevent a terrorist attack—a terrorist attack against the United States?

What flows from a mission change is new thinking. Information sharing and gathering is crucial to that success. Under Director Mueller's leadership, we have changed, we have used existing channels of communication with Federal, State and locals, local police and public safety agencies in a way we had not leveraged before. We have also identified new methods because new thinking brings new methods of communicating information to our partners at the Federal, State and local as well as foreign, and when you share information, you also gather it.

We're also placing a premium on training of individuals worldwide to solidify the kinds of partnerships that we need to successfully win this war. No agency, no country can do this alone. Priorities for our—for funding purposes for the FBI with reference to the counter-terrorism program, our priorities match the priority targets of the radical international jihad movement as well as other international terrorist groups, and with those targets, we plan to apply the funds that the Congress gives us in areas that support what I would call a 360-degree attack against those targets, ranging from on ground investigation here in the United States to investigation overseas with other members of the U.S. intelligence community as well as our foreign partners and a variety of other areas which we can certainly discuss.

In conclusion, September 11th caused more casualties than any other terrorist act. I also add that terrorists have many different

faces, just not one kind of face, that the 19 hijackers who perpetrated this attack were very disciplined, and as a result of terrorists having many faces, and the discipline that these 19 exhibited, it's a very big challenge for the FBI and the U.S. Government.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you, Mr. Caruso.

[The prepared statement of Mr. Caruso follows:]

Testimony of Deputy Executive Assistant Director J. T. Caruso
Federal Bureau of Investigation
Counterterrorism/Counterintelligence

House Subcommittee on National Security, Veterans Affairs, and International Relations

March 21, 2002

Good afternoon Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to testify at this hearing on "Combating Terrorism: Protecting the United States". For the record, I am the Deputy Executive Assistant Director for Counterterrorism/Counterintelligence for the Federal Bureau of Investigation.

The terrorist attack of September 11, 2001, marked a dramatic escalation in a trend toward more destructive terrorist attacks which began in the 1980s. The September 11 attack also reflected a trend toward more indiscriminate targeting among international terrorists. The vast majority of the more than 3,000 victims of the attack were civilians. In addition, the attack represented the first known case of suicide attacks carried out by international terrorists in the United States. The September 11 attack also marked the first successful act of international terrorism in the United States since the vehicle bombing of the World Trade Center in February 1993.

Despite its unprecedented scope and destruction, the September 11 attack underscored many of the trends in international terrorism identified in recent years by the U.S. intelligence community. Among these has been an apparent shift in operational intensity from traditional sources of terrorism--state sponsors and traditional terrorist organizations--to extremist groups, organized under the Al Qaeda umbrella. This trend has been paralleled by a general shift in tactics and methodologies among international terrorists that focus on producing mass casualties. These trends underscore the serious threat that international terrorists continue to pose to nations around the world, particularly the United States.

At the same time, the United States also faces challenges from domestic terrorists. Threats emanating from domestic and international terrorists will continue to represent a significant challenge to the United States for the foreseeable future. Further, as terrorists continue to refine and expand their methodologies, the threats they pose will become even greater.

BACKGROUND

In general terms, the international terrorist threat to U.S. interests can be divided into three categories: the radical international jihad movement, traditional, clearly defined terrorist organizations, and state sponsors of international terrorism. Each of these categories represents a threat to U.S. interests.

The most serious international terrorist threat to U.S. interests today stems from Sunni

Islamic extremists, such as Usama bin laden and individuals affiliated with his Al-Qaeda organization. Al-Qaeda leaders, including Usama bin laden, had been harbored in Afghanistan since 1996 by the extremist Islamic regime of the Taliban. Despite recent military setbacks suffered by the Taliban and the apparent death of Al-Qaeda operational commander Mohamed Atef resulting from a U.S. bombing raid, Al-Qaeda must continue to be viewed as a potent and highly capable terrorist network. The network's willingness and capability to inflict large-scale violence and destruction against U.S. persons and interests--as it demonstrated with the September 11 attack, the bombing of the USS Cole in October 2000, and the bombings of two U.S. Embassies in east Africa in August 1998, among other plots--makes it a clear and imminent threat to the United States.

However, the threat from Al-Qaeda is only a part of the overall threat from the radical international jihad movement, which is composed of individuals of varying nationalities, ethnicities, tribes, races, and terrorist group memberships who work together in support of extremist Sunni goals. One of the primary goals of Sunni extremists is the removal of U.S. military forces from the Persian gulf area, most notably Saudi Arabia. The single common element among these diverse individuals is their commitment to the radical international jihad movement, which includes a radicalized ideology and agenda promoting the use of violence against the "enemies of Islam" in order to overthrow all governments which are not ruled by Sharia (conservative Islamic) law. A primary tactical objective of this movement has been the planning and implementation of large-scale, high-profile, high-casualty terrorist attacks against U.S. interests and citizens, and those of its allies, worldwide.

The second category of international terrorist threat is made up of the traditional and more clearly defined terrorist organizations. These autonomous, generally transnational, groups have their own personnel, infrastructures, financial arrangements, and training facilities. They are able to plan and mount terrorist campaigns on an international basis, and several actively support terrorist-related activities in the United States. Extremist groups such as Palestinian Hamas, the Irish republican army, the Egyptian al-Gama al-Islamiyya (IG), and Lebanese Hizballah have supporters in the United States, though the activities of these U.S.-based cells revolve primarily around fund-raising, recruiting, and low-level intelligence gathering.

Hizballah is a formal organization that has carried out numerous anti-U.S. attacks overseas, including the October 1983 vehicle bombing of the U.S. marine barracks in Lebanon. With the exception of the Al-Qaeda network, Hizballah is responsible for the deaths of more Americans than any other terrorist group in the world. On June 21, 2001, the United States indicted 14 subjects--13 Saudis and 1 Lebanese national--for their suspected involvement in the June 1996 bombing of Khobar towers in Saudi Arabia. Nineteen U.S. airmen died in the blast; Saudi Hizballah is suspected of carrying out the attack. To date, Hizballah has never carried out a terrorist attack in the United States.

State sponsors of terrorism make up the third category of international terrorist threat. The primary state sponsors are Iran, Iraq, Sudan, and Libya. These countries view terrorism as a

tool of foreign policy. Syria, which is also on the U.S. Department of State's list of state sponsors of terrorism, has not been directly involved in conducting terrorist activity for a number of years but still provides a safe haven to international terrorist groups and loosely affiliated extremists. North Korea and Cuba--also on the Department of State's list of state sponsors--have significantly reduced their direct involvement with terrorism due, in part, to the rapidly diminishing capacity of their economies to support such activity.

The trend toward high-profile, high-impact attacks comes at a time when interest is growing among domestic and international extremists in weapons of mass destruction (WMD). A series of anthrax-related cases and threats occurring since September 2001 provide a glimpse into emerging terrorist scenarios of the 21st century.

A series of bioterrorism incidents using b. anthracis spores sent through the mail have resulted in 22 anthrax cases and five deaths since October 3, 2001. The initial anthrax cases occurred among persons with known or suspected contact with opened letters contaminated with b. anthracis spores. Later, investigations identified four confirmed cases and one suspected case among postal workers who had no known contact with contaminated opened letters. This suggests that sealed envelopes contaminated with anthrax passing through the postal system may be the source of these exposures. The number of contaminated envelopes passing through the postal system is under investigation.

Leads continue to be investigated; however, no determination has been made as to whether this is the result of domestic or international terrorism and no suspect has been identified. On November 9, 2001, the FBI issued a behavioral/linguistic assessment of the offender based on the known anthrax parcels. As stated in this assessment, the offender is believed to be an adult male who has access to a source of anthrax and possesses the knowledge and expertise to refine it. The FBI heads a multi-agency effort to identify the perpetrator of these deadly attacks.

During the past several years the FBI had identified a wide array of cyber threats, ranging from defacement of web sites by juveniles to sophisticated intrusions sponsored by foreign powers. Some of these incidents pose more significant threats than others. The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area obviously would have greater consequences for national security, public safety, and the economy than the defacement of a web-site. Beyond criminal threats, cyber space also faces a variety of significant national security threats, including increasing threats from terrorists.

Terrorist groups are increasingly using new information technology and the internet to formulate plans, raise funds, spread propaganda, and engage in secure communications. Cyberterrorism--meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population--is clearly an emerging threat.

OFFICE OF HOMELAND SECURITY

The FBI's new, more focused mission is the prevention of future terrorist attacks. It must be understood, however, that protecting the United States and its citizens and overseas interests from terrorism is a national effort, involving federal, state and local government entities and the private sector. With so many different agencies involved in combating terrorism, the effort to lead and manage these efforts becomes inherently difficult. Subsequent to the attacks of September 11, 2001, the President issued Executive Order13228, which established the Office of Homeland Security. The mission of the OHS is to develop and coordinate the implementation of a comprehensive strategy to secure the U.S. from terrorist threats or attacks. The OHS is charged with coordinating the executive branch's efforts to detect, prevent, protect against, respond to and recover from terrorist attacks. Governor Ridge has announced that the number one priority for the Office of Homeland Security is to create a national planned strategy to effectively coordinate the homeland security efforts of all 50 states, U.S. territories, the District of Columbia, thousands of municipalities and countless private entities.

The Federal Bureau of Investigation has coordinated with and provided input into the Office of Homeland Security through various working groups and Policy Coordination Committees (PCCs) headed by the Office of Homeland Security to promote various homeland security initiatives and programs. These PCCs formulate plans for initiatives and policy matters involving National Guard support to Airport Security, Border Security Organization, Airspace Security, Horizontal Information Sharing, Vertical Information Sharing, and others. In addition, the FBI has detailed a senior Supervisory Special Agent to the Office of Homeland Security to fill the position of Directorate of Intelligence Fusion.

The FBI has been committed to working with the OHS, and it will continue to support the OHS directly. The FBI will provide the OHS with key technical assistance, from a crisis management standpoint, with the creation of a national strategy - as well as many other terrorism prevention efforts.

THREAT AND RISK ASSESSMENTS

A major threat to our nation's security is the use of weapons of mass destruction within our borders by terrorist groups, both domestic and international, hostile nations or individual extremists. In the Spring of 2001, the FBI entered into a partnership with the National Institute of Justice (NIJ) and the Technical Support Working Group (TSWG) in the development of an assessment of those chemical and biological agents that may be more likely to be used in the United States by a non-State sponsored terrorist. The FBI completed the technical review of the results by September 2001, however, additional revisions to the report are being made by TSWG prior to sending the assessment out for interagency review and concurrence. The FBI understands that the TSWG plans to provide a revised report for review in the near future. The FBI does not anticipate there will be any significant changes in the report's findings based upon the events of the past several months. For example, while prior to September 2001, the FBI had

not investigated any cases where anthrax use was confirmed, the topic was still included in the report due to its scientific and technical properties, including those factors which may make it a likely bio-terrorism weapon. The FBI will continue to examine law enforcement and intelligence information to ensure that the findings in the NIJ/TSWG report are accurate and helpful to State and local law enforcement.

In FY99, through the "Defense Against Weapons of Mass Destruction Act of 1998", Congress mandated that, "[T]he Attorney General, through the FBI, and representatives of appropriate federal, state, and local agencies shall develop and test methodologies for assessing the threat and risk of terrorist employment of weapons of mass destruction against cities and other local areas."

Congress also mandated that the Office of Justice Programs (OJP), Department of Justice, utilize a capabilities and needs assessment process in implementation of the Federal government's "FY99 State Domestic Preparedness Equipment Program." This program is designed to provide funding assistance to the nation's fifty-six states, territories, and the District of Columbia. Under this program, States and territories are required to award sub-grants to local jurisdictions based on results of jurisdictional needs assessments. The collection of the assessment data will be used to develop a statewide strategy for domestic preparedness equipment, training, exercise and technical support programs. These programs will assist the state in targeting available resources or activities having the greatest positive impact on levels of weapons of mass destruction (WMD) terrorism response preparedness.

Recognizing that a comprehensive needs assessment would require a threat, vulnerability, and risk component, and the FBI's current mandate requiring the development of the same, the FBI and OJP engaged in a cooperative effort to develop a single comprehensive assessment tool. In furtherance of this objective, the FBI developed a threat assessment process that is being utilized by state and local jurisdictions to help determine funding priorities for WMD domestic preparedness equipment and training. This process was integrated into a larger Needs Assessment process that has been distributed to all fifty-six states, territories, and the District of Columbia as part of the OJP FY99 State Domestic Preparedness Equipment Support Program.

After the terrorist attacks on September 11, 2001, the Attorney General directed all states and territories to complete their needs assessments and state-wide strategic plans as soon as possible. To date, 47 states and territories have submitted their completed package to OJP for review. The results of the individual state assessments are entered into a central database at OJP. The FBI is not currently in possession of those results.

The important work of OJP in the area of threat and risk assessment will be utilized and built upon as part of expanded First Responder Initiative proposed in the President's FY 2003 Budget.

