AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–148

BORDER TECHNOLOGY: KEEPING TERRORISTS OUT OF THE UNITED STATES

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

AND

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY AND CITIZENSHIP

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MARCH 12, 2003

Serial No. J–108–5

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
89–330 DTP 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 THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa	PATRICK J. LEAHY, Vermont
ARLEN SPECTER, Pennsylvania	EDWARD M. KENNEDY, Massachusetts
JON KYL, Arizona	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin
JEFF SESSIONS, Alabama	DIANNE FEINSTEIN, California
LINDSEY O. GRAHAM, South Carolina	RUSSELL D. FEINGOLD, Wisconsin
LARRY E. CRAIG, Idaho	CHARLES E. SCHUMER, New York
SAXBY CHAMBLISS, Georgia	RICHARD J. DURBIN, Illinois
JOHN CORNYN, Texas	JOHN EDWARDS, North Carolina

MAKAN DELRAHIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah	DIANNE FEINSTEIN, California
ARLEN SPECTER, Pennsylvania	EDWARD M. KENNEDY, Massachusetts
MIKE DEWINE, Ohio	JOSEPH R. BIDEN, JR., Delaware
JEFF SESSIONS, Alabama	HERBERT KOHL, Wisconsin
SAXBY CHAMBLISS, Georgia	JOHN EDWARDS, North Carolina

STEPHEN HIGGINS, *Majority Chief Counsel*
DAVID HANTMAN, *Democratic Chief Counsel*

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY AND CITIZENSHIP

SAXBY CHAMBLISS, Georgia, *Chairman*

CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
JON KYL, Arizona	PATRICK J. LEAHY, Vermont
MIKE DEWINE, Ohio	DIANNE FEINSTEIN, California
JEFF SESSIONS, Alabama	CHARLES E. SCHUMER, New York
LARRY E. CRAIG, Idaho	RICHARD J. DURBIN, Illinois
JOHN CORNYN, Texas	JOHN EDWARDS, North Carolina

CAMILA MCLEAN, *Majority Chief Counsel*
JAMES FLUG, *Democratic Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Chambliss, Hon. Saxby, a U.S. Senator from the State of Georgia	4
Cornyn, Hon. John, a U.S. Senator from the State of Texas	12
Craig, Hon. Larry E., a U.S. Senator from the State of Idaho	11
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	6
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah, prepared statement	49
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts	8
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	1
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	9
prepared statement	79

WITNESSES

Flynn, Stephen, Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations, New York, New York	33
Hutchinson, Hon. Asa, Under Secretary for Border and Transportation Safety, Department of Homeland Security; accompanied by Robert Mocny, Director, Entry-Exit Program, Bureau of Immigration and Customs Enforcement, Department of Homeland Security, and Woody Hall, Assistant Commissioner, Office of Information and Technology, Bureau of Customs and Border Protection, Washington, D.C.	13
Kingsbury, Nancy, Managing Director, Applied Research and Methods, General Accounting Office, accompanied by Richard Stana, Director, Homeland Security and Justice, General Accounting Office, Washington, D.C.	31

SUBMISSIONS FOR THE RECORD

Flynn, Stephen, Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations, New York, New York, prepared statement	42
Hutchinson, Hon. Asa, Under Secretary for Border and Transportation Safety, Department of Homeland Security, Washington, D.C., prepared statement	51
Kingsbury, Nancy, Managing Director, Applied Research and Methods, General Accounting Office, Washington, D.C., prepared statement	62

BORDER TECHNOLOGY: KEEPING TERRORISTS OUT OF THE UNITED STATES

WEDNESDAY, MARCH 12, 2003

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY
AND HOMELAND SECURITY, AND
SUBCOMMITTEE ON BORDER SECURITY,
IMMIGRATION AND CITIZENSHIP,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Subcommittees met, pursuant to notice, at 10:04 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl, Chairman of the Subcommittee on Terrorism, Technology, and Homeland Security, presiding.

Present: Senators Kyl, Chambliss, Craig, Cornyn, Feinstein, Kennedy, and Leahy.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Chairman KYL. This hearing will come to order. It is a joint hearing of the Judiciary Subcommittees on Terrorism, Technology, and Homeland Security, and Border Security, Immigration, and Citizenship. Like the new Homeland Security Department, we have some new names and have moved some things around here on the Judiciary Committee. I think it is propitious that as we begin work with the new Homeland Security Department, these two Subcommittees begin work together on issues of importance to us all.

We are going to welcome for his first hearing Asa Hutchinson, who is the Department of Homeland Security's Under Secretary for Border and Transportation Security. I would note that while he was sworn in on January 24, I believe, he and his staff joined together March 1. So with about 10 days under his belt with this new department, we are going to grill him about why things haven't gotten done yet.

I am being facetious, of course. The primary point of this hearing is to share an understanding with Secretary Hutchinson about what needs to be done and to try to get at least his first impressions as to what the department will need from the Congress in order to fulfill the legislative mandates that we have imposed with some of the recent legislation that we have passed.

In addition, our second panel will include the General Accounting Office's Nancy Kingsbury, and Stephen Flynn, who has testified before the Terrorism Subcommittee before. Accompanying Nancy Kingsbury is Rich Stana, and I will let Secretary Hutchinson prop-

erly introduce the two people that have joined him, but it is Robert Mocny and Woody Hall, both of whom have expertise in areas that we will be inquiring into.

This hearing is also propitious because Secretary Hutchinson is going to be joining Senator McCain and me this weekend on the Arizona border with Mexico, studying not only the issues that need addressing at our points of entry, but also how to apply technology to the large stretches of land between the points of entry. I think we will be getting a good firsthand look at the vastness of the land, the fact that people can't possibly patrol the entire area, and therefore we are going to have to continue to enhance the application of technology not just at the ports of entry, but also in those areas in between.

The hearing is going to obviously focus on technology, and while my particular Subcommittee deals also with terrorism, it is not limited to the object of keeping terrorists out of the country, though given the nature of that threat there will be a lot of focus on that particular issue.

There are really three primary parts of the hearing, I think. The first is to identify how far along the administration and the Congress have come to implement the technology systems that we have mandated specifically in the Border Security and Visa Entry Reform Act of 2002; second, to examine the current Customs infrastructure and technology policies, and identify future infrastructure and technology needs at our land ports of entry; and, third, to examine the technology and border needs in between the ports of entry, as I spoke of before.

Broadly speaking, there are three ways that terrorists exploit our Nation's visa processing and immigration inspection system. First, they come here legally with at least facially valid visas that they have obtained by the State Department, and most of the hijackers of September 11 entered the country in that fashion. The application of better technology can perhaps prevent the entry by terrorists into the country by that mechanism in the future.

Second, it is clear that many illegal immigrants and smugglers and potential terrorists use fraudulent documents to get into the United States undetected, and again an integrated interoperable intelligence system will be better able to identify individuals who should not be coming into the country in that fashion.

Third, of course, there is the vast number of people who are smuggled across the border or who smuggle themselves across the border through alien smuggling networks and bring contraband, including drugs and potentially other more dangerous things, into the country.

The Enhanced Border Security and Visa Reform Act that I mentioned before creates a whole series of technology-related requirements. The automated Entry-Exit System is one of them, which requires the electronic exchange of entry and exit information on all travel document-holders. Now, we want to have this in place, if we can, by the end of 2005, but we will hear about whether there may need to be some changes made to that.

The biometric entry documents. The Act requires that all travel documents, including passports issued after October 26, 2004, include a biometric feature.

Three: the readers at ports of entry for these biometric travel documents. It is not clear when we will be able to get this accomplished, but the Act requires that the Attorney General, in consultation with the Secretary of State, use biometric data readers and scanners at all points of entry after October 26, 2004.

Fourth is the Chimera Interoperable Data System. The Act requires INS to fully integrate all of its data bases, and requires the President to develop and implement an interoperable electronic data system that contains Federal law enforcement and intelligence information relevant to making decisions on visa admissibility and removal of aliens. The President is required to establish a commission on this and requires it to report to the Congress annually on its findings and recommendations.

Of special interest to me, from the State of Arizona, fifth is the Mexican Laser Visa and Reader Program. One of the provisions of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 required that the Mexican border-crossing card contain a biometric tamper-proof identifier.

This is the card issued to people who frequently travel back and forth, who come into the United States for up to 72 hours or up to 50 miles. There is just a tremendous amount of that cross-border traffic with my State, and I am sure with the other border States as well.

We extended the deadline for obtaining these cards, and literally millions of Mexicans have gone to the trouble and expense of obtaining the cards. But we have found that, notwithstanding the appropriation of over $10 million for the purchase and deployment of readers, we still have readers at only six ports of entry. And we will want to find out a little bit more about what is necessary to actually complete this process.

I would conclude by noting that, along with these technological requirements in statute, it is also clear that we are going to need additional infrastructure. Legislation has been introduced to this effect, but Senator Feinstein has certainly focused on the Container Initiative at our ports, for example. Our truck-size x-ray systems, the personnel radiation detectors—all of these things are useful. We will want to hear more about them, but obviously also more needs to be done.

The 2000 report of the Customs Service indicated the need for $925 million in facility and equipment improvements at that time, and that was prior to September 11. So clearly we have additional needs here and this hearing will afford us an opportunity, as I said in the beginning, to identify what all of us think some of those requirements are and focus on ways that we can work with the Department of Homeland Security and the person primarily responsible, Secretary Hutchinson, in that regard.

Let me turn next to the new Chairman of the Immigration Subcommittee that I identified before, Senator Chambliss. Following that, I will turn to Senator Feinstein, who is the ranking member on the Technology and Terrorism Subcommittee, and then Senator Kennedy, the ranking member on the Immigration Subcommittee. And because he is the ranking member on the full Committee, we obviously want to give Senator Leahy an opportunity to make any comments that he would want to make as well.

I hope that this process isn't too cumbersome. When we have the witnesses testify—Secretary Hutchinson, since this is your first time, I am not going to use the usual red light system that we have, but we will ask Members to constrain themselves to 7-minute rounds for questioning and hope that we can get through two panels in that fashion.

Senator Chambliss, welcome.

STATEMENT OF HON. SAXBY CHAMBLISS, A U.S. SENATOR FROM THE STATE OF GEORGIA

Senator CHAMBLISS. Thank you, Senator, and I apologize for running late. And I literally am running late. I got held up, I ran all the way over here and I am out of breath. So if I have to stop in the middle of this, I apologize.

Thank you for holding this hearing and asking my Subcommittee to participate, and I appreciate very much Senator Feinstein, Senator Leahy, Senator Leahy, as well as Senator Craig being here.

This hearing addresses some very important issues facing our Nation. I am glad that we have an opportunity to have a discussion with some of the key players at the Department of Homeland Security who will now be in charge of securing our borders.

I am particularly pleased that Secretary Hutchinson is here, an old colleague of mine, a gentleman that I know very well and have utmost respect for. I traveled around the world with him and know him to be not just a great guy, but a great leader. We are sure pleased to have you where you are.

I am pleased that we are able to have a discussion in the form of a joint Subcommittee hearing because I think it is critical that both the Terrorism, Technology, and Homeland Security Subcommittee and the Border Security, Immigration, and Citizenship Subcommittee be involved in solving these issues because we do need the cooperation of both Subcommittees to find a solution to the problem that we are now facing at our borders.

I do not think that anyone here would argue that the events of September 11 brought to light a glaring hole in the security of our Nation, and that is our immigration system. It is overwhelmed and undermanned.

I would say to Secretary Hutchinson that you have a tremendous responsibility on you, and I am glad it is you there and not me.

It seems that things slipped through the cracks, and as a result three terrorists who hijacked the planes that flew into the World Trade Center and the Pentagon were in this country with expired visas. The problems with our immigration system cannot be fixed overnight and I do not think anyone realistically expected them to be. But we can take steps, and we have taken steps to address the myriad of issues that we are currently facing with our immigration system.

The USA PATRIOT Act, which we passed in the 107th Congress, resolved some of the ambiguities in the Immigration and Nationality Act regarding the admission and deportation of terrorists. It also provided the Attorney General with the power to detain suspected terrorists before they had an opportunity to do more harm.

We built upon that legislation with the passage of the Enhanced Border Security and Visa Reform Act. This legislation closed sev-

eral loopholes in immigration law by providing additional staff and training for our borders and by facilitating comprehensive data-sharing between law enforcement officials, intelligence agencies, the State Department and the INS.

It also mandated the use of biometric technology to enhance our ability to confirm the identities of those seeking admission to the U.S., restricted the admittance of nationals from countries that sponsor terrorism by requiring the State Department to first conclude that the individual does not pose a national security threat, and improved upon our foreign student monitoring program.

I am very pleased with the legislation that the Congress passed and the President signed into law. And I realize that we attach short deadlines with many of the mandates that we incorporated into that legislation, but we were eager for action.

Now is the time to check the progress of implementing this legislation and see what more needs to be done to determine the areas in which performance needs to be more effective and to assess how realistic the goals of our last legislative efforts were.

I know that I remain committed to working with my colleagues, our President, his administration, the Department of Justice, the Department of Homeland Security, the State Department, the Treasury Departments, and all other necessary parties to ensure that we are taking the needed steps to secure our borders.

I am concerned with a number of the aspects associated with our immigration system. For instance, I want to know what steps we are taking to track foreign national visitors in the U.S. with expired visas. I have concerns about the number of illegal immigrants coming into our country between ports of entry. I am worried about the smuggling of drugs or weapons across our borders and what we are doing to prevent it.

Today, I will focus on what the departments are currently doing and what mechanisms can be put in place to facilitate the entry of people authorized to come into this country, and to ensure at the same time that certain inadmissible people are prevented from entering.

I am interested in hearing more about the possibility of adding biometrics to visas and passports, and of creating a biometric watch list to identify travelers who are inadmissible to the United States before issuing them travel documents or before allowing them entry into the U.S.

However, I do have questions about the cost of implementing these tools, about the reliability of current biometric technology, and about the effect that pursuing one or several of these options will have on our trade and commerce and on our relations with other nations.

I am eager to begin our discussion with today's witnesses. I thank them again for being here and participating in this important exchange, and I look forward to a dialog.

Thank you, Mr. Chairman.

Chairman KYL. Thank you, Senator Chambliss.

Next is the ranking member of the Terrorism and Technology Subcommittee, formerly the Chairman of the Subcommittee. And I have said it before and I will say it again that there is probably no one on the Democratic side that I have introduced or cospon-

sored more legislation with, and probably more with Senator Feinstein than most of my Republican colleagues, because we have seen eye to eye on many of the issues that we have worked on and it has always been a real privilege for me to work with her. And for her to be the ranking member of this Committee now at this important time is also a real benefit for the people of this country.

Senator Feinstein?

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thank you very much, Mr. Chairman. I appreciate those comments. As you know, I share those sentiments, so thank you very much.

For a year-and-a-half now, Congress, the administration and the American public have searched for answers as to how a large group of coordinated terrorists could operate for more than a year in the United States without being detected, seize control of four different commercial jetliners, and then use those jetliners as weapons of mass destruction without being stopped.

The benefit of hindsight provides a clearer picture of how existing technologies might have been used to at least alert the appropriate officials that some, if not all, of the hijackers' visas should have been denied. Furthermore, these technologies might have tracked the previous history of the hijackers' immigration violations, which should have led immigration inspectors to deny entry to at least some of them.

We all know too well, under our current system, a determined terrorist with unlimited resources who is willing to risk his life as well as the lives of others can probably find a way to enter this country. Since September 11, we in Congress and the executive branch have undertaken efforts to make it harder for that to happen. But if those efforts are to be effective, Federal agencies will have to have the necessary tools to enforce the laws governing the Nation's borders.

We have seen how the September 11 terrorists exploited the Federal Government's lax oversight of our immigration laws. They also exploited what was then our immigration system's inability to transform itself from its current paper-driven and unmanageable bureaucracy into a modern technological system.

For example, had the foreign student tracking system, commonly known as SEVIS, been in operation, the INS might have known that Hani Hanjour, one of the 19 hijackers, had violated the terms of his visa. In late 2000, Hani Hanjour entered the United States on a student visa to learn English at a school in Oakland, California, but he never showed up at that school. He managed to evade detection until that fateful morning of September 11, when we learned that he was at the controls of American Airlines Flight 77 when it struck the Pentagon.

Immigration authorities might have prevented Mohammed Atta from entering the United States. He had violated the immigration laws by previously overstaying his visa long before he flew a plane into the World Trade Center. Atta arrived in Miami on January 10, 2001, claiming that he wanted to take flying lessons. But he carried only a tourist visa, not the required vocational training visa.

Either of the two infractions was sufficient to deny him entry, but like his comrades in terror, he simply slipped through the cracks.

Because of the recordkeeping problem, Miami inspectors were unaware of Atta's overstay violation. So when he convinced the inspectors of his good intentions, he said he had applied for but had not yet been approved for a student visa. Yet, despite the lack of a valid visa, he was allowed to enter the United States.

These blunders and missteps and the consequences that flowed from them represent the end result of having an unfocused, unconnected and unsophisticated technological infrastructure, as well as the systemic lack of resolve to provide the right training, the right tools, the right management and the right incentives for our front-line officers to do their job.

The challenge for our border agencies, therefore, is to establish a state-of-the-art border infrastructure that supports the dual goal of national security and legitimate border crossing.

For example, how do we build on successful pre-screening programs like the SENTRI initiative, which permits Mexican nationals to be pre-screened and pre-inspected in exchange for more rapid travel access across the border in a specially designated lane?

Is it feasible or desirable to extend programs like this to foreign nationals of other countries? I think it deserves a good look. What quality control checks would have to be in place to expand such a program without increasing the risks?

I realize that technology is not the sole answer to meeting the challenges of securing our country from entry by those who wish to do us harm, but it is an essential element. Without it, our border inspectors are essentially left with their hands tied, unable to compete with those who would use even more sophisticated means of gaining illegal entry to the country.

Another example: How do we build an efficient process so that front-line inspectors are not tasked with logging on to several lookout data bases to search for and interpret a complex intelligence report where more scrutiny is required? How can that important step be handled at the front end so that the inspector has only to see a red flag that tells him to send the traveler to secondary inspection? How do we better invest in the skills of our border personnel so that we can be sure that laws are clearly understood and strictly followed? How do we invest in training and retraining on new techniques and new technologies to enhance their risk management skills?

At today's hearing, we hope to hear a distinguished panel of witnesses assess the steps that have been taken since September 11 to harness technology to help our dedicated front-line officers keep terrorists and instruments of terrorism out of the United States.

Again, I thank the Chairman for holding this hearing and I look forward to today's testimony.

Chairman KYL. Thank you, Senator Feinstein.

When I was a new member of the Immigration Subcommittee, then-Chairman Alan Simpson took me to see Senator Kennedy. He said this is something you need to get to know because even though he may be cantankerous at times, he has been here longer———

Senator KENNEDY. I thought you had forgotten that word that Alan used.

Chairman KYL. Well, that is a Simpson word, as you know.

He said he has been here a long time and he knows more than anybody else about this immigration stuff and you really need to work with him. And I have found over the years that the latter is true, never cantankerous, but very knowledgeable and always pleasant to work with. I might way that both Senator Feinstein and Senator Kennedy have extraordinary staffs who are also very easy to work with and that makes our job a lot easier, too.

Senator Kennedy?

STATEMENT OF HON. EDWARD M. KENNEDY, A U.S. SENATOR FROM THE STATE OF MASSACHUSETTS

Senator KENNEDY. Thank you very much, Senator Kyl. We have worked together, particularly on that important border security legislation last year, in a strong bipartisan effort strongly supported by Senator Leahy. I want to welcome Secretary Hutchinson here.