COMPILATION, ANALYSIS AND SHARING OF INTELLIGENCE INFORMATION

It is apparent to everyone that the sharing of both criminal and intelligence information has become the most important tool in combating terrorism. The FBI must do a better job of sharing the information it receives, both through its criminal investigations of terrorist groups within the United States and the intelligence information that it receives from its own collection efforts and those of the Intelligence Community and other foreign services. The FBI has several on-going initiatives to enhance the cooperation between the FBI and other law enforcement and intelligence agencies.

In 1996, the FBI centralized many specialized terrorism operational and analytical functions in what was then called the "FBI Counterterrorism Center". The FBI counterterrorism center was established to combat terrorism on three fronts: international terrorism operations both within the United States and in support of extraterritorial investigations, domestic terrorism operations, and countermeasures relating to both international and domestic terrorism. This center was eventually overtaken when the FBI formally created the Counterterrorism Division. Eighteen federal agencies maintain a regular presence in the Counterterrorism Division and participate in its daily operations. These agencies include the Central Intelligence Agency, the Secret Service, and the Department of State, among others. This multi-agency arrangement provides an unprecedented opportunity for information sharing, warning, and real-time intelligence analysis.

This cooperation led to other important changes. During the past several years, the FBI and CIA have developed a closer working relationship that strengthened the ability of each agency to respond to terrorist threats and improved the ability of the U.S. government to respond to terrorist attacks that do occur. An element of this cooperation is an ongoing exchange of personnel between the two agencies. Included among the CIA employees detailed to the FBI's counterterrorism division is a veteran CIA officer who serves as the deputy section chief for international terrorism. Likewise, FBI agents are detailed to the CIA, and a veteran special agent serves in a comparable position in the CIA's counterterrorist center.

In addition to the CIA, since the mid-1990's, FBI's Counterterrorism Division in FBI Headquarters has been composed of FBI personnel and personnel representing the U.S. Intelligence and Law Enforcement community, including the NSA, DIA, INS, Customs, Naval Criminal Investigative Service, and Department of State. In return, FBI regularly assigns personnel to U.S. Intelligence Community Headquarters agencies all in an effort to expedite information sharing and processing.

FBI's Counterterrorism Division regularly collects raw and finished intelligence from Intelligence Community systems (Intelink) currently installed at FBIHQ and in about half of the field offices. These systems provide raw and finished intelligence reporting prepared by CIA, DIA, NSA and State Department on State-Sponsors of Terrorism and transnational terrorist networks/groups.

The FBI regularly participates in Interagency Intelligence Community Working Groups – CIA's Interagency Intelligence Committee on Terrorism: Monthly General Meetings and Warning and Forecast Meetings-- designed to share sensitive intelligence. Many of these working groups work jointly in combating various forms of transnational terrorism. These groups make every effort to track fugitive terrorists worldwide and render them back to the United States to face trial.

The FBI maintains a robust working relationship with multiple foreign intelligence services. Furthermore, FBI's Legal Attache Program, composed of 44 LEGAT's stationed overseas, works jointly with host foreign intelligence and law enforcement agencies in pursuing international criminals and terrorists wanted for outstanding violations.

In the aftermath of the terrorist attacks of September 11, 2001, the FBI established a threat assessment/prevention unit tasked with assisting current FBIHQ domestic terrorism and international terrorism personnel with assessing the potential threats existing in short and long term environments. Raw intelligence collected by the intelligence community is compared with investigative data accumulated by the FBI to determine the feasibility and credibility of threat information received in various venues.

The FBI has found that success against terrorism is best achieved through cooperation between the various federal, state and local law enforcement and public safety agencies. However, in order to more effectively combat terrorism, cooperation must extend beyond the mere exchange of information. Thus, the FBI formed Joint Terrorism Task Forces (JTTFs) to maximize interagency cooperation and coordination to create cohesive units capable of addressing the terrorism problems worldwide. The first Joint Terrorism Task Force (JTTF) was established in 1980. In 1996 Congress appropriated funds to establish additional task forces throughout the nation. We presently have 44 task forces, which include nine new task forces added since September 11, 2001. The FBI anticipates having a task force in each of its 56 FBI field offices by the end of this fiscal year. This would result in an increase of 21 new task forces this fiscal year.

To improve interagency terrorism related information sharing, the FBI Counterterrorism Division is piloting an "information integration initiative". This pilot program will facilitate having law enforcement and public safety agencies warehouse their agency data in a single secure database. The operational objective of this database is to facilitate terrorism information sharing between the FBI and the law enforcement and public safety community continuously. The goal is to have a field office operational this fiscal year with others to follow.

The FBI created a sub-file within the National Crime Information Center (NCIC) data base called the Violent Gang and Terrorist Organizations File (VGTOF). The subjects of counterterrorism investigations are being added to the file daily and are accessed by other Federal, State and local law enforcement agencies whenever these agencies access the system for the purpose of running criminal history checks on individuals of interest to their own

investigations (i.e., during routine traffic stops). When accessed by an officer, the system is capable of automatically notifying the officer that the name is of interest to the FBI and should be treated with caution. The system can provide further instructions such as, requesting the officer to notify the FBI of the reason for the inquiry and the results of that inquiry. The purpose of the data base is to share pertinent biographical information with other Federal, State and local law enforcement agencies for officer safety and mutual investigative interest.

Because warning is critical to the prevention of terrorist acts, the FBI also has expanded the terrorist threat warning system (NTWS) first implemented in 1989. The system now reaches all aspects of the law enforcement and intelligence communities. Currently, sixty federal agencies and their subcomponents receive information via secure teletype through this system. The messages also are transmitted to all 56 FBI field offices and 44 Legats.

If threat information requires nationwide unclassified dissemination to all federal, state, and local law enforcement agencies, the FBI transmits messages via the national law enforcement telecommunications system (NLETS). In addition, the FBI disseminates threat information to security managers of thousands of U.S. commercial interests around the country through the awareness of national security issues and response (ANSIR) program. If threat information needs to be directly provided to the American people, the FBI coordinates with the Office of Homeland Security to issue a threat warning under the Homeland Security Advisory System.

The FBI's Counterterrorism Division, after consultation with state and local law enforcement officials, has initiated the publication of a weekly FBI Intelligence Bulletin. This bulletin is intended for patrol officers and others who come in contact with the public on a routine basis. The publication is disseminated by several methods including Law Enforcement On-line (LEO), NLETS, and the Regional Intelligence Sharing System (RISS), administered by the Office of Justice Program, DOJ.

The above are just some examples of the FBI's on-going initiatives to share both criminal and intelligence information with other law enforcement agencies and the Intelligence Community as a whole. The FBI is also exploring additional avenues to share information with the public sector and companies responsible for the protection of the nation's infrastructure.

ESTABLISHMENT OF PRIORITIES FOR ADDITIONAL CT FUNDS RECEIVED

To effectively neutralize threats emanating from terrorist activities, the FBI must concentrate on both prevention and response. To this end, the FBI's Counterterrorism Division has developed a five-level strategy which focuses on building maximum feasible operational capability in order to identify, prevent and deter terrorist activities.

- Level one of this strategy focuses on maximizing the FBI's capacity to respond to terrorist issues as they present themselves in FBI field offices.

- Level two seeks to maximize the capacity of FBI Headquarters to receive, react to and disseminate information pertaining to terrorism-related issues.

- Level three is aimed at maximizing proactive capabilities to utilize resources Bureau-wide in support of the CT Program. (ie: the leveraging of key services such as analysis, language/translation and technology)

- Level four uses the establishment and maintenance of sound and productive relationships with external counterparts in the intelligence and law enforcement communities, defense establishments, foreign governments and state and local governments to obtain maximum support.

- Level Five seeks to build capacity by using all the necessary assets and capabilities of the FBI and external components of the US Government to support and initiate complex domestic and extraterritorial investigations and operations designed to get ahead of the threat by penetrating and neutralizing terrorist organizations.

In connection with these efforts, the CTD has established mechanisms for use in measuring the CT Program's progress toward applicable five year program goals and has focused its allocation of resources against noted performance gaps. The performance indicators used by the FBI's CTD serve to measure the CT Program's activities against the applicable program goals.

Under the FBI's mission of prevention, the top priorities of the Counterterrorism Division continue to be 1) enhancing the level of analytical support to the counterterrorism program; 2) enhancing the FBI's capability to electronically share information/intelligence and 3) enhancing the FBI's field offices capacity to respond to terrorist issues. The FBI measures achievements in these areas by focusing on the following indicators: 1) number of investigative matters pending, closed, and open during a specified period; 2) arrests; 3) locates; 4) informations; 5) indictments; 6) convictions/pre-trial diversions; 7) recoveries/restitutions; and 8) fines.

REORGANIZATION OF THE FBI

In December, with the approval of the Attorney General, we began a major reorganization of the FBI. The first phase of the comprehensive plan created a Headquarters structure that will help the executive team lead and manage the Bureau more effectively. As you know, it establishes four new Executive Assistant Directors who report directly to the Director of the FBI and oversee key areas: Counterterrorism and Counterintelligence; Criminal Investigations; Law Enforcement Services; and Administration. This structure reduces the span of control of the former Deputy Director position, a management concern raised here on Capitol Hill and in internal and external reviews of the Bureau. These changes also increase accountability and strengthen executive-level management oversight of day-to-day operations, and permit a greater focus on strategic management issues.

The reorganization addresses some of the other significant management issues and concerns raised by members of Congress and others in recent months as well. It is consistent with substantive comments culled from Congressional reports as well as various Administration and Congressionally-directed reports published since 1996. The reorganization creates a stand-alone Security Division, headed by an experienced professional from the CIA, to raise the security practices and standards to the level needed, to fix what the Hanssen investigation made painfully obvious. It also includes an Office of Records Management, led by an experienced records expert, to help modernize the record-keeping systems, policies, and processes to prevent another OKBOMB document situation. The reorganization elevated the position of Chief Technology Officer (CTO) so that the position reports directly to the Director. It establishes an Office of Law Enforcement Coordination that will not only improve relationships and information sharing with state and local police professionals and others, but will also help the FBI tap into the strengths and capabilities of its partners. The Bureau is working now to identify an experienced, qualified executive from state or local law enforcement to head this new office, someone who will help the Bureau understand how best to integrate state and local counterparts in the war against terrorism and into major investigations.

At the same time, the ongoing reorganization responds directly to the events of September 11th and the new environment by consolidating FBI oversight over the Counterterrorism and Counterintelligence programs. The new structure creates the Office of Intelligence, which will focus on building a strategic analysis capability and improving the capacity to gather, analyze, and share critical national security information. It also creates a new Cyber-Crime Division dedicated to preventing and responding to high tech and computer crimes, which terrorists around the world are increasingly exploiting to attack America and its allies. The old structure was fractured and not well coordinated. This change will bring together various cyber initiatives and programs under one umbrella, so the FBI is better focused, organized, and coordinated in working with our public and private sector partners to protect our nation's growing digital marketplace and electronic infrastructure.

The FBI is now beginning the second phase of the reorganization. As part of this phase, we are developing a comprehensive strategy to permanently shift resources to the fight against terrorism and in support of a massive prevention effort. The Director will present this strategy to the Department, Administration, and the Congress soon. The FBI is working to identify areas where we can redirect resources without compromising our investigative priorities or our partnerships with law enforcement and other government agencies. Given the gravity of the current terrorist threat to the United States, the FBI must make hard decisions to focus its available energies and resources on preventing additional terrorist acts and protecting our nation's security. At the same time, we will continue to pursue and combat international and national organized crime groups and enterprises, civil rights violations, major white-collar crime, and serious violent crime consistent with available resources and the capabilities of our federal, state, and local partners. We want our mission driven by the simple principle that whatever we do, we will devote the resources and expertise to be the best in the world.

ADDITIONAL STEPS WHICH NEED IMMEDIATE ATTENTION

The FBI's top priority is the prevention of any further terrorist acts in the United States or against U.S. citizens and interests abroad. The FBI was provided with an increase in investigative personnel for its counterterrorism program in FY 2002. We are now in the process of hiring and deploying these positions. However, an effective investigative capacity not only involves putting Agents on the streets, it also requires strong programs and resources to support these Agents. These resources include surveillance operations; technically proficient, well-equipped, and well-trained personnel; effective response capabilities; and the ability to combat terrorism in the cyber arena These resources have been requested. The resources are need to, among others, expand the FBI's LEGAT program; fund and train the additional personnel required in the field offices (both Agent and Analysts); and train federal, state and local law enforcement agencies in the complexities of terrorism investigations.

CONCLUSION

Despite the current focus on international terrorism, it is important to remain cognizant of the full range of threats that confront the United States. These threats continue to include domestic and international terrorists. The 169 lives claimed in the Oklahoma City bombing and the potential very heavy loss of lives that could have resulted from various thwarted plots, demonstrate the interest among some domestic extremists in inflicting mass casualties.

On September 11, 2001, the scope and sophistication of the international radical jihad movement was demonstrated with horrendous clarity when 19 hijackers commandeered four commercial airliners, crashing two of them into the World Trade Center, one into the Pentagon, and the other into a remote field in Pennsylvania. This attack resulted in more casualties than any other terrorist act ever recorded.