As we have heard, much can be done with technology. A great deal can be done with technology and we have to make sure that we have the best technology. That is true about our service men and women, to have the best technology and be well-led, and it is true in terms of homeland security. We know that a great deal more has to be done in this area not only in getting the best technology, but also having it interoperable. That is absolutely essential.

We have seen, as we did at the time of 9/11, that we had the CIA actually fail to provide the INS with the information on the watch list which would have given them a heads-up. The fact that the CIA did not provide it permitted the INS to let two of the hijackers to gain entry into the United States. So you can have the best of technology, but if you don't have the policies in terms of sharing information and using it effectively, it is not going to be effective.

Second, if you don't have the best trained people who are going to stay there and be highly motivated, highly committed, and with good morale—and this is constantly a challenge particularly in the INS. We have got a lot of very dedicated, committed people. It is an enormous challenge that they are facing, with 500 million people coming in and out of this country over a period of a year. How are we going to follow them, keep track of them, and do it in a way which is sensitive to their rights of privacy, gaining the right information but not unnecessary information, making sure that the information that is gathered is not going to be released in such a way as to compromise people's privacy or identity kinds of crises in terms of duplication and replication of this? So this is an enormous challenge.

In many instances, the newest technology isn't always the answer. We want to try and do this, but we are mindful that sometimes technology slows the process down with all of its implications. So it is a tough job for you to be able to finally select and make that judgment, and we want to try and work with you.

Finally, there were reports that were required from the agency in our legislation which we all sponsored and was supported and signed by the President about the relationship between the CIA and the INS and sharing information. That was due in October of last year. That was before you even sort of thought about these

matters. We should have that when you have an opportunity to get that to us at the earliest possible time.

The NSEERS program also requires that you provide information to us by early March and we haven't gotten that information from you. I don't want to be overly bureaucratic, but those are very important policy issues about shared information, which is the key to the success of this program.

Also, the NSEERS program—I know you have got some reference in your testimony about this, but we are trying to work with local communities, helping to get their cooperation in helping to identify potential terrorists within various communities, because we know there are cells of Al-Qaeda in the United States, and on the other hand with the process of fingerprinting and other kinds of activities and the extent to which that is counterproductive. These are judgmental values and I think we want to monitor these closely and find out your reasons for doing it, what is working and what isn't working.

We thank you very much and congratulate you on your job.

Thank you, Mr. Chairman.

Chairman KYL. Thank you, Senator Kennedy.

Now, we have the distinguished ranking member of the full Committee with us as well and I would like to Senator Leahy to make any comments that he would like to make.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman, and I thank you for your courtesy which is consistent with what you always do, and I appreciate that very much.

It is nice to see our friend, Asa Hutchinson, here. I recall on your last appointment I think we set a world speed record getting you through this Committee. In fact, it surprised somebody at the White House who, when I was talking to them, said, well, are you going to be able to get him up there soon? I said we did it this morning, and they said but we thought it was going to be 2 weeks from now.

Senator Kyl, I think you and Senator Chambliss and Senators Feinstein and Kennedy are doing great service in having this hearing. I am glad you are doing it as a joint hearing because you have got to improve the technology to keep terrorists from coming across our borders. No matter how much personnel we have, technology is going to play a vital, vital role. But then we also have to make sure the technology is such that it keeps an orderly flow across our borders.

I think of it, of course, from a somewhat parochial view, living less than an hour's drive from my home to the Canadian border. I am also aware of the fact that Canada is our largest trading partner and we need an orderly flow across that border. Besides, it also helps when my wife wants to go and visit her relatives.

But in seriousness, it is difficult to strike a balance, and yet we have to. It is going to be very, very difficult. I think this is going to be one of the things that is going to bedevil you during your tenure, and probably appropriately so because what you do may well set the standards for years to come.

In the USA PATRIOT Act, Congress and the President supported my proposal not only to triple the number of INS inspectors and Border Patrol agents and Customs officers at our borders, but also to provide $100 million to improve the technology we use to monitor the northern border. Actually, it requires more monitoring and equipment.

Last year, Congress passed the Enhanced Border Security and Visa Reform Act that added additional steps to improve our security. Now, Mr. Chairman, I think what we are doing is using our oversight to make sure that that is implemented.

Just this past week—and I brought this up when Secretary Ridge and Attorney General Ashcroft and Director Mueller were here—the day before they testified, a helicopter had come through and, by accident, some snowmobilers saw them dumping a huge amount of drugs in Vermont. Yet, it could have been a terrorist, it could have been any type of thing, and it was totally undetected either on the Canadian side or the U.S. side.

When you discuss border security, you have to consider both the administrative challenges the new Department of Homeland Security faces and the budgetary constraints the administration has imposed upon it. We have to have the effective integration of dedicated officers who worked for 22 different Federal agencies at this time last month—22 different ones. They have a lot of questions about what they are going to be doing now.

It is a national concern and a local concern. It is a national issue because performance suffers if they don't know what their future is going to be. It is a local issue. I know many dedicated people in Vermont who are now Department of Homeland Security employees. There are more than 1,600 INS employees in Vermont who are now working for DHS. They protect our borders, they assist in the enforcement of our immigration laws in the interior, and they foster legal immigration and commerce by processing applications for immigration benefits.

They are well-trained, highly educated, and extremely professional. We want to make sure they are still there working for all of us and helping you and everybody else. So I would hope the DHS would provide as much guidance as you can to these new employees.

I am supposed to be at an Appropriations Committee meeting with CIA Director Tenet right now, but I want to raise an issue that we will discuss in Appropriations. House Appropriations Committee Chairman Young, with whom we have all served, called it a pointless and harmful debate with the President's own party on the question of underfunding of homeland security.

When the bill passed, the last bill, it was gone over line by line by the administration. Now, they say they want more funding for homeland security. If they had even asked for it during that time, they would have gotten it. They would have had support from everybody in the committee. I think we have to make sure that we back up the money to what we promise. We can't just say the check is in the mail.

Many, many months after the September 11 attacks, the White House declined to respond to repeated bipartisan requests from Congress to begin funding the northern border security section of

the USA PATRIOT Act, ones that I negotiated with the White House and which they said they strongly supported, until it came to asking for the money. The new budget the President is proposing does not come close to meeting our security needs. It provides less than a 3-percent increase.

These are questions where, Mr. Secretary, you are going to get strong bipartisan support both in the authorizing committees and in the appropriating committees for the money, and I think now is the time to ask for it.

So, Messrs. Chairmen and Senators Feinstein and Kennedy, I think you do us all a great service, the four of you, in holding these hearings. Thank you.

Chairman KYL. Thank you, Senator Leahy.

I am afraid our two other members would feel left out if I didn't give them an opportunity to make a brief comment.

Senator Craig?

STATEMENT OF HON. LARRY CRAIG, A U.S. SENATOR FROM THE STATE OF IDAHO

Senator CRAIG. Well, I will be brief. I am one of the freshmen on this Committee, so my colleagues to my left in most instances have a great deal more experience and knowledge in this area than I.

I come to the Committee with a micro view instead of a macro view as it relates to immigration and what happens when you tighten up and gain border security, and I strongly support it. As a border State where not much entry occurs but could occur, the security of those borders is critical.

At the same time, when you secure a border and you limit access and you don't have public policy that allows the kind of access necessary to address an economy, you create an even greater crisis. I believe the impending crisis in agriculture today, because we are doing the right things at the border, could well damage the food and fiber processes of our country.

We process about 40,000 H2-A workers through each year, and yet there are a million illegals in this country in that economy necessary to make that economy function. That is a reality. But as we tighten the border and we deny that kind of illegal access, as we should, we create a crisis.

We have got another policy issue to address here that is very important. If you are on the border in Texas, it takes on a different dynamic. If you are on the border in Arizona—and I have visited closely with my colleague, Jon Kyl—it takes on another dynamic. If you are in Idaho and your crops are rotting in the field, it takes on another dynamic.

The other side of this great concern of ours is that we also dehumanize the process, and I mean it in this simple way. It is now costing a great deal more at the hands of a coyote to move across the border, and the risk as you tighten the border down of these innocent people simple trying to find a job could well cost them their lives.

We have got to address this issue because as we tighten our borders, we put a lot of people at risk both domestically and in the economies of food and fiber in this country and the service indus-

try. And those who come to seek out that economy, we put them at risk. It is a phenomenal catch–22, but we are doing it and we are doing it for all the right reasons, in some instances with the wrong impacts.

I am very anxious to hear from all of you this morning.

Thank you, Mr. Chairman.

Chairman KYL. Thank you, Senator Craig.

Now, the Senator with the longest border with another country, Senator Cornyn from Texas.

STATEMENT OF HON. JOHN CORNYN, A U.S. SENATOR FROM THE STATE OF TEXAS

Senator CORNYN. Thank you, Senator Kyl. I want to say how much I appreciate the witnesses coming to address this very important issue to the United States, and particularly to my State which does have a 1,200-mile border with Mexico. These immigration issues that I know subcommittee Chairman Chambliss is going to be addressing and the issues that Senator Craig just talked about are of vital concern to me as well.

I will cut my remarks short so that the witnesses can talk, but let me just say that I am mystified when I hear members of the U.S. Congress talk about budgetary constraints imposed by the executive branch, since the way I read the Constitution and the way I understand the process to work it is the legislature, it is the Congress that appropriates money, not the executive branch.

In fact, I know the President has expressed his concern that some of the money that he asked to be appropriated for first responders, in particular, was not appropriated during the omnibus appropriation bill that was passed after I got here, after January 7, for the year 2003, since we did not pass a budget when ordinarily we would have.

So we all have an important responsibility, each branch of the Government, but I think Congress ought to own up to its responsibility and not try to foist that or point fingers at the administration when, in fact, we are the ones that appropriate the money and not the executive branch.

With that, I will yield my time.

Chairman KYL. Thank you, Senator Cornyn.

Now, the moment we have been waiting for, the second part of the two-way dialog here, to hear from our new Under Secretary, Asa Hutchinson.

Welcome again, and we really appreciate your willingness to come here after all of 10 days or so with your department. Thank you.

STATEMENT OF HON. ASA HUTCHINSON, UNDER SECRETARY FOR BORDER AND TRANSPORTATION SECURITY, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.; ACCOMPANIED BY ROBERT MOCNY, DIRECTOR, ENTRY-EXIT PROGRAM, BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY, AND WOODY HALL, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION AND TECHNOLOGY, BUREAU OF CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. HUTCHINSON. Thank you, Senator Kyl, and thank you for the welcome. Ranking member Feinstein, thank you, and members of the Committee. I want to first tell you that I am very encouraged by each of your comments this morning. The expertise that resides in this Committee is very helpful to the Department of Homeland Security and I think that we can build a good team together to take on these tasks. Your background, experience and knowledge is certainly encouraging to me, as well as the right questions that are being asked.

As the Chairman indicated, this is my first appearance before any congressional committee as the first Under Secretary for Border and Transportation Security, and I am honored to be able to be here with you.

I am pleased to be joined by two experts in some of the subject matter areas of your interest. Robert Mocny, to my left, is the Director of the Entry-Exit Program at the Bureau of Immigration and Customs Enforcement. And then to my right is Woody Hall, who is the Interim Director of the Office of Information and Technology in the Bureau of Customs and Border Protection. I am very pleased that they have joined me today.

Before March 1, the INS and Customs Service were working to develop and deploy technologies to enhance the screening of people and goods at our Nation's points of entry and between. These efforts continue today as they become a part of the Department of Homeland Security under the two bureaus that have been created—Customs and Border Protection, and Immigration and Customs Enforcement.

Many lessons were learned on September 11, 2001. Some of those have been pointed out by the members of this Committee. Congress has responded by providing aggressive leadership, and the men and women of the agencies that now comprise the Department of Homeland Security have responded with long hours, dedicated service, and a commitment to get critical information about cargo and people to the decisionmakers at our points of entry.

For example, more information is available to our inspectors at the points of entry on the thousands of people who seek visas to enter our country everyday. But as we all know, much remains to be done, and the leadership at the Department of Homeland Security understands the enormous challenges ahead.

One of the challenges is the Entry-Exit System, including the biometrics that have been required by the USA PATRIOT Act, and the Enhanced Border Security Act which the members of this Committee provided the leadership on. The goal is to collect records of arrival and departure from every alien entering and leaving the

United States. In addition, it will capture and process biometric data and improve information-sharing among the agencies. We share Congress' desire to field this system as soon as possible based on a well-defined project plan, and look forward to working with you to do so in the coming months.

As part of that overall objective, the NSEERS, or the National Security Entry-Exit Registration System, was launched by the Department of Justice. That responsibility was transferred to the Department of Homeland Security. The NSEERS allows us to continue welcoming visitors to our country, but it also allows us to intercept terrorists and criminals at ports of entry and identify aliens who deviate from their stated purpose or overstay their visas. Certainly, that is an objective that we have to have.

Nearly 90,000 enrollees have been fingerprinted, photographed and interviewed since its implementation. I sometimes point out that that is the same requirement of someone who wants to engage in public service, and anybody who has appeared in a confirmation hearing has gone through that same process. We have now required that for certain visitors who come into our country for national security purposes.

It also requires the non-immigrant aliens who came to the United States before it began to report to an interviewing office to be registered. All of these aliens must fulfill continuing registration requirements and complete a departure check when they leave the U.S.

NSEERS has provided a benefit. Eight suspected terrorists have been apprehended, 40 investigations of suspected terrorist activity have been opened, and 555 aliens with warrants or other criminal violations have been apprehended or denied admission. But others go about their legitimate business in our country with minimal inconvenience.

In another area, since 1988 over 6 million biometric border-crossing cards have been issued. Funding was provided in the fiscal year 2002 budget to deploy card-readers, and a recent pilot program identified more than 250 impostors. It also has helped us to move commerce and people through our ports of entry. We hope to employ additional readers at targeted points of entry by the end of this fiscal year.

Two other tools we are using to ensure the integrity of the immigration and visa issuance process include the SENTRI and NEXUS programs. These allow pre-screened low-risk travelers to proceed quickly through dedicated lanes at our land borders. SENTRI is deployed at three southwest border-crossings and NEXUS is deployed at six northern border-crossings, and we have a strong partnership with both the Government of Mexico and the Government of Canada to implement these initiatives.

We are also working to ensure the integrity of our borders between the ports of entry. We have increased the number of Border Patrol agents at our northern and southern borders, and are using many technologies, including aerial surveillance and other sensors where practical. We work closely with the DHS Science and Technology Directorate to continue to identify and deploy additional technologies that make sense, are cost-effective, and produce a good result.

In regard to our efforts to ensure the security of goods and materials entering the United States, Customs and Border Protection has deployed over 6,000 personal pager-sized radiation detectors to our ports of entry. I think it is important to note that on March 1, as these 22 agencies came on board Homeland Security, the day before that the Customs inspectors had the detection monitors, but the INS inspectors did not. The first day, as they came over, they were deployed to everyone who are inspectors on our borders.

We also deployed 112 large-scale, non-intrusive inspection systems at our air, sea and land border ports, and additional systems have been ordered. We are also testing and deploying other technologies, including portal monitors and isotope identifier devices that will help inspectors conduct non-intrusive inspections quickly and efficiently.

We are employing and refining risk-based targeting systems to incorporate intelligence and target unusual, suspect or high-risk inbound and outbound shipments for intensive examination. This is our Container Security Initiative, combined with others, that will help us to target the cargo of risk coming to the United States.

Customs and Border Protection has successfully required airlines to submit passenger manifests to our advanced passenger information systems prior to departure. We hope to issue regulations by October to require advanced provision of electronic information for all modes of transportation. Finally, Customs and Border Protection's Automated Commercial Environment, or ACE, will improve the collection and sorting of trade data, expediting trade and enhancing our targeting of high-risk cargo.

Technology is a critical tool that enables the hard-working men and women of the Department of Homeland Security to balance our national security imperative with the free flow of goods and people across our Nation's borders that form the essence of our culture and values here in this country.

We look forward to an important partnership with this Committee, as well as the State and local and private partners that help us to implement these initiatives and to comply with the mandates that Congress has given to us.

Thank you for this opportunity to appear before this Committee.

[The prepared statement of Mr. Hutchinson appears as a submission for the record.]

Chairman KYL. Well, thank you very much, Secretary Hutchinson. I will begin by asking you a couple of questions, and would ask all of the members of the panel to address your questions to Secretary Hutchinson and if he needs to defer to one of his colleagues at the dais, then he will do so.

In your testimony, you note the force-multiplying nature of technology, and I especially appreciate that at the border between Mexico and Arizona where we have such vast stretches of land that it is really impossible for Border Patrol agents to secure that border by their mere presence at all times. As a result, they are using technology.

Since we are going to be there this weekend and see some of this firsthand, and also recognize the vastness of the area that needs to be covered, perhaps you could talk a little bit about what you have learned about the department's deployment of technology and

what you think we might be looking at in the future to use this force-multiplier at our border.

Mr. HUTCHINSON. Thank you, Senator. Technology is critical if we are going to protect our borders between the points of entry, in particular. I am delighted that Congress gave the Homeland Security Department a Directorate of Science and Technology, an R and D shop, and I envision even our Border Patrol agents out there identifying technologies that might be helpful, or industry applications that will be reviewed by the Science and Technology Directorate to see if they are appropriate to be deployed.

At present, we are using aerial flights, of course, but also motion sensors. And then, in combination with that, we have the integrated surveillance and intelligence system that has cambers on poles that are triggered by sensors that are monitored. That allows the Border Patrol to monitor what is happening in the open spaces and to be able to respond. Of course, those are between the ports of entry.

We have to look at new technologies. Drones have been mentioned, unmanned surveillance vehicles that can be used. Those have previously been tested by the Border Patrol in a pilot study and they declined to use them. I think that we have to revisit some of this technology since September 11 and see if it has greater application. We have relied upon the Defense Department to explore and develop this technology to a greater extent and, as they have improved its capability, we have to look again to see if there is some capability on the border.

Chairman KYL. Thank you. One of the things we will see when we go to Nogales, Arizona—Senator McCain and I visited there a couple of months ago, and you mentioned the bright, hard-working people who now work with you at the department. Some of these people literally on their own designed a facility for large semi-tractor trailer trucks to pass through in a very rapid way, permitting them, however, to check for a variety of things.

I won't mention all of the things they can check for here, but it looks just like a huge, giant car wash for a truck. But I am told, as they proudly pointed out all these different kinds of sensors, and so on, that it will enable them to rapidly pass the vehicle through, but at the same time be able to detect pretty much anything that they would want to try to find. So I am looking forward to hearing from some of the folks who are actually at the border having to make these things work.

Quickly turning to a couple of different subjects with the money that we have made available and just to see if you have determined yet how this might be spent or, since you have been there such a short period of time, to at least acknowledge the issue that we will have to deal with, in the President's 2004 budget $500 million is available for additional inspection technology to increase our border and port security. Do you have any knowledge yet as to how the department will be putting that money to use?

Mr. HUTCHINSON. That money will be handled through the Science and Technology Directorate, and we have, I believe, Under Secretary-Designate Chuck McQueary, whom I have talked with on a number of occasions. That is going to apply good standards as to looking at existing technology. That money can be used to provide

grants to businesses or academic institutions to explore technology and test and pilot projects for implementation.