Even as the Al-Qaeda command structure in Afghanistan is destroyed, Al-Qaeda cells in countries around the world will continue to pose a threat to U.S. and other western interests. The plotters who carried out the September 11, 2001 attack maintained a low profile and appeared to actively avoid coming to the attention of law enforcement agencies. Such operational discipline underscores the challenge to U.S. law enforcement agencies in uncovering and disrupting Al-Qaeda cells in the United States. Although the public mind often groups international terrorists into a standard stereotype, such a view fails to accommodate subtle but important differences in goals and tactics among different extremist movements. Despite the military setbacks suffered by Al-Qaeda, extremists adhering to the international jihad movement will continue to focus on attacks that yield significant destruction and high casualties, thus maximizing worldwide media attention and public anxiety. It also appears likely that as governments "harden" official targets, such as Embassies and international schools, these terrorists will increasingly seek out more vulnerable "softer" targets, such as high-profile offices of multinational firms and Americans traveling and working abroad.

Terrorism represents a continuing threat to the United States and a formidable challenge to the FBI. In response to this threat, the FBI has developed a broad-based counterterrorism program, based on robust investigations to disrupt terrorist activities, interagency cooperation, and effective warning. While this approach has yielded many successes, the dynamic nature of the terrorist threat demands that our capabilities continually be refined and adapted to continue to provide the most effective response.

Mr. SHAYS. Lots of opportunity for questions in your statement that was not delivered, in other words, your whole statement, and I appreciate your entire statement and I appreciate your summary. Look forward to asking questions.

Mr. Greene, you're going to close up and then we're going to get to all of you in our questions.

Mr. GREENE. Thank you.

Mr. SHAYS. By the way, I just want to thank again your willingness to participate in a full dialog, because there will be some exchanges, and I was feeling a little guilty in thinking you have to listen to the testimony of some of your colleagues. I don't always like to listen to the testimony of all of my colleagues. Sometimes it's a mutual thing here but——

Mr. KUCINICH. I love to listen to you, Mr. Chairman. I just want that on the record.

Mr. SHAYS. But I think it's important that you hear each other, isn't it? So there's some good to this. So excuse me.

Mr. Greene.

Mr. GREENE. Thank you. I will be brief, Mr. Chairman. I'd like to thank you and the members of the committee for the privilege of being able to talk today about the——

Mr. SHAYS. I'm going to ask you to lower the mic. That's the one to your left, the one that magnifies——

Mr. GREENE. OK. And this is the one that picks——

Mr. SHAYS. So use the one to your left and just slide it in an angle that way.

Mr. GREENE. All right. Is that better, sir?

Mr. SHAYS. That's good.

Mr. GREENE. OK. Thank you. It's a privilege for me today to talk to you today about the—the work of literally thousands of dedicated men and women in the Immigration Service, and what they're doing to set new priorities and strengthen our border security in connection with the overall effort to enhance our national security. Since the terrorist attacks, the INS has taken a number of steps on its own initiative to increase domestic security, and some of these we've already discussed with this committee.

We dispatched over 300 border patrol agents to major airports in the immediate aftermath of the attack to increase security at airports. We committed 50 percent of our special agent resources and maintained that level of commitment for the first 3 months after the attacks in order to support the FBI in their investigation of these attacks and auxiliary matters that grew out of that.

This occurred within the framework of the Joint Terrorism Task Force and of the recently newly established antiterrorism task forces that the—that the Attorney General had established. We also detailed an additional contingent of border patrol agents to the northern border to provide additional security along that border. More importantly, very quickly after the attacks, we coordinated with a number of important agencies to increase the—reduce, rather, the vulnerability of our visa entrance process and the process by which people come to the United States.

With the Department of State, we have expanded the screening process for overseas consular officers in connection with the visa issuance processing. We have also made—the Department of State

has also made available to us temporary visa application data that is now available to INS inspectors at the port of entry where they do their work. With the Department of Treasury Office of Foreign Assets Control, we've assisted in the identification and freezing of assets, a project of which you all have widely heard.

But our most productive partnership to date has been with the Federal Bureau of Investigation. We've worked with the FBI on leads that have arisen directly out of the attacks themselves. The intelligence and information that we gathered with respect to movement of people in and out of the United States was of material assistance to that investigation. We have interviewed with the FBI and with State and local law enforcement agencies, people who have been identified as potential witnesses that would be useful not only in the direct investigation, but also in our counterterrorism efforts.

With the Department of State, we've taken steps to tighten our procedures regarding passengers traveling without visas into the United States and also tightened our refugee processing. We have worked under the umbrella of the antiterrorism task forces with State and local agencies and the FBI in an—an initiative that is currently directed at identifying, locating, arresting and removing from the U.S. people against whom final orders have been pending for years.

We have worked with the Department of—with the Office of the Inspector General in the Department of the Interior, with the Department of Labor and with the FBI on an initiative called Operation Tarmac, which was ordered to be begun within days of the attacks. This is where agents of the Immigration Service working with FBI, working with the Department of Transportation, have identified employers whose employees have access to secure areas of major airports and other critical national infrastructure locations.

To date, we have looked at over 800 employers. We have examined records pertaining to over 200,000 people. We have arrested over 100 people in connection with this initiative on various charges including immigration violation, and that effort is continuing. We have worked with the FBI and national security agencies under the framework of the interagency working group, an arm in the Department of Justice that is responsible for looking at international smuggling and we have identified and are working on a number of significant law enforcement cases that will materially affect the security—the national security of the United States.

Finally, I'd like to say that the INS has had to redefine its priorities and look overseas as well in ways that we have not had to before, and frankly this is the critical area where the INS has—has worked successfully, and well with the Office of Homeland Security.

As you know, the Commissioner of the Immigration Service proceeded to Ottawa several months—rather in December to work with the Canadians on the groundwork which led to the Ridge-Manley document. Our Commissioner accompanied Governor Ridge to Mexico to initiate and participate in discussions there with respect to border security.

We are in fact stepping forward to reset our priorities in terms of extending the ambit of our concern outside of the ports of entry at airports, outside of the port of entry at land borders, and to the places where people are originating to come to this country, and we think that there is great promise in these bilateral negotiations with Mexico and Canada, not simply with respect to the national security interest, but also with respect to some of the more festering problems that we have faced in the national migration discussion that we've had in this country for more than 10 years.

That concludes my remarks, Mr. Chairman and Members. I'll be happy to take your questions.

[The prepared statement of Mr. Greene follows:]

U.S. Department of Justice
Immigration and Naturalization Service

STATEMENT

OF

JOSEPH R. GREENE
DEPUTY EXECUTIVE ASSOCIATE COMMISSIONER
FOR FIELD OPERATIONS
U.S. IMMIGRATION AND NATURALIZATION SERVICE

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND
INTERNATIONAL RELATIONS

REGARDING

COMBATING TERRORISM: PROTECTING THE UNITED STATES

MARCH 21, 2002

2247 RAYBURN HOUSE OFFICE BUILDING
1:00 P.M.

Thank you for the opportunity to testify today on "Combating Terrorism: Protecting the United States." Since September 11, the Immigration and Naturalization Service (INS) has responded, in conjunction with other agencies, to perform direct law enforcement activities, provide identification and intercept capabilities, increase border security, supply intelligence information and complete investigative and detention functions with the goal of strengthening national security.

We are conducting these efforts along with our other immigration mission responsibilities. The focus on national security and counter-terrorism has enhanced enforcement efforts and strengthened enforcement policies.

Today, I will describe how the INS is strengthening our border security, setting priorities, and working in coordination with the Office of Homeland Security. Some examples of the joint efforts we have pursued to enhance our Nation's security follow:

- We are working with the FBI and other members of Joint Terrorism Task Forces on the investigation of the September 11 attacks, and to remove from the U.S. persons identified in the course of that investigation, where appropriate;

- We have been working with the State Department to expand data sharing to ensure that Immigration Inspectors have access to the issued visa information in the Consolidated Consular Database. As a result, this information is now available at all

U.S. ports-of-entry (POEs), and we have trained our inspectors on how to use it to detect and prevent fraud, particularly imposters;

- Immediately after September 11, the INS, and other Department of Justice components and the State Department developed new criteria for scrutinizing visa applicants, which are now in place. Together, we also accelerated plans to reassess the eligibility of six countries to participate in the Visa Waiver Program and we have joined with the State Department to tighten regulations regarding various entry procedures that under ordinary circumstances facilitate travel, but which could be exploited to do the U.S. harm;

- We are working with the Treasury Department's Office of Foreign Assets Control to identify and freeze the assets of terrorist organizations and their various front groups, and to pursue removal proceedings, when possible, against principals and directors of those organizations and fronts;

- We worked with other agencies and the Office of Homeland Security to develop 7 interagency initiatives for refugee program security enhancements. These includes additional database, records and fingerprint checks, and pre-flight notification to the FBI,

- We have been working diligently with the U.S. Coast Guard, the U.S. Customs Service, the Department of Energy, and the Department of Defense to improve container inspection and tracking. Together these agencies will coordinate development of chemical, biological, radiological and other nuclear detection devices to increase our inspection capability.

STRENGTHENING BORDER SECURITY

Ports- of-Entry

Since September 11th, the Inspections Program has focused its resources on meeting our Threat Level One operating instructions. Threat Level One commitments include: staffing all small and remote land ports 24 hours a day/7 days a week[1]; ensuring that all flights are fully inspected at their first POE; completing record checks of those seeking admission; completing enhanced checks of vehicles as they cross the land borders; and working with the U.S. Coast Guard and other agencies to safeguard our seaports. This increased commitment to thorough and accurate determinations will affect the more than five hundred million persons who are inspected at our POEs every year. The post-September 11th procedures put into place at POEs have strengthened the enforcement posture of the Nation and contribute directly to improved border security.

[1] All land ports-of-entry are staffed, with the exception of two POEs, one in Alaska and one in Montana, that are closed because they are seasonal ports. Appropriate steps have been taken to ensure that both locations are monitored.

In order to support and sustain Threat Level One operations in terms of monitoring and security at our land POEs, we requested support from the Department of Defense (DoD). This request was supported through $34 million provided in the recent emergency supplemental. INS will reimburse DoD for personnel and equipment support to Inspectors at the POEs and to Border Patrol Agents between the POEs. The DoD is supplying personnel to land border POEs to provide a heightened security presence, assisting in physical inspection of vehicles, and performing traffic management and pedestrian control duties. Between the POEs, the DoD is supplying technical and administrative support to sector intelligence centers, helicopters in six sectors, and assistance in deploying sensing and surveillance equipment. This partnership is helping the INS to maintain Threat Level One anti-terrorism operations to protect the integrity and security of our border.

The INS also has increased its use of Passenger Analytical Units (PAUs) at air and sea POEs. These units generate tactical information for inspectors engaged in determining whether a non-citizen seeking admission to the United States is admissible. Using the Advanced Passenger Information System (APIS) in conjuncture with the Interagency Border Inspection System (IBIS), INS PAU inspectors are able to precisely analyze the passenger arrival and departure information. Combined with other passenger information systems or information obtained through on-line airline reservation systems, inspectors can make associations between suspected fraud and smuggling activity and, through link analysis, identify individual enforcement targets before the passengers arrive in the United States for

inspection. This critical work assists the INS in identifying illegal aliens, criminals, and terrorists that attempt entry.

The Border Patrol

In 1994, the Border Patrol implemented a four-phased multi-year national strategy to deter, detect and apprehend illegal entrants, smugglers and contraband along our 8,000 miles of border. The strategy directed a phased forward deployment of personnel, equipment and technology along the Southwest Border and then along the Northern Border, Pacific, Atlantic, and Gulf Coasts.

Following the events of September 11, the Border Patrol undertook a number of enforcement initiatives to assist in supporting and augmenting U.S. national security. Within 36 hours of the attacks, the Border Patrol detailed 318 agents to 9 airports across the country. Additional agents were detailed to POEs on both the Northern and Southern borders to assist with providing security and to facilitate the entry of legitimate commerce. In January, 100 agents and additional air assets were detailed to the 8 Northern border sectors to augment existing capabilities and expand coverage within the sectors' areas of responsibilities. The Border Patrol, working in cooperation with the U.S. Coast Guard, conducted joint operations on the Great Lakes and surrounding waterways to deter illegal entry and apprehend violators. 245 new agents from the FY 2002 appropriations and the

counter-terrorism supplemental will be deployed to the Northern Border, resulting in a 67% staffing increase over FY 2001 levels.

The Border Patrol is also working with the Royal Canadian Mounted Police, Citizenship and Immigration Canada, Canada Customs and Revenue Agency and U.S. Customs to establish Integrated Border Enforcement Teams (IBETs) at several key locations along the Northern Border. IBET teams serve as a "force multiplier" by combining team personnel, resources and technology to enhance border integrity and security at our shared border with Canada. IBETs operate as intelligence-driven teams to address terrorism and identify and investigate persons and organizations that pose a threat to national security or are engaged in other criminal activity.