So from the operational standpoint, we will work closely with Science and Technology to carry on these pilot projects. Some of that will be in the Entry-Exit System because we are going to have to obviously pilot areas there and work with Science and Technology to make sure we get the right system.

Chairman KYL. One other item of expenditure. In our homeland security 2004 budget outline, we have a comment that true homeland security requires technology that guarantees real-time information-sharing, improves response time to detect and respond to terrorist threats, and improves decisionmaking. We go on to talk about the inclusion of the Chimera interoperable data system to help facilitate that purpose.

Even though the law that the President signed last May didn't outright fund the program and money was not included, therefore, in the 2003 omnibus appropriation bill, there was $245 million dedicated to IS information technology infrastructure. I am wondering if you have determined yet how to apply that $245 million and whether any of it can be dedicated to the interoperable systems such as Chimera.

Mr. HUTCHINSON. The answer is yes. We are working very diligently to accomplish the goals of the interoperable system. Steve Cooper is our chief information officer at Homeland Security and I have visited with him, looking at how we can accomplish these goals. He brings the expertise in from an IT standpoint.

We have made significant progress and I want to invite my colleagues to comment further on that.

Mr. MOCNY. As I understand it, Senator, the 245 is a ceiling that we can spend up to in order to supply this technology. I think what we are looking at is across the board, as the Secretary has mentioned, exactly how to best apply that technology.

One of the things that we have included within our spend plan for the Entry-Exit System is an infrastructure increase. As noted earlier, biometrics will be part of the entry-exit program. We currently don't have the infrastructure in place to accommodate that. So I think money such as that $245 million, plus portions of the $362 million that we received for entry-exit, will go for that infrastructure improvement.

Chairman KYL. Mr. Hall, anything further?

Mr. HALL. Yes. There is a review currently underway that was mandated that is being jointly done with the Department of Justice that is nearing completion and we will be reporting back in the May timeframe.

Chairman KYL. All right, thank you very much.

Senator Chambliss.

Senator CHAMBLISS. Thank you, Mr. Chairman.

Mr. Secretary, you have probably heard Speaker Hastert use this example and I want to cite it to you as a real flaw in the procedure that has been ongoing particularly at our border on the south, and that is that at any one location, whether it is Nogales or whether it is Laredo, we have any number of stalls that every vehicle has to go through. And it is very obvious that the bad guys have people

sitting in the woods on the hill with binoculars checking each of these sites where the vehicles are going through.

Because of the various jurisdictions that are in place at the border, the INS folks may be checking one lane and they have the power and authority to do certain things, maybe look in trunks, maybe not. DEA may be at another location and they have power and authority to do certain things, maybe look inside the vehicle, maybe ask people to get out, maybe not.

The people who are sitting on the hill are directing their truck drivers or their automobile drivers to a certain number of entry points based upon where they have illegal people or illegal drugs. The folks are going to that particular location knowing that that particular agent can't look in his trunk. I know this was somewhat addressed in the Border Enhancement Security and Visa Reform Act.

Have you had an opportunity to address this in the short time you have been in your position? What are we doing with respect to long term trying to solve this problem?

Mr. HUTCHINSON. Senator Chambliss, likewise I have been with Speaker Hastert and he has made that comment and there is some reality there. Certainly, those who want to bring illegal goods in across the border do their own surveillance and they look for weaknesses.

I think from our standpoint, strategically we have to be flexible to respond to that. We have to shirt our mode of operation so that it is not as predictable, and then I think we have taken a good step at the Department of Homeland Security.

As you know, you had Customs inspectors and you had INS inspectors and Agriculture inspectors at each port of entry all reporting up to three different port directors, all reporting up to three different departments of Government. We have combined the inspection services with the Border Patrol into the Customs and Border Protection Bureau. So you have clear leadership, lines of authority, and you have got the greater potential for cross-training that will address some of those weaknesses.

I think, finally, obviously it is intelligence. They try to look at what we do. We need to know what they are planning, and so we want to be able to enhance our human intelligence capability, too, so that we can have effective procedures to counter that.

Senator CHAMBLISS. So is everybody that is going to be checking at the border now going to be physically under your jurisdiction?

Mr. HUTCHINSON. That is correct, through Commissioner Bonner, who will be head of Customs and Border Protection.

Senator CHAMBLISS. That will make a huge difference.

Second, as you know, one primary focus that I have had over the last couple of years is information-sharing between Federal agencies as well as vertically down to the State and local level.

Picking up on what Senator Kennedy said and what Senator Kyl mentioned there, how are we doing with respect to information-sharing with regard to INS, APHIS, everybody that is under your control, and the respective law enforcement agencies—FBI, CIA, or whoever?

The CIA and FBI are doing a better job, but it certainly doesn't need to stop there. That is just the very, very beginning point. I

want to make sure that your folks have an ongoing relationship at the horizontal level of sharing this information across agencies; also, your relationship with the State and local folks particular at these borders, where intelligence information has got to be shared in real time.

Mr. HUTCHINSON. That is the goal that we have and the urgency of that is very clear. Substantial progress has been made since September 11. The mandate of the President, the Attorney General and Secretary Ridge is to make sure that we share information. There are some obstacles in terms of systems and that is what we have to work with this Committee to overcome.

For example, since September 11 the visa applications and information from our overseas consular offices have been made available to our inspectors at the border. When you look at what the FBI has in their NCIC system and their wanted persons, those have been added to the immigration IDENT system.

This last week, I was at the Newark Airport port of entry and the inspector was showing me that they have access to the INS data base and they have access to the FBI data base, and it has made an enormous difference. These are new accesses since September 11.

The problem is there are two different systems. We still need to make them more interoperable, but enormous progress has been made. Since January 2002, INS checks have produced over 4,500 hits on this new availability of records. That is more than 300 a month, on the average, of individuals being checked that have committed crimes or have some basis to explore further.

Senator CHAMBLISS. The integration of those systems, I agree with you, is critical. Are we giving you the resources to do that?

Mr. HUTCHINSON. I think we are where we need to be right now. I think it is important as you look at the commitment of resources that we get organized, we have a good plan, and we have a logical way to evaluate that. So Congress has appropriated money to start on these initiatives and we report back as to the progress that we are making and continue to evaluate it.

Senator CHAMBLISS. Thank you.

Chairman KYL. Thank you.

Senator Feinstein?

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

I just wanted to quickly followup on something Mr. Chambliss said. The street name for the people he is referring to are called spotters, and I have been to the border at Otay Mesa twice and watched the spotters work. In the last administration, I weighed in as heavily as I could to try to create an effort to do something about it and it always came back legally that there was nothing the department could do.

I suspect that some of them are legally directing traffic. I suspect that others are illegally, when contraband comes across, diverting that traffic to an overcrowded area where they know that truck can go through. But it is a problem out there and I can even show you where to stand at Otay Mesa to observe without being seen. I think it is important that, in view of 9/11, we take another look at that issue.

I wanted to ask you for a couple of updates in two areas. One is the entry-exit area and the other is visa waivers. The bill that we passed in 2000 requires that automated entry-exit systems be deployed at all land and sea ports by December 31, 2003—those are ports of entry—at the 50 largest land ports by the end of 2004, and all land ports of entry by December 31, 2005.

Are you on track? What problems do you find? Is this doable?

Mr. HUTCHINSON. There has been a substantial amount of work that has gone into that and after I make some comments, I would like to ask Bob Mocny, who has worked on that very closely, to add to my comments.

They have worked in a planning arena. The biometric component has been added to that, which adds to the complexity but also the effectiveness of the program. It is now over at Homeland Security. We are going to do our own measurements and move very aggressively on it.

We believe that the first deadline of entry-exit information at our airports and seaports can be met this year. The greater challenge will be the 2004 and 2005 deadlines of the land ports of entry because that takes new systems, new infrastructure likely to be built, and systems that are not even in existence today. We are going to more closely evaluate that and report back to Congress as to where we stand on that and where we stand in relation to the deadlines. We believe there is an urgency there. We are going to work very hard, but there are many challenges there.

Bob?

Mr. MOCNY. Thank you, Mr. Under Secretary.

As the Under Secretary mentioned, we plan to meet the date for December 31, 2003, for the Entry-Exit System. What we will buildupon is what Congress also mandated as of October 1, 2002, for the visa waiver program. So we are currently collecting arrival and departure data for all visa waiver passengers arriving to and leaving from the United States. We will buildupon that to meet the 2003 date, December 31.

But again I will reiterate the challenges for the land border are daunting, especially when you talk about the 50 largest land border ports of entry—some of the environmental laws that apply, some of the infrastructure improvements that we will have to take care of—without doing some of the things that we have talked about here which are backing up traffic. We have to make sure we have an efficient flow, at the same time a secure flow.

Senator FEINSTEIN. Let me, if I might, followup on that and ask you about the visa waiver. I believe there are 27 countries and about 23 million people that come in without a visa, and nobody knows if they leave again.

Can you say that that is no longer the case?

Mr. MOCNY. Again, yes, we collect the arrival and departure records of all visa waiver applicants at this point.

Senator FEINSTEIN. So you know if somebody comes in and doesn't leave? You know that?

Mr. MOCNY. Well, yes. We would have an exception report that would tell us who hasn't left.

Senator FEINSTEIN. And then what happens?

Mr. MOCNY. Well, it is a resource issue about applying the appropriate resources to go and find that individual.

Senator FEINSTEIN. You are not saying nothing happens?

Mr. MOCNY. No, I guess I am not saying nothing happens, Senator. One instance I know for sure is that we have had some visa waiver applicants encountered as part of the NSEERS process and we have been able to deny their entry. But as far as immediately understanding when a visa waiver applicant has not left the country, at this point we are not in a position to be able to go and find that person immediately. That is why we want to work on expanding the program to do so, but we are collecting arrival and departure data as we speak.

Senator FEINSTEIN. I know how difficult it is, so I am not trying to be critical. Of these visa waivers, how many has your system shown up do not leave the country?