With the FY 2002 regular appropriations, and the counter-terrorism supplemental appropriations, we will continue to deploy agent staffing, technology and support resources to meet our long-term border management objectives to maintain and extend control along the Southwest Border and increase control along the Northern Border.

INVESTIGATIVE PRIORITIES IN THE INTERIOR OF THE UNITED STATES

The Investigations Program has responded to this crisis in a number of ways. Although the INS continues to investigate anti-smuggling activity and to identify and arrest criminal aliens, antifraud and other violations of immigration law, our highest priority is to

support the criminal investigation of the terrorist attacks of September 11 and the war on terrorism. INS Investigations Program has 2,246 Special Agents authorized to accomplish these tasks.

INS Investigations Program is conducting several initiatives to enhance national security, such as the Alien Absconder Project and work-site enforcement investigations which focuses on airports and other sensitive installations. INS Headquarters directed each Region to initiate work-site investigations into the hiring practices of companies employing people who work at airports and have direct access to commercial aircraft and other secure areas.

In the aftermath of the September 11th terrorist attacks on the United States, the INS Anti-Smuggling Program is focused on dismantling smuggling organizations with links to terrorism and others that pose a risk to the national security of the United States. Investigations of these organizations play a vital role in the INS' overall homeland security efforts.

The INS, along with other agencies, target alien smuggling organizations that pose a serious threat to the national security of the United States or are linked to terrorism. The INS participates in an interagency working group (comprised of the INS, the FBI, and other Department of Justice components, the Department of State, the Central Intelligence Agency, the National Security Agency, and the U.S. Coast Guard) which coordinates the

government-wide response on various alien smuggling issues. The INS Anti-Smuggling Program accords top priority to investigations of the organizations targeted by the Interagency Working Group.

In addition, the INS Anti-Smuggling Program is currently conducting "Operation Southern Focus," an initiative in Central and South America and the Caribbean, involving the investigation and prosecution of organizations identified by the interagency working group as smugglers of special interest aliens. Generally, special interest aliens are from countries hostile to the United States or where global terrorist groups are known to have operated or recruited. Agents have been detailed from various domestic offices to overseas locations, where they are working under the direction of the INS Officers in Charge in conjunction with Department of State and the host country governments, to develop investigations and prosecutions against targets. Those targets are being prosecuted, either by the Transnational Unit of the U.S. Attorney's Office in Washington, DC, or in another appropriate venue.

FOREIGN TERRORIST TRACKING TASK FORCE

The INS has a leadership role on the Foreign Terrorist Tracking Task Force. The Task Force serves to facilitate communication and coordination among the INS, the FBI, the Treasury Department led by the U.S. Customs Service, the State Department, and other

agencies that are tasked with counter-terrorism responsibilities. It is a multi-agency task force that leverages agency expertise to produce intelligence to keep terrorists and their supporters out of the United States and detect and remove those who may already have entered our country. The INS and other Task Force agencies coordinate their efforts to develop lead information on counter-terrorism-related subjects and to neutralize the threat of alien terrorists.

COORDINATION WITH THE OFFICE OF HOMELAND SECURITY

The INS and other components of the Department of Justice are enhancing enforcement efforts and strengthening our government's counter-terrorism efforts, through coordination with the Office of Homeland Security, particularly in our relations with Canada and Mexico. In December 2001, Commissioner Ziglar headed an INS delegation to an Office of Homeland Security-led international conference in Ottawa, Canada, that included representatives from the Departments of Justice, Transportation, Defense, State, and Treasury. An important product from that conference was a Smart Border Declaration signed by Homeland Security Director Tom Ridge and Canadian Deputy Prime Minister John Manley. The Declaration includes 30 initiatives aimed at enhancing security along our shared border. The INS was a major contributor to this agreement. By working together, the United States and Canada will create a more secure border.

Earlier this month, Governor Ridge, Commissioner Ziglar, and other senior Administration officials traveled to Mexico City, Mexico, to develop broad-based proposals for strengthening our joint security and to build on recent cooperative efforts with the Mexican government.

CONCLUSION

The Administration and Congress are working together to enhance our Nation's security. We at the INS will use every means at our disposal to mobilize personnel and resources in the most effective way. We look forward to continuing to work closely with Congress and other federal agencies to combat terrorism and protect the American people.

Thank you for this opportunity to appear, Mr. Chairman. I look forward to your questions.

Mr. SHAYS. Thank you very much. Let me say that I'm going to start out with Mr. Putnam and then go to Mr. Kucinich. We're going to do 10-minute questioning. When a Member asks you a question and you ask a question of one of you and you want to jump in, you know, just try to stick your finger up and let that Member know that you would also like to make a contribution. It's their discretion on whether they want to use their time in calling you forward, but I would hope the Members, given that we have as much time as we need, would allow for that interaction.

You all are involved interacting in some way. We need to get—to see how this is working. We'll have a number of questions. We'll get right to it and, Mr. Putnam, you have 10 minutes.

Mr. PUTNAM. Thank you, Mr. Chairman. Mr. Greene, it has been not exactly a chamber of commerce a couple of weeks for your agency. Tell me, if you would, if the INS has run the names of the other 17 terrorists to ascertain whether or not they have documents pending within the INS.

Mr. GREENE. Yes, sir, they are and they are doing it a second time, and I think we're working a third time now.

Mr. PUTNAM. And under the Patriot Act, there was also a provision that prohibited INS from issuing visas to relatives of known terrorists. What steps have been taken to comply with this provision?

Mr. GREENE. It's my understanding that enabling regulations are in the process of being worked on that. I don't have a date for you, but—as to when that will be done. I'll be happy to provide you with the status report on that effort.

Mr. PUTNAM. What is being done in the meantime?

Mr. GREENE. Well, right now, as the commissioner has testified before the Judiciary Committee last Tuesday, we have a complete freeze on all of the documents, the I–20's, for example, which were the issues. All of the applications that have been filed with the INS that are pending with the INS and that will be filed are being run through our IBIS system which contains our lookout system before they are adjudicated. There are a number of other steps specifically with respect to schools. Some of the loopholes that we—that our analysis of this event disclosed, such as allowing students to begin their course of studies before the change of status had been approved, have now been closed. You will not be able to study in the United States, if you're already here without the change of status having been officially adjudicated, and I will tell you that the effort to tighten the process of visa application is ongoing and continuing.

Mr. PUTNAM. Thank you. Dr. Raub, Director Ridge spoke at a food safety summit on March 14th and indicated that one of their priorities was to consolidate the functions of food safety and inspection. At various times Secretary Veneman and Secretary Thompson have each indicated that one of our key vulnerabilities is in our food safety system. We have—if you make a cheese pizza—if you have a cheese pizza factory, you have one agency inspect you. If you throw pepperoni on it, another agency inspects you. When we go to our airports and seaports, if we're bringing in fruits and vegetables, you have one set of inspectors. If you're bringing in meats, you have a different. How far along is that planning, and please elaborate on that consolidation plan.

Mr. RAUB. I've not been involved directly, sir, in the details of those discussions, so I can't provide more than some very general knowledge. I know that the two Secretaries have been in precisely those discussions with the staff and the Executive Office of the President. In the short run, the emphasis has been on strengthening the respective capabilities in our department and the Department of Agriculture, in our case, through the Food and Drug Administration by expanding the number of inspectors and seeking broader authorization for inspection capabilities, focusing on especially the ports and other activities.

I know the discussions will continue about the pros and cons of consolidation of those regulatory structures, but the objective is the same in any case, and that is to strengthen and ensure that our highly centralized system of food production and distribution is not vulnerable.

Mr. PUTNAM. Is there a specific objective that any of the agencies have outlined where we're going to move the number of cargo containers inspected from 3 percent to 15 percent or from 12 percent to 70 percent? Is there any specific, tangible, measurable, quantifiable goal that we can view the homeland security budget and the consolidation plans and the added emphasis on information and detection and be able to measure progress?

Mr. RAUB. I don't have those numbers with me, sir. I'll be glad to provide them.

The FDA has as part of its budget development and justification laid out the goals it believes it can achieve with the expanded work force of inspectors and with the new authorities.

Mr. PUTNAM. I'd like to—very much to see that. I look forward to receiving it.

Mr. Burris, the—one of the key issues that this subcommittee explored long before September 11th in its discussions over homeland security and the competing legislative proposals involved improved coordination and communication and standardization of equipment, interoperability of equipment among local first responders, among the myriad of State and Federal agencies. What has been done to standardize our communications equipment, our decontamination procedures, our detection equipment, and what is—what is the blueprint for progress on that?

Mr. BURRIS. Well, our FEMA IT directorate is undertaking the responsibility to provide some type of standardization within the communications arena. There's a lot—there's several, you know, manufacturers. It has to do a lot with the type of spectrum that's available to public safety users for their radios. While, you know, I doubt that we'll ever be in the business of telling a first responder community or telling a local community which radios they're going to buy, we can go about the business of identifying the specifications of what that equipment is, and we're working with the FCC to do just that. Some of the other compatibility issues revolve around working within a common incident command system or—and issues in that arena, and we're working on that.

There happens to be a lot of consensus-based standards in this country, and they're voluntarily used around the country. Part of what our responsibility will be is to encourage wider adoption of

those consensus-based standards by local communities and the States.

Mr. PUTNAM. Mr. Verga, there have been reports that prior to the September 11th attacks, at least one of the terrorists involved in the flights that—in the flight that struck the Pentagon was known by the CIA to have met with a group of Malaysian—a known terrorist organization in Malaysia. He then entered the United States before that information was transferred to the INS and subsequently to the FBI. Have we successfully cleared the hurdles of intelligence-sharing, and have we improved the communication between agencies with primarily nondomestic responsibility and those with domestic responsibility, or are there still jurisdictional barriers that are clouding up our communications capacity?

Mr. VERGA. Let me say, first of all, I have no personal knowledge of that particular incident that you—I reported, and of course the director of Central Intelligence would probably be better in a position to address the overall coordination among the intelligence community.

I will say from the Department of Defense's perspective, we recognize it as a challenge, and we're working very hard to be able to get the information, and I would differentiate between information and intelligence, because what is needed at the local level to deal with problems is the information that—for example, the State patrolman needs to know that an individual is somebody who is on a watch list that, when he stops him for a traffic stop, he needs to make further followup. That can be differentiated from the source and the method by which we obtain that information, and the Department of Defense is working as part of the intelligence community to be able to develop a system that will allow that information to get transmitted down to the level that it needs. We're making some progress. We have—we do have a long way to go.

There are issues of classification of information. There are issues of how do you transmit the information over secure means, and we are working with that. For example, during the Olympics in Salt Lake City, we solved the problem essentially by establishing a classified facility on one floor of the major headquarters used for Olympic security, where defense and all intelligence information was funneled into it, analyzed, and then sanitized to put out to be used during the security operation.

Mr. PUTNAM. Mr. Caruso, perhaps the FBI would like to add to that.

Mr. CARUSO. Thank you very much. I'll go back to the phrase that was used earlier, new thinking, as an effect that ripples out well beyond this so simple a phrase. The U.S. Patriot Act is one example of the Congress's leadership in fostering agencies that share information. In the U.S. Patriot Act, the prohibition of sharing Federal grand jury information was lifted. That allowed us and the FBI and others in the law enforcement community to share information with the intelligence community. It's something that wasn't—existed before, and that was an important—an important—important door to open. So from a legislative point of view, that's something that was really very helpful.

New thinking also goes beyond—it goes into policy, and people look—struggling with an issue and coming about it in a new way.

For example, through the National Law Enforcement Telecommunications System, it's called NLETS, it's the way the FBI communicates with other Federal agencies, as well as police departments across this country. Shortly after September 11th, we with the U.S. intelligence community made a conscious decision to take classified information and declassify it and send it out through the National Law Enforcement Telecommunications System, NLETS, and that goes to thousands of police departments and public safety departments across this land, reaching hundreds of thousands of policemen and public safety men and women. Before September 11th, that did not occur. After September 11th, that kind of new thinking brought on that kind of information-sharing, and information-sharing is a two-way street, because when you share information, you're providing essentially leads for policemen and women, and you get information back, and it's a two-way system.

So there are just two examples of some of the new thinking that occurred, one because of legislative leadership, and the other because people sat back and thought anew.

Mr. PUTNAM. Thank you. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much. At this time I would recognize the ranking member, Mr. Kucinich, for 10 minutes.

Mr. KUCINICH. Thank you very much, Mr. Chairman, members of the subcommittee. As I'm sure all of us would agree, democracy and accountability thrive on openness and universal access to information, and that's why this committee has held over two dozen open hearings on terrorism. We've heard from virtually every agency involved with counterterrorism. We've had experts—panels testify. We've sought advice from the GAO. And one constant theme through our witnesses that we've heard over and over is that we need to put one job above all others, and that is a job of conducting a comprehensive and analytical assessment of whatever threats or concerns that our country might face. And it's been suggested over and over that without this assessment, we have no way of knowing what the priorities should be, that our strategies wouldn't be fully informed, that our budget may not be key to what might be the most dangerous concerns we face. So we've had this repeated recommendation, conduct a comprehensive threat assessment, figure out priorities based on the assessment, craft a strategy to address these priorities and link up the budget. And as I indicated earlier, our committee actually sent a bipartisan letter to the President detailing our findings, recommending that the office's first priority be to conduct a comprehensive assessment.