Mr. MOCNY. I don't have that number with me today, Senator. I could provide that to you.

Senator FEINSTEIN. Well, I would like to ask some questions in writing, then, if I might, about that particular program.

Let me ask you about false documents. Current immigration law doesn't require all travelers, such as U.S. citizens and Canadian nationals, to present documentation when entering our country at land border ports of entry. But one concern that has been raised is that aliens might falsely claim United States or Canadian citizenship and circumvent the Entry-Exit System.

What changes, if any, to administrative law, treaty obligations or current practices will be required to address this potential limitation of the Entry-Exit System?

Mr. HUTCHINSON. There is going to have to be a substantial review of our working relationship with Canada and our other partners that have traditionally had minimal documentation to enter the country. As part of the Entry-Exit System, Congress is requiring travel documents to have a biometric qualifier that is readable and that has a level of integrity, forgery-proof.

So when that is in place, that will impact all of our partners and we are currently discussing these relationships with the State Department and others, and with our Canadian counterparts. There are going to have to be some changes in order to accomplish those objectives.

Senator FEINSTEIN. I note that the GAO report entitled "Border Security: Challenges in Implementing Border Technology" on page 3 mentions that they have found four different scenarios in which biometric technologies could be used to support your operations. They make the point that certain biometric systems don't help with forgeries, et cetera, and others do. I am sure you are probably aware of that and whatever system you choose will be one that supports being able to get at forged documents.

Mr. HUTCHINSON. Absolutely. That is the mandated objective and if we can't accomplish that, then we have wasted a great deal of effort.

Senator FEINSTEIN. Right. Thank you. Thanks, Mr. Chairman.

Chairman KYL. Thank you.

Senator Kennedy?

Senator KENNEDY. Thank you very much.

Looking at false documents, Secretary Hutchinson, I can remember my good friend, Al Simpson, having hearing after hearing on this and the one conclusion he came to, and I agreed, is unless you have a temper-proof birth certificate, you are not really going to be able to get a handle on the legitimacy of these documents.

The idea of getting a tamper-proof birth certificate and for the Federal Government to require this from every town and village in this country is really unthinkable, although he talked about it and tried to do it, quite frankly. So you are facing a daunting challenge, and you have got a lot of able, gifted people in your department and if they have other ideas about how to get back to that root document, it is just incredibly important. Otherwise, you are going to get whipsawed through this.

You talked about risk management, I think, and you talked about the visa waiver countries. The visa waiver countries have to have, as I remember, 96-percent return in order to continue to be part of the whole program. I think it was 96; there was a 3- or 4-point difference. That has to be maintained or they can't maintain that.

The basic point, as I remember, when it was developed was to—as you mentioned, you are talking about risk management and the allocation of personnel. These are people from these various countries that come back to the country and therefore they pose less of a challenge in terms of following people that are coming into the United States and overstaying their visas.

They present less of a challenge, and therefore you need less personnel in terms of monitoring this and setting up shop in these various countries. That is the principal reason that program had been set up and worked reasonably well, I think, over the period of time. It is constantly being reviewed, but I, like others on the Committee, want to continue to make sure that it is doing what it should.

There are two areas I want to cover and that is the training of personnel that you have and how you are going to keep good personnel. It has come to our attention that a lot of the very skilled, trained personnel in immigration are going out to other agencies.

How are you able to really keep the best of the personnel that can really help you do the job? What are the training methods, if you could review those? You can provide this in greater detail, but this is, I think, very important.

Then I want to get just finally to the issue of risk management. Your response to an earlier question about the border—we have got 130 million vehicles that come into the country every year, and 500 million people moving back and forth. I always thought that the terrorists are the problem, not immigration. The real question for you people is how you get the difference on it using the technologies.

I am interested in how you are setting up these risk management decisions. I mean, that is going to be key in terms of trying to do it. Maybe some of this is classified. I don't know, but how do you do it? We don't want to have others that want to try and break through the system listen to you and then find out how to avoid it. but as much as you can tell us on what you are doing on the training, what you are doing to get good people to stay in the de-

partment, and also if you can talk a little bit about the risk management, those are two areas I would like to just cover in the time that I have, please.

Mr. HUTCHINSON. Thank you, Senator Kennedy. In reference to the visa waiver program, the Justice Department started the review and we are going to complete it as to some of the countries and their compliance rate, whether there needs to be any adjustment on that, and we owe some reports to Congress on that.

In reference to the training, you hit it right on that this is essential to keep a motivated work force, to keep them on top of the technological skills that are necessary. I am delighted that in the Border and Transportation Directorate, in addition to the agencies that are out there on the front line, we have FLETC, which is the Federal Law Enforcement Training Center. So we want to utilize them, as these agencies have done, from TSA to Customs to INS, to make sure that training is at a high quality.

One of our challenges for the worker is that we have disparate pay scales for the different agencies that have come on board, the inspectors for Customs versus INS, and the Agriculture inspectors. Janet Hale, our Under Secretary for Management, will be working with the employees over the coming months, having hearings and looking at ways that we can bring this together. This is a congressional mandate and we owe a report back, I believe, in November, as to how we are going to be reconciling these different pay scales.

Finally, on risk management, this is an essential part of the strategy that we have to implement. In reference to the cargo side, we have the Container Security Initiative that gives us manifest information for cargo coming into this country 24 hours in advance to the time that it is loaded on the foreign port. If it is Hong Kong or Rotterdam, we get the information in advance going to the national targeting center at Customs, and then you have the analysts that look at this cargo and they have a rules-based system that asks the questions—is it a trusted supplier, what is the record, what kind of cargo is being represented—a whole host of rules. You give it a scale and you identify the risk to it.

The objective is not to inspect one hundred percent of all the cargo coming to the United States, but a hundred percent of the at-risk cargo. So that is the system. I saw it demonstrated in Newark, again, when I was there. It is not perfect by any means, but it certainly moves us in that direction.

We are doing the same thing for at-risk people. One of the responsibilities is we look at the visa issuance overseas and take a greater role in making sure that it does not go to high-risk people.

Senator KENNEDY. Also, just with regard to people, you want to make sure that the visa that you are giving to the person is actually the person that has been cleared and the one that is arriving is the person that goes back to the country. That is a continuum and we tried to spell that out in the legislation, and that has been area that has been a challenge in the past and that is absolutely true about the people, as well.

Well, if you could just supply the other training programs and how you are setting up this training to get your people up to speed on this, I would be interested in what the department is doing.

Mr. HUTCHINSON. I would be happy to.

Senator KENNEDY. Thank you.

Chairman KYL. Thank you. To just add on what Senator Kennedy was just talking about, to retain the Border Patrol agents, for example, who speak Spanish by their required training and are not paid particularly well compared to some other law enforcement agencies who constantly raid the Border Patrol for these experienced agents, I think that is also referred to in Senator Kennedy's comments and we would like more information on that, too.

With my Republican colleagues' indulgence, I would like to turn next now to Senator Leahy.

Senator LEAHY. Mr. Chairman, I thank you and thank you again for your courtesy. I especially wanted to hear what Secretary Hutchinson had to say, although I should also note that any time I have called the Secretary, he has been immediately available and I have always felt that he was willing to answer questions. I appreciate that.

Mr. HUTCHINSON. Thank you, Senator.

Senator LEAHY. I think it comes from his experience here on the Hill when he was faced with having to ask similar questions, and all of us do our jobs better when they are answered.

I mentioned earlier what a massive undertaking the Department of Homeland Security is—170,000 employees, 22 different agencies. One day they are all separate; the next day they are one agency. It doesn't say anything that you don't already know that a lot of those 170,000 employees are not quite sure how their jobs changed on March 1 or what their future is. They are focused first and foremost on protecting America, not just on their job security, but you know it has to be in the back of their minds and that can affect job performance.

What kinds of steps are you taking to communicate with the rank-and-file in the DHS to assure them that questions they might have on their own status don't affect the mission of improving our domestic security, a mission that we all agree upon?

Mr. HUTCHINSON. It is essential to give them the facts, communicate with them clearly. We are doing it in a couple of ways, obviously through Internet communication, but Secretary Ridge has been very engaged in employee town meetings both in Washington and in Miami. I have done the same thing, listening to them, but also trying to assure them that when they came on board March 1, same mission, same pay, same job responsibility. The only issue was whom they would report to and there were minimal changes there.

As time goes on, there will have to be more changes that are made. We want to work with both the union leadership as well as with all of the employees to make sure there is a good line of communication both ways. We don't want them to worry about it, and I think that there is really not reason to worry. Congress has protected it, rightly so, for a year to make sure no one is displaced. But we are still growing in numbers and so I don't think there will be a displacement; there will just simply be effective reorganization, I would trust.

Senator LEAHY. Well, that goes to another issue. Incidentally, I would invite you or your designee at any time to come up to Vermont. As has been pointed out, it is a tiny State, but we———

Mr. HUTCHINSON. Can I get some syrup?

Senator LEAHY. Yes, sir, I will give you that anyway, as you know. But come on up. We have the northern border. Senator Kyl spoke about agents who speak Spanish. Right where we are, we are more apt to find them speaking French.

But we have the border. Actually, we have a couple of the alien tracking facilities and others that we have in Vermont. You see some very dedicated people, but you also see the kind of problems we have; on the one hand, keeping commerce and families moving back and forth on a border which they think of almost being like a border between two States, and at the same time, as we saw, one of the terrorists came down on the northwest border with designs against the Space Needle in Seattle. So there are all the different issues there.

But I look at the fact that the Justice Department Inspector General recently reported that 26 percent of the INS inspections work force was hired in fiscal year 2002, showing a lot of attrition and change. Now, this is a very important fact. If you have 26 percent of it in 1 year, are you focusing on the fact that you don't want attrition beyond the normal attrition you always face because some of these are highly skilled jobs?

Mr. HUTCHINSON. Absolutely, and we want to be able to keep the morale up. I think that some of the factors previously were morale, a tremendous amount of responsibility. Congress has helped on the pay scale side of it, and then we also had TSA setting up and that was a factor in losing some Border Patrol and INS personnel. I think it has settled down substantially since that timeframe because TSA is organized now and functioning. They are not having to have that huge hire-up.

And then, second, the fact that Homeland Security was created, I believe, is a motivating factor and the mission is renewed. But these are things that I assure you we are attentive to because we want to keep a motivated work force.

Senator LEAHY. I don't mean to keep harping on the northern border, but we always focus on the southern border, and rightly so, but they are entirely different things. We are not having people streaming across our northern border looking for jobs or a better standard of living. They are very happy with the standard of living in their own country, in Canada.

We face other issues and I think because of that, well before September 11, we kind of neglected the northern border. We always worried about what was happening on the southern border. We have proposed increases. S. 22, for example, is pending, the Justice Enhancement and Domestic Security Act. We propose additional increases in the Border Patrol.

I mentioned the helicopter that came down, and in this case a group of snowmobilers spotted the bales of marijuana, 250 pounds, being tossed out. Well, we can handle the issue of the marijuana. I am far more concerned, and I am sure you are, too, if that been explosives, weapons, or terrorists coming down, knowing that they then could drive to New York City or Boston or several of our major ports in literally a matter of a very few hours from where that was.

Do you support our efforts to authorize additional border security personnel?

Mr. HUTCHINSON. Well, I support what you have done in terms of increasing the presence at the northern border. I want to make sure I understood the question correctly.

Senator LEAHY. Let me put you in a more difficult position, if I might, and you may not want to answer this, but I want you to think about it. The President's budget for the Bureau of Customs and Border Protection calls for less than a 3-percent increase over his budget for those functions in fiscal year 2003. That is not going to even cover inflation.

Is the status quo in terms of personnel on our northern border adequate?

Mr. HUTCHINSON. Let me answer it this way, Senator, with great respect. We certainly need to finish the deployment of more Border Patrol agents on the northern border. There is an increased need there. Since February 8 of this year, 220 agents have been deployed to the northern border, so we are continuing to do that. There needs to be an increase.

In reference to the overall budget, which I think is the essence of your question, my figures show that there was a little bit more of an increase in the overall homeland security budget. The discrepancy might be the fact that TSA obviously had some enormous startup costs that were not reflected and needed in the 2004 budget.

I think it is important that Homeland Security gets an opportunity to organize effectively, then to evaluate our needs, and we will report back to you. So I think we are where we should be right now, but obviously we need to continue to evaluate it with you.

Senator LEAHY. Well, Mr. Chairman, I thank you for the time.

I would say, Mr. Secretary, I know you obviously are constrained by what is in the President's budget and I understand that. I would expect that of anybody speaking for the administration, but please understand that I and many others feel that we are not doing enough on the northern border. I would like some time perhaps in the near future where you and I might discuss this because I really feel strongly that we have some problems that could come back to bite us both from a security angle, but also from the question of just keeping the free flow of commerce between two great nations.

Mr. HUTCHINSON. I welcome that opportunity, Senator.

Senator LEAHY. Thank you. Thank you, Mr. Chairman, and again I applaud you and the other Senators for having this hearing. I think it is one of the most important ones this Committee will do.

Chairman KYL. Thank you, Mr. Chairman—well, I am used to calling you "Mr. Chairman."

Senator LEAHY. Oh, I love it.

[Laughter.]

Chairman KYL. There is a University of Texas study now a few years old and we need to be sure and get that to you, Secretary Hutchinson, if you haven't seen it. It calls for about 16,000 Border Patrol agents on the southern border and doesn't even begin to address the number that would need to be put on the northern border

to secure that border. That was a pre-9/11 study, so it is the kind of thing that we would maybe appreciate to get your feedback on.

It is probably not possible to achieve that level any time soon, but Senator Feinstein and I have sponsored legislation that was adopted that called for adding 1,000 new agents each year, net. We are now beginning to fall behind that again, so perhaps we can revisit that.

Senator Craig?

Senator CRAIG. Well, Mr. Chairman, you in one of your questions and Secretary Hutchinson's response was one of my questions as it relates to the vastness of these borders beyond points of entry or between points of entry and how you deal with it.

I come on the heels of Senator Leahy's questions to react very similarly. The uniqueness of these borders, north and south, are very real. The port of entry that Idaho has is one of many. There is an official one and then there are hundreds of small, back-country wilderness roads, logging roads, because that relatively small border expanse compared to Texas that Idaho has against the Canadian border is in many instances wilderness or very close to it.

But people traffic it and it is nearly impossible to control it, patrol it, shape it in any given day or hour unless you just had a phenomenal work force that is probably not that justifiable at the moment, compared to the southern border or more concentrated areas where heavy commerce is moving, although the commerce between the Pacific Northwest, Idaho being a conduit, has increased rapidly over the last couple of years.

I guess my question would be, briefly, could you talk about your working relationship with Canada, because if you gain access through Canada and your intent is to come into the lower 48, my guess is you can get there without going through a port of entry and you can probably get here without being detected if you spend a bit of time studying the terrain, whether it is the State of Washington, Idaho, Montana or Vermont. Those northern borders are in many instances obscure, almost dense forested wilderness areas that have very little patrol.

Mr. HUTCHINSON. Thank you, Senator Craig. It is important that we make sure we protect the northern border and devote resources to it. In reference to Border Patrol agents, we have increased them substantially on the northern border. Eighty-one percent of the requirement for the northern border, a goal that Congress gave us, has been met for 2003. We are going to continue to make that deployment.

In reference to our relationship to Canada, it is excellent. Both while I was at the DEA and here, I have had a great relationship with the Royal Canadian Mounted Police. Secretary Ridge has met numerous times and developed the Smart Border Accord with Canada that has a number of different points to it, including shared information, including some of the fast lanes at our ports of entry, but also the information for our rural areas, our isolated areas. We have to know what they observe on their side, what the risks are, threats are, and then we have to share that information. The relationship is good. The challenge is great. We are going to continue to focus on that.

Technology is important. We have enhanced the number of helicopters that the Border Patrol has available and their presence is becoming more significant on the northern border and needs to continue to do so.

Senator CRAIG. Do they do a good job screening those who enter Canada from foreign countries? Do they have a fairly rigid system of control, application, tracking of those coming in, because part of my question, Mr. Secretary, was if you can gain access through Canada—that means to Canada from outside—and your intent is to come to the United States through that conduit and you spend any time trying to do it, my guess is there is probably a pretty good chance you can get here without going through a port of entry.

Mr. HUTCHINSON. It is a significant area of concern. I know that Canada has tightened up their entrance requirements and their protective systems since September 11. It was a wake-up call for us and Canada, but there is much work to do there. We are continuing to work on that, and obviously the interest of both is to make sure we don't stop the flow of commerce. That is their objective and our objective, but they recognize a huge security need, so we will continue to work with them.

Senator CRAIG. What kind of sharing goes on of information of individuals flowing into Canada that for some reason would draw attention, or is there any of that kind that they share with us?

Mr. HUTCHINSON. For example, when I was in Miami—we have an exchange with Canadian Customs so that a Canadian Customs officer was physically located in Miami working side by side our agents because there is a great deal of commerce going from Canada down to Miami. The same thing was true in Newark. We had a Canadian Customs officer there working side by side. We have the exchange there so that we have access to some of their data bases and their information through their Customs officers, and likewise for our personnel up there. Whenever we are looking at our data bases for names and suspects, we can have that relationship to exchange information with Canada. So it is getting better everyday. There are some real signs of encouragement there.

Senator CRAIG. Thank you. Thank you, Mr. Chairman.

Chairman KYL. Thank you.

Senator Cornyn?

Senator CORNYN. Given that all 19 terrorists from September 11 entered the United States on legal visas, would you just summarize what both the Department of Homeland Security and the State Department have done to address that specific challenge?

Mr. HUTCHINSON. The first thing that was done is that whenever the consular offices overseas get information on visa applicants, that information for the first time has been made available to our inspectors at the ports of entry. That was a significant breach in communication prior to September 11 that has been remedied. That way, you really have a layered protection so that now they can screen them closely in the overseas consular offices, look at them, interview them, and then there is information so that before they arrive at the port of entry, they will be again examined. Hopefully, both of those checks will keep someone who has harmful intent from coming into our country.

The visa issuance responsibility for regulation and training has been transferred to Homeland Security. We are now negotiated with the Department of State on a memorandum of understanding to accomplish this exchange of authority, because they will continue the technical work of issuing the visas, but we have the oversight responsibility with people present there in some of the overseas offices to make sure that program is working effectively.

Much progress has been made, but it is an ongoing effort. We still need to enhance the information in those data bases for checks and for a quick response. Now, when those applications are made, they go through the State Department lookout list. They also go through the FBI and all the other checks interagency-wise to try to make sure we detect those that might have a harmful intent or a criminal record.

Senator CORNYN. Knowing what we know now about these 19 individuals, could the changes that you have just described have prevented their entry into the United States?

Mr. HUTCHINSON. Well, I don't know if I would want to—I would certainly hope so. It would increase the likelihood of it. I would add that Senator Feinstein made reference to some that were here on expired visas, and that is what the SEVIS program, the student visa monitoring program and information, will help us with.

We will know who is here on an expired visa or who is not reporting to school when they are here for that purpose. So we have enhanced our capability to better protect America and we are continuing to do so. But as was pointed out, it is one thing to have the information of people who are here visiting our country and leaving and maybe they didn't leave in time, but it is another thing to have the analytical capability to pinpoint them, find them and make sure they leave our country. So we are working on each of those levels and it gives us a safer America.