I'll ask Mr. Caruso, are you familiar with that issue of a comprehensive threat assessment?

Mr. CARUSO. Mr. Kucinich, I know that there is an interest in creating and developing a national threat assessment. That's as best as I can frame that.

Mr. KUCINICH. Did the FBI actually begin one a few years ago, like 1999? Was the FBI involved in starting to put together a threat assessment?

Mr. CARUSO. The FBI has conducted a number of different threat assessments. There was an effort in—I know that in 2001. It may have started in 1999. I do not know that. But in 2001, there was

an effort to put together a national threat assessment, and as it was progressing, the September 11th attacks occurred, and suddenly, as you can—as you understand, everyone moved to that.

Mr. KUCINICH. So that was—that assessment by the FBI was basically put aside. Is that——

Mr. CARUSO. Yes. The FBI is—since September 11th, which is the timeframe I can speak to, since September 11th, we have an ongoing national threat assessment, and you see that ongoing, national threat warnings, and ultimately you see it in the proposal that Governor Ridge has made with reference to his national threat warning that is now out for public comment. So that would be an ongoing threat assessment.

Overall, the FBI has conducted about 85 or so threat assessments that are event-specific or site-specific. For example, they will do a threat assessment when Pope John was here in 1999, and in the midwestern Ohio. We would do one—we also did one for, of course, the 2002 Olympics. So the FBI's overall consistent thrust has been threat assessments that are based either on an event or a specific site, not national——

Mr. KUCINICH. Right. The one that—the one that started a few years ago was an attempt, from what I understand, anyhow, that there was an attempt to establish a generalized assessment, and I understand what you have told this committee, in that the FBI has been dealing with some of these things on a case-by-case basis, but generalized, you did—you did at some point start a generalized threat assessment that was——

Mr. CARUSO. Yes. I also believe that a generalized threat assessment is too broad for the kind of dynamic country that we have, in the sense of size and complexity, to have much meaning to it even before it's published, because things do change. So my own personal opinion and professional opinion is that a national threat assessment is not quite as valuable a tool, that you could turn into actual—actionable items.

Mr. KUCINICH. Yes. What I'd like to know, I mean, just—and let me say that I appreciate the work of the FBI, that I feel that the FBI has done everything it can to help this country, and I think generally the people of this country appreciate it. What we're trying to figure out here is that how do you know your priorities if you don't have an assessment, how do you develop a strategy? You know, because we don't have anybody from the Office of Homeland Security here who could help guide us. Does the FBI have any recommendations that you might want to address to the public as to what steps might be taken to be able to assure the public that the big picture, which is really what this office is about with this $38 billion budget, that the big picture is going to be addressed?

Mr. CARUSO. I need to defer to Governor Ridge for the bigger picture. All I can speak for is the FBI, and what I would say is we do know the No. 1 threat that faces the United States and it's al Qaeda in the terrorism area, and we know that because we have investigations that—of the East Africa bombings in 1998, the USS Cole in 2000, and now the September 11, 2001. Those investigations and information that we've gotten from our partners in the intelligence community and that partnership is crucial to success, as well as our partners overseas, point to al Qaeda, which is the

No. 1—the No. 1 terrorist that the United States—threat that the United States faces so it's the investigation and the sharing of information that leads us to the conclusion, and I think it's shared by the U.S. Government, that al Qaeda is the No. 1 group that we need to be concerned about. That's not to the exclusion of others, but that group, that sometimes amorphous group, has caused extraordinary damage to us, as we all know.

Mr. KUCINICH. Well, I thank the gentleman for his answer and I just want to point out that I—you know, as you said, you can't answer for Governor Ridge. I respect that. We're talking about two different things. One is that—the very sharp specific focus of the response of the FBI to whatever challenges come up—you come up with a plan, you learn about something—as opposed to just a general broader picture.

So I respect that you can focus on that one and respond well as you did.

Now you indicated that al Qaeda is not the only problem we face. One of the things that I thought was instructive in your testimony was you cited a number of groups, including—in addition to al Qaeda, you cite extremist groups such as Hamas, Hezbollah, al-Gama'a, al-Islamiyya, and then you also mention the Irish Republican Army. In all of the hearings I've been in, this is the first time that I've heard a reference to the Irish Republican Army in the context of activities in the United States. I guess what I'm looking for is a response as to how—it's the first time I've heard of that. Would you like to tell this committee what the—what kind of activity the IRA has in this country?

Mr. CARUSO. Our interest in the IRA is—in this country is in the area of garnering funds to support violence overseas, garnering funds for—funds for—from individuals here in the United States and also weapons, of procuring weapons here and shipping them back overseas to support a violent cause. We have examples of that—an example of that is in the—in our Miami division in Florida a year or so ago, maybe a bit more, but it's primarily fund-raising to support violence, as well as weapons.

Mr. KUCINICH. Yes. Again, it's the first time that I had heard that. So under the Patriot Act, then, if someone had given funds to any of these organizations, they then would be subject to prosecution. Is that correct?

Mr. CARUSO. I can't speak exactly to the Patriot Act. The case I'm talking about occurred before the Patriot Act, so we were able to use existing laws that were there to prosecute these individuals.

Mr. KUCINICH. You're talking about something in the past, then, not something going on right now?

Mr. CARUSO. Not—I'd rather stick—I'd rather remain with the case that I cited, because that's been through the public and the judicial processes, etc. Etc. is not the word I want to use, but——

Mr. KUCINICH. I think I get the gist of what you're saying there, and I respect that.

I'd like to—how much time do I have, Mr.——

Mr. SHAYS. Probably about—how much time is left? 40 seconds. You've got a good minute.

Mr. KUCINICH. Mr. Chairman, thank you very much for this opportunity to ask these questions, and I'll yield back. It's OK. Thanks.

Mr. SHAYS. At this time I would recognize Ms. Watson.

Ms. WATSON. I'm going to yield some of my time back, because I can't spend the whole 10 minutes, but what I've noticed is that the further we are away from the attack sites, the quicker people are getting back to their regular routine. I represent an area that abuts the airport, LAX, and we have gone after airport security with a great passion, but what I see on the West Coast could be a threat to our waterways. We get water from the Colorado River, from the dam and so on. Our transportation system may be a big tanker full of high octane gasoline running directly into a wall, that suicide mission. Our borders and our seaports. Just anyone along the panel, maybe the FBI, would want to comment on what are our short-range priorities and long-range priorities in addressing these various systems? That's what is troubling to me. When I go back to my district and hold one of these forums, they want to know where the nearest bunker is, and do we have water there and what kind of food will be there, because they expect terrorism will continue, this time on the East—West Coast. So can someone respond?

Mr. MCHALE. The Transportation Department has got a number of different programs that address some of your concerns. We do not deal with the water supply. So I'll leave that to one of my fellow panelists. But on the—on port security, we have a number of programs, including some in Los Angeles and Long Beach that address where we place sea marshals on ships, particularly ships carrying hazardous cargo, and the sea marshals stay on that ship as it comes into port to make sure that it remains secure and to protect the navigational stations on that ship.

In addition, you mentioned tanker trucks carrying hazardous cargo. Our Federal Motor Carrier Safety Administration has conducted almost 40,000 visits to companies that have hazardous material licenses and has talked to those companies about safety measures that they should take, reporting a suspicious activity, checking their records and licenses of various individuals employed by those companies. And in the course of those, they referred over 100 cases to the FBI.

It's a vast system. The transportation system is a huge system, and we're trying to look at it in a comprehensive way, but we really have to leverage all of the resources of the State and local governments, as well as the Federal Government, and frankly the private sector. The responsibility is very broad. The airlines and the airports have very much stepped up to the plate. We've gotten terrific competition—terrific cooperation from the trucking industry and the railroad industry. The broader we work with them and communicate with them, I think the stronger we're going to be. TSA is only about 2 months old, so we've got a long way to go, but the other administration modes—modal administration of Transportation have been doing a terrific job outreaching to their specific transportation modes, trying to raise awareness and to give them appropriate points of contact within the Federal Government to report suspicious activity.

Ms. WATSON. Since our country is so vast, so broad, have we considered a regional approach to securing these different systems and a coordinated effort here, maybe homeland security? I do know there's been difficulty communicating across the various department lines, but would it not be better in the nooks and crannies of this country to work out a plan that would address these categories I just mentioned?

Mr. CARUSO. Ms. Watson.

Ms. WATSON. Please.

Mr. CARUSO. Governor Ridge's proposed homeland security advisory system is out for public comment, to improve it if it can be, but it lays out a foundation of warning. And if you have an opportunity to take a look at the various colors——

Ms. WATSON. Yes. I——

Mr. CARUSO. With each one of the colors comes an increasing level of vigilance, and so—and that can be—and that threat warning can be applied to the Nation, to a region, to a section. So that would be one way for individuals to be able to—they best know their critical locations, and this system would be a step in the direction of allowing them to take a uniform precaution, a uniform understanding as to what they need to do and their fellow citizens need to do to protect certain vital critical key assets.

The second is that there is a—the National Infrastructure and Protection Center, NIPC, which is a multiagency center which has very good connectivity with what we call the eight industrial communities, telecommunications, banking, finance, and they have a very good connectivity and growing increasing good connectivity with the various businesses and those industries. And that's another method to target, if you will, industries that there's a particular threat that's been leveled against. And so you have those two systems which are very much complementary in raising the bar with reference to awareness and then responsiveness to that.

Ms. WATSON. Two systems just failed. One was Bank of America and its deposit system. You know, I'm just wondering how we are going to assure that the systems are up and functioning, and I look at the INS, it's been the whipping boy in the last few weeks, and maybe rightfully so. I think probably what you need—and I understand there's a new structuring. You probably need more resources to hire more people and train them better, more educational dollars and so on. But my concern still is what do we know, and I'm talking about the Members—we have to go back to our district. I'll be on a plane in less than an hour—and we have to assure our——

Mr. SHAYS. Excuse me. You've got to be on a plane in less than an hour?

Ms. WATSON. Well, I'll be leaving, not on the plane.

Mr. SHAYS. Mr. Verga wanted to know how you were going to do that.

Ms. WATSON. Going through the security, it will be more than an hour.

But we have to be able to be partners in all of this, and when we go back, we have to assure those American people out there that we got it under control. I try not to tell them about September 11th, but we need to know something concrete that we can take back to our Governors, our mayors, our board of superviser mem-

bers and so on, something concrete. I have seen the color system on television, heard about it on the radio, read about it in the newspapers, but it still doesn't tell me anything. I know what green stands for and red and so on. You know, I know the levels, but what's behind all of that? And so we need more clarification. Maybe we should get a one-on-one in secret. I don't know. Because I guess when we have our briefings, there are too many people in that room and too many people listening in. But I'm looking for concrete information. I'm not getting it.

Mr. GREENE. If I may respond to that, please, there are a couple of concrete things I can tell you that buildupon the statement that I made up front about the increased partnership of the FBI, and there have been two things I can point to immediately. The first is that very soon, like within a day or two of the attack on the United States, that some total of INS information with respect to people coming to the United States was delivered to the FBI. The kinds of information that we collect and then have to analyze in order to determine the movements of certain people or to be able to even do some predictive work with respect to folks coming into the United States, the fusion point for that kind of information is now the Foreign Terrorism Tracking Task Force, which I believe the committee has been briefed on, and that provides a concrete step toward the kind of information-sharing and the kind of analysis that we need to do to complete the kind of prevention work that the Attorney General has said is the strategy for the FBI, the INS and the justice components in that regard, and I want to keep this short because I know you have a plane to catch.

Ms. WATSON. I'll yield back my time, Mr. Chairman.

Mr. SHAYS. Thank you very much. And thank you for being here today.

Mr. Clay, you have the floor.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. SHAYS. We're just starting new time.

Mr. CLAY. Mr. McHale, let me ask you, has there been an assessment of the new airport screener process since the new public law went into effect?

Mr. MCHALE. We have an ongoing assessment, and we're actually still in the process of Federalizing the work force. We took over the private sector contracts on February 17th. We have worked to some extent to improve that process. We're engaged in a very detailed planning to how we will operate the screening check points when we bring in the Federal employees, but the first Federal employees will not be reporting until some time in May. So I'm not sure that answers your question or not, but we're engaged in a very—very detailed assessment of the current screening process.

Mr. CLAY. In the meantime, I read a pretty disturbing report about the lax security at the Salt Lake City airport during the Winter Olympics. I don't know, have you all looked at that situation?

Mr. MCHALE. Yes, we have. We've appointed an associate under secretary for inspection, David Holms. He's been on the job about a month, and we received—we received that report about—about 2 weeks ago, and Mr. Holms and his staff, which is still growing, small and growing, like our entire agency, has actually assigned

some people to go out there and look at that and report back to us as soon as he can.

Mr. CLAY. And they will make recommendations to that airport and hopefully others that——

Mr. MCHALE. I think that's right. The situation in Salt Lake City, of course, was, I think, quite extraordinary. I mean, it's huge, huge influx of people into a relatively small airport, but I think we can probably draw some lessons from that we can apply nationwide.

Mr. CLAY. How about your—the current status of the Federal air marshal program? How is that going?

Mr. MCHALE. I can't discuss in an open session the numbers of Federal air marshals, but I can tell you that the program has greatly expanded. We have been greatly assisted by the other Federal agencies, some—many of whom are here, by assigning to us on detail many of their criminal investigators who are serving as temporary Federal air marshals, and we at Transportation are greatly increasing that program.

Mr. CLAY. OK. Thank you for that.

And, Dr. Raub, tell me, are you familiar with the precautionary measures that are in place in the postal service as far as mail handers who handle the mail on a daily basis, and if you are, are you pleased with the precautions?

Mr. RAUB. I'm not aware in detail, sir. I know that considerable attention has been expended through the Centers for Disease Control Prevention and the post office with respect to that. I think that will be a continuing effort of—to ensure the level of improvements that are necessary.

Mr. CLAY. Does your office meet regularly with the Homeland Security Office here?

Mr. RAUB. Yes, sir. Not only does our secretary and deputy secretary meet regularly, but the director of our office, Dr. Henderson, is in frequent contact with Governor Ridge and other senior staff there.

Mr. CLAY. OK. OK. Thank you for that.

And, Mr. Caruso, you noted in your opening statement that al Qaeda was the No. 1 threat to this Nation. Can you give us any indication of what their strength is today and where they are? Do you know? I mean, I read a recent report that they may be in Indonesia, and may have left Afghanistan and went to Indonesia. Do you have any information on that?

Mr. CARUSO. Sir, terrorism does not have one face. It's made up of individuals of various nationalities and hail from various countries. We believe that al Qaeda is—al Qaeda sympathizers are spread in many places around the world, just not in where these 19 hijackers came from. It would be unfair to say that's where they came from, that all terrorists are based there. We find them not only in the Middle East, but we find them in places in Southeast Asia and in other locations as well.

With reference to the numbers, I think individuals of good will could vary on that, and so I don't think there's a precise number. I think what you're—what will be there is a dedicated group, hard core. How many that is, I do not know. It might be several thousand, and then you have a concentric circle that goes out of individ-

uals who are less dedicated but would be there to lend a hand if a situation presented itself, and then you have a larger group who are just sympathizers who would not be participants, but to put hard numbers on them, I don't have them, nor does anyone else.

Mr. CLAY. OK. Along those same lines of thinking, when you talk about terrorism not having any single face, does the—has the Justice Department and the FBI paid attention to the sensitivity as far as Arab Americans and Muslims, because, you know, history tells us that when we use a broad brush and say, for instance, in World War II when we locked up an entire race of people or a lot of them, it comes back to haunt us, through reparations, through lawsuits. Is that going to happen a few years out from today where we come back and look and say, oh, we made a terrible injustice. We painted this group with a broad brush. I mean, for instance, the guy that's locked up in Virginia, I'm sure you all have more information than I on—Moussaoui is his name, I think? I mean, is this going to come back to haunt us?

Mr. CARUSO. The FBI is very cognizant of its—of the investigative tools that we have and the need to use them for the good. The rule of law is what we are guided by, and we are pledged to uphold. At the same time where we are vigorously investigating with over 4,500 agents, we are utilizing over 4,500 agents to investigate the attack of September 11th, at the same time we were conducting civil rights investigations and hate crime investigations, because there were unfortunately Arab Americans, innocent Arab Americans, and the vast majority of them are, who were the victims of hate crimes, who were the victims of just absolutely un-American kind of activities. And so at the same time we're vigorously investigating the 19, we were out conducting an investigation to prosecute, and we have prosecuted individuals who have set upon these very, very innocent people.

At the same time, we've also gone out through the individual leaders of our field offices, 56 across the Nation, and they have gone out and reached out to the—into the Arab American communities, to the mosques and other cultural centers, to extend a hand because they are part of the community we're there to protect and we've made that a conscious effort, because without the cooperation of the American people, the FBI is not going to be effective, and we want to be effective.

Mr. CLAY. I appreciate your response, and thank you. Thank you all for your testimony. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you, Mr. Clay, for being here and for your nice and your helpful questions.

I'm going to proceed with 10 minutes, and then Mr.—Dr. Weldon will have some questions, and then I'll have some questions again. I would just like to say before I begin that Nick Palarino, who is next to me, has always insisted for years that I not ignore a doctor when they are before me. I called you Mr. Raub, and he said Dr. Raub, and I never figured out why he was so insistent, until I realized on February 2nd of this year he got his doctorate. He'd been working on it for so many years, so I would like the record to note that you will no longer be Nick to me. You will be doctor, Dr. Nick. Congratulations, Doctor.

What brought that on was I was noticing that I had professional staff, and we had counsel there before. He happens to be the director, and I was thinking, if I was the director, I'd rather have professional staff than counsel.

I have a number of questions, and I'm going to start by, this is what I believe. This is what I believe: I believe that we are at war with terrorists, that we have been at war with terrorists for over 20 years and didn't know it. They did. We didn't. That this war with terrorists is a fight to the finish, that it is a fight to shut terrorists down before they use chemical, biological agents, which we believe they have, heaven forbid, radioactive material or, even worse, nuclear weapons which they may have. If you ask me do our terrorists have nuclear weapons, I say I don't know. I don't think so. But that makes an assumption that every time a terrorist nation tried to buy nuclear weapons, we caught them. If you ask me will terrorists have nuclear weapons, the answer is yes. I'm absolutely convinced of it if they don't have it now. And if you said there was a nuclear explosion, heaven forbid, in this country, would I be surprised, the answer would be no. So for me the stakes are very high, and I think for every one of you here.

And, Dr. Raub, I note when we had the anthrax attack, there was a real sense that if the terrorists used anthrax the way they could potentially use it, what we encountered would look like a cake walk. In other words, as serious as that was, it could be far, far worse. So we all know the stakes are very, very high.

And I think it is very helpful to have all of you here. You all play a role in what we knew we had to address in the 19 hearings we had before September 11th. We had all three commissions come before us, the Kramer Commission, the Hart-Rudman Commission, the Gilmore Commission, all saying to us we don't have a proper assessment of the terrorist threat, we don't know what our strategy is, and we aren't organized to deal with it. And we're in the process of doing all three. It's difficult for us to have an assessment of where we're at, because really the only one who has anything dealing with homeland security in a general sense is you, Mr. Verga, and you're not Tom Ridge. And I know Tom Ridge.

So having said that, we're using all of you to help put the pieces together, but there's going to have to be a time, and I have to say this, in which the administration is going to recognize that while they're seeking to protect the advice and counsel to a President of someone who is close and intimate to the President, Mr. Ridge, that ultimately there has to be a process for Congress to respond to, and that doesn't require a yes or no from any of you. You have your own roles to play, but I want to state that for the record.

And I want to state for the record that ultimately I believe that the assessment of the threat will require a strategy that will require some reorganization of government where we will have potentially a homeland office.

Now, Mr. McHale, let me start with you. When we passed legislation dealing with terrorist threat as it related to protection of airplane travel, I will say something else I believe. I don't believe airline travel today is safe. I believe it will be safe, but I believe that it is still possible for terrorists to get explosives on an airplane, particularly if they're willing to ride an airplane, and since we had

19 go under riding an airplane, we know that's not going to inhibit them, the old strategy.

Now what I'm interested in knowing is we put a law that said originally in the House check for explosives the end of 2003. That was legislation that was pushed by me and others, and the reluctance was that we didn't even know if we could do it by 2003. What was fascinating was when it came back from the conference committee, it said by the end of the year—I don't mean 2003. By the year 2003, that by the year 2002 now it has to be done.

Now we don't have the equipment yet to check for explosives on an airplane, so I need to understand what it means by the legislation language that says you will check all baggage by—it's—the date has already passed. It doesn't say for explosives. It just says you'll check all baggage. So help sort that out to me. We need a candid conversation, and we'll go from there.

Mr. MCHALE. There are two dates in the statute. One is within 60 days of enactment, we had to screen all baggage for explosives, ideally using explosive detection equipment or—and then Congress listed a number of alternative means if we couldn't do it. The second is a date the end of the year, December 31st, by which we have to screen all checked baggage using explosive detection equipment, with very limited flexibility there.

We met the deadline of January 18th, I think it was, by using explosive detection equipment where it was located. We required that it be used to the maximum extent possible. We had discovered that a lot of the equipment that had been out there—and there weren't very many machines out there but the equipment that was out there was not being used full time, and we mandated that it be used if it is operational, that it be—being used.

Mr. SHAYS. So is it fair to say we're using all the equipment available, but we don't have enough equipment to check all bags?

Mr. MCHALE. That's right. So we supplement it with dogs, with manual search, and with origination bag match, all of which were things that Congress recognized that would probably be the only tools available to us on that short a timeframe.

To get to the end of the year, we have really worked on a multiple strategy. There are two manufacturers in the United States of what are called EDS machines. Those manufacturers are relatively small. In the past they produced a relatively small number of machines every year. We've been working with them to get them to ramp up their production, but we've also worked with them to procure the intellectual property rights to their products on a license basis, and we are going to be using additional—the assembly of these machines is not actually as difficult as it is to develop them. So we can use additional manufacturing facilities to put the machines together with the intellectual property rights. So we're going to be able to greatly increase the production.

And we're also going to be using other equipment to help us deal with some of the issues that machinery raises. So there's a lot of—we're proceeding on a lot of tracks.

We're also in the process of testing some additional explosive detection equipment to see if we can certify it and add to the total—I guess the total types of machinery that are available to us.

Mr. SHAYS. OK. Let me ask you, though, the very clear answer is not all baggage is checked yet for explosives?

Mr. MCHALE. All baggage is subjected to some form of check, but one part of that check may be the origination bag match, which is to ensure that the passenger gets on the plane with their bag or that the bag does not get on the plane without the passenger.

Mr. SHAYS. Now if you were walking on the plane, you take the risk that your baggage will be randomly searched?

Mr. MCHALE. That's right.

Mr. SHAYS. But if you load it on the plane, it's less likely that it's going to be opened up? Correct?

Mr. MCHALE. We use a lot of different techniques. It is—you know, I don't—we don't open up every bag at the passenger check point either so——

Mr. SHAYS. No. I understand. There's a difference. There is a random check process. You don't have a random check process to open up baggage that's in the belly of an aircraft.

Mr. MCHALE. We do.

Mr. SHAYS. How do you? Most of the baggage is locked. You destroy the lock? What do you do?

Mr. MCHALE. We use—as I said, we use explosive detection dogs. We use EDS equipment when it's available.

Mr. SHAYS. Here's what I asked you. You don't open up a bag?

Mr. MCHALE. There are bags that are opened up at the baggage check-in point. If there is a reason to open the bag, we will call the passenger over and we will open the bag.

Mr. SHAYS. So your point is that it's a—is that the first round? That was 10 minutes. Boy, it goes quick. Let me just pursue this and then we'll go right to Mr. Weldon. I want to be clear on this. You're saying that the way you make it random is that sometimes before it's sent down, they check it right on the spot?

Mr. MCHALE. There is a process that we use to identify individuals whose bags we want to check very carefully, and those bags are generally opened—they can be opened, or they can be checked by explosive detection machine, or they can be checked by a canine or whatever else is——

Mr. SHAYS. OK. So what you're saying is your sense of search isn't necessarily that it is opened up, but if you suspect a bag, you're going to make a second pass.

Mr. MCHALE. Right.

Mr. SHAYS. With an animal, with—I'm told animals have hundreds—dogs have—certain dogs have hundreds—thousands of—hundreds of thousands of times the capability of smell that humans do.

Mr. MCHALE. Yes.

Mr. SHAYS. That——

Mr. MCHALE. The dogs are very effective.

Mr. SHAYS. Yes. That's what I've been told.

OK. Dr. Weldon. Dr. Weldon. I'm sitting next to Dr. Nick.

Mr. WELDON. I just have a quick followup question on the random searches, Mr. McHale. I've gotten some complaints from constituents, elderly people, young women carrying babies, families with small children coming up on the random checks. Have you any information that these random checks have uncovered any po-

tential terrorists getting on planes since September 11th, or dangerous materials? And when I say dangerous materials, I don't mean, you know, the little pen knife that the Secretary of the Air Force gave me 4 years ago that they took away from me shortly after September 11th. I mean—it's—you know, my concern is, you know, aviation is a big part of our domestic economy, and there are a lot of people who are saying I'm going to drive, mostly out of fear of flying, but I have had some people—constituents complain about the random searches. Can you give me some information that I can tell my constituents about these——

Mr. MCHALE. There is a 2-week period—unfortunately I don't have all of the statistics here but there's a 2-week period from the first 2 weeks we took over the check points. We took over the check points on February 17th and during the first 2 weeks of that time, we confiscated over 100,000 items. Probably a lot of those were little pen knives and things, but among that were 40 weapons, firearms, a number of them loaded, a large number of knives in excess of 3 inches and other things, box cutters, etc. So there is a—there is a lot of material still being recovered at check points. But we, too, are concerned about the number of searches of individuals who fall in those kind of categories——

Mr. WELDON. Perceived as harassment——

Mr. MCHALE. I don't think it's harassment. The system we've got set up is one—we use the cap system to identify individuals. That's still a somewhat crude tool that we're working very hard to refine. That will actually pick up some—many individuals who probe—who certainly are not terrorist terrorists.

Another thing, though, is that we also do have random searches. We have a certain number of passengers who are identified for random search, particularly at the gate as they board. And last, a requirement that we put into place right after September 11th that is still in place is that the individuals who stand behind the check point and use wands to check passengers should be fully occupied so that if there isn't someone who is alerted by going through the metal detector, at a time they will actually call someone over to check them. That again is another form of random search.

We actually have a number of projects under way to make our checks a lot more sophisticated. Improving the cap system is a project that we are engaged in with the hope of deploying the new system by September, and one of the problems we have at the passenger check point today, as those passengers arrive, they arrive anonymously. We don't have a way at most passenger check points to know who's arriving at that check point to be checked. Not until you get to the gate do we often know who you are.

Mr. WELDON. I hate to interrupt you, but I'm going to run out of time. You answered my question right at the beginning. You've discovered weapons, and you feel that the random checks are justifiable—well, he's saying something to me that I think you really ought to look at. Women with small babies, you know, I guess it's within the realm of possibility that somebody would do that. The terrorists that we're facing, I believe, are the most diabolical and demonic opponent America has ever faced.

But I have a question for you, Mr. Greene. And maybe we can get back to this issue. But as you probably are aware, Congress

provided in the USA Patriot Act some requirements on the INS to develop access and sharing of intelligence and criminal background information, a tamper-proof machine-readable passport and tamper-proof and machine-readable immigration documents as well, along with the development of a biometric evaluator like an iris or fingerprint scan. Also we provided resources for the expedited implementation of this visitor tracking system.

Mr. GREENE. Yes, sir.

Mr. WELDON. It's been a few months. Can you report to us the status on implementing a lot of these——

Mr. GREENE. Just in two areas, and I can provide a fuller piece on this after the hearing, but we have a project manager in charge of the entry/exit system now that is looking at the technical side of the sorts of questions that will have to be in place in order to make an entry/exit system a viable system for us. We know that in the airport environment and, to a slightly lesser degree, the seaport environment, it is a—it is not anywhere near as challenging as it is at a land border environment, and so the plan, as I think it has been discussed, is to look at a phased implementation starting with the—in the airport environment at first and then proceeding directly to overcoming the more difficult technical challenges.

Mr. WELDON. Well, it's safe to say at best for months, and some cases we're years away, from implementing most of these provisions.

Mr. GREENE. Well, I don't know. The entry/exit system is on a very fast track. I think we're looking at I want to say airports by the end of this calendar year. That's my recollection. I can confirm that with you when I get back to the office. In terms of the—in the meantime, we have a companion piece which arises out of the Congress's Data Management Improvement Act, where the private sector who are affected by this is also being folded into this process of development, so that the exhibition impact, especially at land borders of entry, again are sort of evaluated and their concerns taken into account.

Mr. WELDON. Well, I just want to share with you, Mr. Chairman, that while the INS is making its best effort to implement all of these features, some of the provisions in the act are months away. Some of them are actually years away, and that we do have a period of vulnerability where the Immigration and Naturalization Service cannot protect our borders from the continued ongoing entry of terrorists in the United States, and that's why I think I've spoken to you before, I've introduced legislation to place a moratorium on entry from about 15 nations that are known to sponsor, harbor or produce terrorists.

I just—I have a followup question for you, Mr. Greene. I spoke with Congressman Hal Rogers who used to chair the appropriations subcommittee that had the INS jurisdiction, and he informed me that the budget for the INS was double to twice during the 1990's. The impression I get is that with 11 million visas that are issued every year, and I don't know what the figure is, several hundred million tourists and students that are coming in and out of the country and people who come back and forth and back and forth, that even with all of these added resources, that the agency is totally overwhelmed.

Mr. GREENE. Well, I think the commissioner, Congressman, has looked at the problems facing the INS in a number of different dimensions. The first one certainly is a resource question. The budget growth that Congressman Rogers described to you is accounted for primarily by the increased assets that were placed on the southern border to address a problem that was, you know, demonstrably out of control in the beginning of the 1990's.

In addition to the sort of management issues that the INS faces, which the commissioner intends to address through his restructuring plan, we also have problems with information management which he has indicated he would like to address through chief information officer appointed, working for him and under him, and the current process that we're looking at, the enterprise architecture project which we're looking at to sort of standardize and consolidate the various discrete information systems that have been set up through the INS over the last 25 years to address specific missions and specific problems that arose.

It is more than a resource problem, clearly. I think the recent events have demonstrated that, and I think the commissioner has acknowledged that it is more than a resource question and he is taking steps to address those issues as well.

Mr. SHAYS. I would like another round here, and if you can stay, we can go back. I would like to ask each of you, first off, is there any question that was asked of someone else that you had made notes that you wanted to comment on before we go? Is there any comment that any of you would like to make based on any question that has already been asked? Yes, sir.

Dr. RAUB. Just a brief comment related to Representative Watson's comment before. I think appropriately her question and the response of my colleagues keyed on prevention and securing infrastructure and interdiction of events, but there's a corollary side of detection and response in areas and particularly related to biological terrorism, and the only point I would have made—points, there were two, one is that this spring, thanks to the President and the Congress, we are investing more than $1 billion in the upgrading of State health departments, local health departments and hospitals, with a major emphasis on improving infectious disease surveillance and response such that we could detect and respond quickly to a biological event, and I believe that was important in the context of your questions because that preparation has to be uniform across the country. A communicable infectious disease starting in any one place, given our mobile society, could quickly end up in any number of other places. So it's important that our protection be as nearly uniform as possible.

Second, while we're—bioterrorism is our No. 1 concern, we recognize that the most likely type of terrorist event remains the conventional explosive or variance thereof, and so we need to continue investing in the—the medical response systems with respect to burn and trauma and other types of medical consequence management.

Mr. SHAYS. Thank you. When we had our hearing last week, one of the witnesses basically—let my preface my comment by saying that in the early 1950's, President Eisenhower recognized we had a new threat, we had a new assessment of threat, we had a new

strategy, and we reorganized, and that was the cold war. And it was a whole different war. It lasted 40-plus years, and ultimately we were successful. It was based pretty much on containment and responding to acts of aggression. It was based on mutual assured destruction, and we basically outlasted the Soviet Union economically, politically, socially, and militarily.

The new strategies—the new type of response suggested by I think former Ambassador Bremer on counterterrorism is that we need to detect and to prevent—that a mutually assured destruction would guarantee basically we would mutually destruct each other, that it would in fact happen given that people have a different sense of the value of life.

I'm interested in knowing from each of you, do you think it is reasonable, based on your side of the equation, for us to assume that the Office of Homeland Security will be able to come up with an assessment of the total threat and to integrate it to all your different parts, that it will be possible to develop an overall strategy much like we did, and do you ultimately see that would require some reorganization of government?

Now I'm asking you all to go a little outside your box, but, Mr. Verga, not as much for you. This is probably more apt for you to respond to, and maybe Mr. Caruso, but all of you are welcome to respond.

Mr. VERGA. Thank you very much. First of all, let me say we—we in the Department appreciate the leadership that the Congress has taken on this issue and, quite frankly, those of us in the executive branch recognize that in some cases Congress was out ahead of us in looking at the homeland security problem in a more holistic way than—than we have looked at it, and we appreciate that leadership.

It's clear that traditional ways of looking at a threat, counterthreat-based strategy, are not adequate for this situation that we find ourselves in. By the same token, the flexibility that's necessary to deal with these asymmetric threats and essentially nondeterrable actors because to be—be able—for deterrence to work, the other actor has to be a rational actor, and in this case they're not rational actors, as you pointed out—requires that we have a great deal of flexibility and moreover a capability——

Mr. SHAYS. Can I—just since you attributed it to me, it's rational to them, though, isn't it?

Mr. VERGA. I would not pretend to be an expert on their culture. I think that they think that the acts that they take have a purpose in their—in their way of looking at it. So you could probably say it's rational, but——

Mr. SHAYS. It's not our way of——

Mr. VERGA. True, that's a good point. What I was about to say is that in order to be able to accomplish and to have an effective strategy in—in this world of asymmetrical threats, we have to be much more flexible, much more adaptable, and move more toward a capabilities-based approach, particularly in the defense arena as opposed to trying to say you've got tanks, we have to have tanks, you've got airplanes, we have to have airplanes, because you can't find those—those symmetries that you can balance off against. So that's why you find that we're moving in those types of directions.

With regard to trying to do a threat assessment, you somewhat run up against the same problem in that if you guess wrong or even if you analyze wrong of what the threat is and you counter that threat, you may have missed the one that you end up facing, just as we did on September 11th and, therefore, if you move toward analyzing vulnerabilities that you find inside your own system and then develop capabilities to counter those vulnerabilities, it may give you a better strategic way of approaching this problem of asymmetrical threats.

Mr. SHAYS. Would anyone else like to respond? Because I have a followup. Anybody? Yes, sir, Mr. Burris.

Mr. BURRIS. Yes. If I could, I think—and I want to echo sentiments on this capability assessment. You can go about this in a different manner, as opposed to, you know, a threat assessment, by doing a capability assessment, and FEMA's done just that, assess, you know, States' capabilities to handle catastrophic disasters.

A good example is the REP program which does our nuclear power plants, provides for preparedness initiatives around our nuclear power plants. Whether or not you have a radiation incident from a nuclear power plant because it's accidental or because it's intentional, you still have to have the capability to deal with it. And so a part of, I think, the first responder initiative that the President's put forward is just to do that, to address as a down payment, as it were, some of the capabilities that we know need to be racheted up for our local and State responders to be able to handle those incidences, should they take place. So while the vulnerability assessment is certainly important, I think we have a beginning point by moving forward with the capability assessments that's taking place in the States by the Department of Justice, by FEMA, after September 11th and other agencies as a starting point to start off in preparing our country.

Mr. SHAYS. Yes, sir. Dr. Raub.

Mr. RAUB. Mr. Chairman, in a similar vein I'm optimistic that the executive branch and the Congress can make some considerable progress toward a broader base of assessment and a better integrated look at the various threats and their consequences.

For example, in the area of biological terrorism, over the last several years we have consulted extensively, not only with the medical and public health community, but with the intelligence community, the law enforcement community and—and others, and have been able to develop what we think is a strong list of what the major threats are, either because the probability is high or the consequences of their use are enormous. We'll continue to build on and refine that, but we believe that can and should be integrated with a broader look.

In our case, as I indicated before, our responsibilities are primarily those of early detection and medical and public health response. We need to rely heavily on others to interdict those events in the first place, whether they be from other nations, whether it be through law enforcement. We have a limited role ourselves in the regulation of the transfer of certain hazardous materials called select agents, but we need to be an integral part of a larger effort from the whole scope from prevention and interdiction all the way through detection and response.

Mr. SHAYS. Well, what I'm struck with is that when we were dealing with the Soviet Union, our strategy, our assessment was pretty simple when you came right down to it. It was symmetrical. We matched them, they matched us, we tried to not make it a fair fight and to have superior whatever they had. Here we—it being asymmetrical, we don't know where it will come from and we don't know what it will be. And so, for instance, I wonder if we decide that we have a pretty good idea that if it's a biological agent, it's going to be this kind of a biological agent, we almost can't make that a public disclosure because then our enemies say, well, they're wise to this, we'll do this. And the only thing I have comfort with right now, the only thing, really, is that we are going to hold the country accountable that allows the terrorist act to take place in that country, and that simplifies it. But I mean—and then Dr. Weldon will have the floor here, but we had one of our witnesses say to us his biggest concern that relates to your area is that a group of cottage industry scientists will develop an altered biological agent that will wipe out humanity as we know it.

So it's a real determination that we have great intelligence work and also law enforcement efforts to uncover this, but I guess what I'm saying is in the end when we hear from Homeland Security, are we going to have—do you anticipate that we are going to have a strategy that we can put—an assessment that we can put on one page and a strategy that will fit on another page, or will it fill an encyclopedia? I dated myself.

Mr. RAUB. Or a CD ROM, perhaps.

Mr. SHAYS. Yes. Just let me get a response to that and then, Dr. Weldon, we'll go with you.

Mr. RAUB. From my vantage point, sir, I think it's most unlikely you'll see two side-by-side pages. I don't think it needs to be the CD ROM or the encyclopedia either, but I think realistically, given the array of different types of threats that we can identify or imagine and the myriad ways they have to be addressed, I think this will be of necessity a fairly complex document.

Mr. SHAYS. Do you want to make a response?

Mr. VERGA. I would just say I would imagine that you'll see something that will be akin to the President's national security strategy that's published every year, a book of about 50, 60 pages that will lay out in various shapes and forms that approach.

Mr. SHAYS. And constantly being revised and so on?

Mr. VERGA. Yes, sir.

Mr. SHAYS. But there will be some basic tenets in it like we go after terrorists wherever we find them, that it's preemptive rather than reactive? Those things will probably last in all of them?

Mr. VERGA. I think—I think that's fair.

Mr. SHAYS. And just the point that we are learning that we have to somehow learn intent in order to know the likely areas of vulnerabilities that we want to focus on, will intent matter a big deal?

Mr. VERGA. We in the Defense Department, of course, in prosecuting the global war on terrorism are—are approaching it from the—removing the capability of others to have safe havens upon which they can then plan and train and attack the United States from, and I think that will continue to be our approach. It is very

difficult and, of course, we have no internal security function in the United States. That's left to the law enforcement community. But it's very difficult to determine intent on the part of terrorists. At least that's been my observation.

Mr. SHAYS. Yes.

Mr. CARUSO. Mr. Chairman, I would just add that the human—human intelligence, whether it comes from the lips of an individual or document he or she has written, is—is the—is our best avenue for understanding what's in the hearts and minds of men who want to destroy us, and that is a premium on—that's something that we need to as a government have as important key to our strategy.

Mr. SHAYS. I just would say—did you want to say, Mr. Greene, anything?

Mr. GREENE. No.

Mr. SHAYS. Before giving it to Mr. Weldon—Dr. Weldon, excuse me, there is a conviction on the part of some of us that when we look at September 11th we will say if we listen to what they said in Arabic and not English we would have known about September 11th, which is basically saying that if we had even used our information systems and just monitored newspapers and public discussions in other communities we might have known, besides the human intelligence. I'm led to believe that will be found to be true, but we'll see.

Dr. Weldon, you have at least 5 minutes.

Mr. WELDON. Thank you. Thank you, Mr. Chairman, and I did want to commend you for calling this hearing and I apologize for missing the verbal testimony from the witnesses in getting here a little late, and I do want to say to you, Mr. McHale, that I would like to followup with you on the random search issues particularly at the gate. I think that's the area of concern of a lot of my constituents.

But, Mr. Greene, I did read your written testimony and there were a number of questions I had about it. I was very glad to hear that the INS is implementing an improved information and data sharing system. Right after September 11th we were provided some very disturbing information about the inability of INS to communicate with various agencies that have very valuable information that can help INS agents. You said at the bottom of page 2 in your statement, "We have been working with the State Department to expand data-sharing to ensure that immigration inspectors have access to issued visa information and the consolidated consular data base. As a result, this information is now available at all POE's."

Have there been any results from any of this? Can you point to any cases where we've been able to prevent a terrorist entering the United States based on the information——

Mr. GREENE. I don't think we——

Mr. WELDON [continuing]. Sharing that's available?

Mr. GREENE. I'm sorry. I don't think we have information with respect to terrorist prevention. It has been very useful, though, in a number of other cases with respect to fraud. What this data base provides us is a copy of the—basically the nonimmigrant visa application that's filled out by the applicant overseas and also a photograph. So it's—the photograph that was presented with that appli-

cation at the time. So it has dramatically cut down on the photo substitution vulnerability that we used to face with a valid visa in a valid passport with a photo substitution allowing people into the United States. I don't have those numbers off the top of my head. There has been an increase in fraud detections since September 11th——

Mr. WELDON. The photo substitution issue was one of the major reasons why the language in the bill calling for the development of a biometric evaluator was replaced——

Mr. GREENE. That's right.

Mr. WELDON. So are you saying the need for that biometric evaluator is diminished——

Mr. GREENE. No. We——

Mr. WELDON [continuing]. Or do we still need——

Mr. GREENE. Yes. We want to be able to have a biometric identifier on all of the nonimmigrants who travel to the United States because that's going to be key to the eventual success of our entry/exit system.

Mr. WELDON. I think you go on in page 5 and you talk about the passenger analytical units, PAUs, at airports, seaports, determining whether a noncitizen seeking admission to the United States is admissible. Particularly dealing with airports, shouldn't a lot of this screening actually be done at the consular level before it actually gets to the INS?

Mr. GREENE. Well, I think that's part of our strategy and that has become more and more prominent in—in our strategy working with the Department of State since September 11th. We used to talk about the immigration inspector as being the first line of defense, but in actuality we appreciate that it's the consular officer overseas who is the first line of defense, and that's why we have also provided information to the Department of State to assist them in—in doing the evaluation necessary to—to make the right decision on whether to grant a nonimmigrant visa or not.

Mr. WELDON. On page 10 you mentioned the INS and other task force agencies. If anybody wants to contribute to this response, feel free to do so. Coordinate their efforts to develop lead information on counterterrorism-related subjects and to neutralize the threat of alien terrorists. How many leads have been generated by all this? What type of actions have been the result? You've gotten a lot of bad press lately and you've got an opportunity for some good press here if you've kept some people out.

Mr. GREENE. The—well, we actually do have some information that I could brief you on separately with respect to——

Mr. WELDON. Classified——

Mr. GREENE. Yes, sir.

Mr. WELDON. Yes. I would be very interested in hearing that.

Mr. GREENE. Above and beyond that, the Foreign Terrorism Tracking Task Force is the—the group that has done the manipulations of INS and other data bases in order to identify potential witnesses who would come forward during the last interview process, the—the list of approximately 6,000 people that were jointly interviewed by Federal agencies and State and local officials inviting them to come forward with information that might be useful in our

counterterrorism effort. The President announced a similar initiative yesterday following on that—that same line.

In terms of specific leads, I'd be happy to give you a—a more thorough conversation about that in a different setting.

Mr. WELDON. Mr. Chairman, I yield back. Thank you very much.

Mr. SHAYS. Thank you. I don't have many more questions and so we'll probably get you out of here by 4 o'clock.

Mr. Greene, it's been reported that the administration is considering a merger of INS and Customs within the Department of Justice. What are the statuses of that consideration?

Mr. GREENE. I'm not in a position to—to comment on that at all, Mr. Chairman. The commissioner has—has put forward a reorganization plan for the INS that was reviewed and approved by the President. That was the proposal that was brought up to the Hill in December. What we—what we are able to say about any subsequent considerations——

Mr. SHAYS. Fair enough.

Mr. GREENE. It's just——

Mr. SHAYS. OK. One of the issues on the Patriot Act was that information the FBI—our committee had dialog in another hearing before September 11th in which we learned that some information that the FBI had was not—it was being shared with INS but not with the State Department, and the Patriot Act requires information to be shared with the State Department. Can you give me any insights on how that's working out, Mr. Caruso?

Mr. CARUSO. Mr. Chairman, we are—the State Department has a system, a visa system, known as Class, also known as Tip-off, where U.S. intelligence—the U.S. intelligence community and the FBI contribute names to that system so that consular officers, when they are confronted with an individual who's applying for a visa, can check that system and determine whether there's an interest in a particular person by the U.S. intelligence community or the FBI. We've contributed to that in the past and we've stepped up our contribution of names to that system. We are doing that—we want greater electronic connectivity direct with that system so that we can avail ourselves with modern technology to get the information in versus disk and bringing it over periodically.

With reference to requirements beyond that, I would like to provide you with some additional information outside the hearing here only because I don't have the kind of satisfactory answer that your question deserves.

Mr. SHAYS. Fair enough. That would be something I would like you to convey with the committee staff, if you would. Just to say parenthetically, I don't have a lot of faith in our—I have a lot of faith in the people who work in our government, all of you and your dedication. Most of you I believe are civil servants as opposed to appointments of the President, though both are appreciated and—but I don't have much of a comfort level with our information technology in government. We put out the bids, it takes so long, the system seems to be outdated before it's implemented.

When we chaired the Human Resource Committee, we were never happy with what we saw happening with Social Security, with Medicare, with a whole host of systems that were put in place, obviously not pleased with what INS has, and I will—the State De-

partment isn't here, but the State Department was using Wang computers 4 years ago and they can't even communicate internally in some cases within their own embassies, much less communicate with other embassies. They can communicate with Washington, but you can't have Ambassadors from neighboring countries communicate.

So we know that there is a lot of work in this area and Mr. Horn in particular in our Government Reform Committee has been working on it.

Can any of you say anything that can make me feel comfortable about any progress using information systems, anything that I can—that this committee can say, well, this is a good sign? I don't mean a hopeful sign, I mean a good sign. Anything beyond hope? Yes, Doctor.

Mr. RAUB. It may be one of those times when it's—when it's dangerous to volunteer, Mr. Chairman, but I'll try. One of the major emphases in our billion-dollar-plus investments that I mentioned earlier in State and local preparedness is on information and communication technology for public health, and a major element of that is striving for interoperability of those systems. The worst thing that could happen would be for us to invest in myriad ways in State and local health departments and our hospitals only to find that information about infectious disease could not be shared efficiently and effectively among them. So the guidance that we set out has as one of its cornerstones a set of communication standards developed at the Centers for Disease Control and Prevention that is to guide the implementation of those activities. We are going to work very hard at achieving that. I don't present it as a completed act. I present it as one of our highest priorities to achieve.

Mr. SHAYS. And will you be able to break the red tape and the procurement challenge—my view is almost when I voted for some of—for this immense amount of new dollars that in the process I would waste some money, but do a lot of good in the process, but we don't have time to not—we have to just move forward quickly. Are you going to be able to move forward quickly?

Dr. RAUB. We believe we will, sir, and that the principal acquisitions for this are going to be done by the State and municipal entities. It's not important that we prescribe which particular brand of hardware one gets or which particular modem, but rather that certain functional characteristics are met, and in general those functional characteristics have been designed with knowledge of the market in mind. So there should be for almost any entity an array of choices so long as the connectivity and the so-called interoperability is achieved, and—and that's our goal.

Mr. SHAYS. Just dealing with your area, I had been led to believe before September 11th, based on previous committee work, that we monitored every day potential outbreaks in urban areas and that we checked with every hospital every day more than once, and we learned after September 11th that we weren't. Will there be a day and, if so, when will that day occur, when—just like my Department of Transportation that can tell you an accident any place on I–95, any place where it's cueing up, will there be a day that you will be able to look on a board and tell us there's so many outbreaks of this disease in Cleveland, so many outbreaks of this dis-

ease in San Francisco, so many issues of concern in another area? Will that day happen where it will be centralized, up to date, kind of like what a major company will do in being able to tell you how many products they sold every day and what they were and what towns they sold them?

Dr. RAUB. I'd be overstating my knowledge and misleading you if I said I thought I could tell you exactly when that might happen.

Mr. SHAYS. Is that a goal?

Dr. RAUB. Yes. That's one of the major goals of this investment in the infectious disease surveillance. In many parts of this country still, the surveillance of an infectious disease depends upon an alert and conscientious and energetic physician noticing something and reporting it to the local Health Department. In many parts of the country that's still done with a postcard, and perhaps a telephone call, perhaps a fax message. We're a long way away from having any kind of routine transaction recording that would get that information to the local Health Department and enable it in turn to look across the whole community and be able to see unusual patterns.

One of the interim steps that have been taken in association with certain of the special events such as the Olympics or the two national conventions in the last several years, our Centers for Disease Control and Prevention, in collaboration with the Department of Defense, implemented what they've referred to as drop-in surveillance, that is, ad hoc capability where the local hospitals, using an Internet and Web-based connection, were on a daily basis reporting certain information about syndromes that they were seeing, certain characteristics of patients, that information not—being recorded and not only returned to that particular hospital but looked at regionally for patterns for possible outbreaks of activity. That's a forerunner of the kind of thing we would like to see routine, and I know that's a high priority for the Office of Homeland Security to see us achieve that kind of electronic surveillance. We're not there. We're not close. It's certainly doable within the technology. It will require the will and the investment to follow through and make it happen.

Mr. SHAYS. I'll just say that of all the concerns expressed before this committee, the greatest one was the biological. It wasn't chemical, wasn't nuclear, wasn't conventional. It was biological. And it would strike me that the long way off has got to be a concern to us because I don't believe that we have the capability to deal with an outbreak that we didn't see early enough. Counsel has—OK. Basically I'm going to just be true to my word at 4 o'clock and just ask is there anything you wish we had asked that you had prepared to answer and that you would feel good knowing that you were prepared to be—is there anything you would like to respond to before we close the hearing, any question you would like to ask yourself and answer? Mr. Greene. Mr. Caruso. Mr. Burris. Mr. Raub.

Dr. RAUB. No, sir.

Mr. SHAYS. Mr. McHale. Mr. Verga.

Mr. VERGA. I would—would only say that when you talk about homeland security for the Department of Defense, the biggest and best contribution, of course, that we are making is in fact the glob-

al war on terrorism and we look at—we look at everything that we do in the Department of Defense as homeland security because that's the mission of our Department.

Mr. SHAYS. I think that's pretty clear. I appreciate your making that point. I appreciate all of your contribution today, particularly your patience in having a large panel, but I think it certainly helped us out a lot and I appreciate that. And if there's no further comment, we will call this hearing adjourned.

[Whereupon, at 4 p.m., the subcommittee was adjourned.]

○