Senator CORNYN. As you know, the United States and Mexico are important trading partners and a lot of the commerce that flows between our two countries comes across the Texas border. And, of course, it is important to the economy not just of my State, but to the United States, that we maintain as free a flow of commerce as possible. One of the things I know of at the State level, because I worked on it when I was attorney general, is the establishment of one-stop border inspection facilities.

Could you describe for us from the Federal perspective what the Federal Government is doing to try to implement a one-stop inspection facility? In other words, notwithstanding the fact that Customs and Immigration may need to do an inspection, we also need to make sure when a truck comes across that the Department of Public Safety in my State, for example, can assure that this truck is in a safe condition so as not to jeopardize the safety of the driving public.

Mr. HUTCHINSON. Let me ask Mr. Woody Hall to respond to that, if I might, Senator.

Mr. HALL. We are doing a number of things. We have always had cross-designated inspectors and we are going to put more emphasis on that training so that folks who come from a different background as we stand up the new bureaus can be interchangeable.

We also are working closely with the Department of Transportation to see what we can do to improve this relationship with the State organizations that need to do these safety inspections. And we are also investing in the modernization of our information technology infrastructure so that we can share this information not only across the bureaus within Homeland Security, but as appropriate with other departments and local law enforcement agencies. I think all of these efforts taken together will help improve the situation that you have described.

Senator CORNYN. Well, I certainly don't underestimate the challenge that you have or that our country has in this area of trying to strike a balance between our security and commerce. Both are important and we need to strike the right balance, but I would like to have my staff perhaps talk at a staff-to-staff level to try to get some more details.

I think it is very important that the Federal Government work closely with local officials and with State officials to make sure that as much as possible we try to remember that the commerce aspect of this is also an important element to consider and that we do as good a job as we possibly can striking that right balance.

Thank you very much.

Mr. HUTCHINSON. Thank you, Senator, and we would be glad to visit with you more about that.

Senator CORNYN. Thank you.

Chairman KYL. Senator Cornyn, I agree with you. Because of our same issues in Arizona, I remember kidding with then-Senator Spence Abraham, who, of course, representing Michigan at the time, had a border with Canada. He was really irate about these 2-minute delays at the border. And I said, Spence, 2-minute delays? I said we would be happy if we could it down to 2 hours at certain points of time.

So we do have those kinds of issues of accommodating the interests both of commerce and recreation, I might add, visiting families back and forth, as well as the whole need to ensure against contraband, against illegal alien smuggling, and certainly against terrorism.

Secretary Hutchinson, you have mastered a lot in a very short period of time. I think what we will do is submit any other questions—unless anybody else on the dais would like to make a point, submit any other questions we have for the record, and we will leave the record open for a couple of days, let's say 3 days, so that anybody that would like to submit additional questions to you can do so.

Perhaps after you have had a lot more time under your belt and had a chance to digest some of the things that have been thrown your way, you could come back and report status to us at that time. In the meantime, we would invite you to be sure to let us know—as you discover things that we could help you with that we could either put in appropriations bills or give you more authority or whatever might be needed, please convey that to us because our two Subcommittees and the full Committee are really dedicated to helping you be effective in your job.

We are just very glad you are there and, as I said, your very quick command of a lot of details is very, very impressive. We ap-

preciate Mr. Mocny and Mr. Hall for being with us today. Thank you very much. All the best.

Mr. HUTCHINSON. Thank you, Senator. Thank you, Committee.

[The prepared statement of Mr. Hutchinson appears as a submission for the record.]

Chairman KYL. Now, our second panel—and we promise not to take as much time speaking from dais here and we will hear from our witnesses a little bit more quickly—is comprised of two people and I will ask them to come forward as I am introducing them.

One is Nancy Kingsbury, who is the Managing Director for Applied Research and Methods at the General Accounting Office. In this capacity, she manages the GAO's advanced analytic staff, including economists, computer engineers, statisticians, and other scientific experts. She has done a great deal of work in the entire area of homeland security. She will be accompanied by Richard Stana, who is Director of Homeland Security and Justice at GAO.

In addition, Stephen Flynn is the Jeane Kirkpatrick Fellow in National Security Studies at the Council on Foreign Relations. He is the Director of the Independent Task Force on Homeland Security Imperatives, which is commonly referred to as the Hart-Rudman Commission, and was a consultant on homeland security for the previous Hart-Rudman Commission on National Security, and as I mentioned before, has also testified here and probably was listening carefully when we talked about moving our perimeter out further and getting more cooperation from people abroad even before we get to the border here as the last measure of defense. I read your testimony. Thank you.

So, Ms. Kingsbury, let's begin with you, and then I will turn to Stephen Flynn. Since we do have two votes in about 40 minutes, we will try to move forward as quickly as we can.

STATEMENT OF NANCY KINGSBURY, MANAGING DIRECTOR, APPLIED RESEARCH AND METHODS, GENERAL ACCOUNTING OFFICE, WASHINGTON, D.C.; ACCOMPANIED BY RICHARD STANA, DIRECTOR, HOMELAND SECURITY AND JUSTICE, GENERAL ACCOUNTING OFFICE

Ms. KINGSBURY. Thank you, Mr. Chairman.

Chairman KYL. I think you have been advised to limit your testimony to 5 minutes.

Ms. KINGSBURY. Yes, sir.

Chairman KYL. Thank you.

Ms. KINGSBURY. I will whiz right through it.

Thank you for accepting our longer statement and we are very pleased to be here. Rich Stana does most of our work on our immigration issues in GAO and so he is here to represent that work as well.

Facilitating the flow of people while preventing the illegal entry of unwanted travelers at our many ports of entry requires an effective and efficient process that authenticates the traveler's identity. Based on our work, we believe that biometric technologies—that is, technologies that can be used to verify a person's identity by measuring and analyzing his or her physiological characteristics—have a lot to offer over the current paper document examination and

interview processes to facilitate travel while protecting our borders and also facilitating commerce.

That said, it is important to understand that technology is only a part of the solution. Effective border security at ports of entry requires technology and people to work together to implement a decision system that is grounded in well-developed and implemented policies and procedures.

The Department of Homeland Security faces huge challenges to implement the requirements of recent legislation to improve border security, and I think, Mr. Chairman, you have cited some of the numbers—440 million border crossings, 300 designated ports of entry, et cetera. I don't need to belabor the magnitude of this task.

Last year, under a pilot technology assessment process directed by the Congress, we evaluated the utility of a variety of biometric technologies for use in border security. Our report, which, as you can see, is fairly thick, provides considerable detailed information on the maturity of the technologies and on the policy context in which they would be used for border security.

In the end, it appears to us that fingerprint recognition and facial recognition, perhaps in combination, are the most mature of the technologies for this purpose, and that iris recognition held considerable promise as a unique identifier for future use, but it hasn't really been tested yet.

Even in the case of fingerprints and facial recognition systems, however, there are issues of scalability that will require considerable testing and development to bring to the point where hundreds of millions of identity checks annually are feasible, accurate and efficient.

By way of an example, the current fingerprint system, while now automated and very efficient, only contains about 60 million records. So when you are talking about that many border-crossings and that many checks, you have got a real issue of scalability, we think.

Biometrics have been used in border control environments for several years. In the U.S., INS has used hand geometry in its INSPASS system at U.S. and Canadian airports to facilitate the movement of trusted travelers, and INS has implemented a border-crossing card, as we have talked about this morning. Several foreign governments have also adopted limited programs of biometric-based identification for transit of travelers across borders, but they are all on a fairly small scale.

While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control.

In addition, a number of other issues need to be considered—the system's effect on existing border control procedures and people, including how you transition from one type of system to another. The costs and benefits of the system need to be assessed. We did some analysis based on some assumptions. I think Senator Feinstein referred to our scenarios in her question a few minutes ago.

Suffice it to say we are talking billions of dollars just to implement biometrics in this application. We believe it is very important that a thorough and documented concept of operations be created

and examined before these decisions are made and before this starts down the path of spending huge amounts of money.

Finally, the system's effects on privacy, convenience and the economy also need to be assessed. Representatives of civil liberties groups and privacy experts have expressed concern regarding the adequacy of protections for security, data-sharing and identity theft, and about the potential for the evolution of secondary uses and so-called function creep.

These issues can be addressed, and should be, early in the development of a concept of operations. Because there is no general agreement yet on the appropriate balance of security and privacy, or to go back to Senator Craig's point, security and commerce, further policy decisions are clearly required. And I am very encouraged by the interest of this Committee in participating in that process because I think that is very important.

Because visa policies are often reciprocal with other countries, introduction of new requirements could stimulate additional new requirements on American travelers to other countries. This is another policy issue that probably needs to be addressed.

In any event, it is important in that regard when we do this that countries work together to seek a common standard for the introduction of biometric technologies at border-crossings. The inability to do that is likely to escalate the variety of equipment and processes needed at our borders and consulates, potentially further increasing costs.

Finally, Mr. Chairman, we have some ongoing work on current practices for screening travelers at land border crossings that offer some information about potential challenges faced by the Department of Homeland Security as it introduces new technology at our borders. You and your colleagues have talked about a few of these.

We have found problems with the integrity of the inspection process that permits entry into the country with false or even no documents, and some inspection processes are inconsistent or incompletely implemented. Current technology is sometimes cumbersome or not available. There was some comment earlier about multiple entries into data systems. Workload demands prevent meaningful processing or sharing of available intelligence.

And last but not least, the merger of INS and Customs brings together inspectors that to date have been trained in two separate academies, using different curricula, and on-the-job training is often pushed aside by the pressures of inspections itself. They have got a huge job ahead of them.

Thank you for your attention. I would be happy to answer any questions.

[The prepared statement of Ms. Kingsbury appears as a submission for the record.]

Chairman KYL. Thank you very much for your testimony.

Mr. Flynn?

STATEMENT OF STEPHEN E. FLYNN, JEANE J. KIRKPATRICK SENIOR FELLOW IN NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS, NEW YORK, NEW YORK

Mr. FLYNN. Thank you, Mr. Chairman. I am delighted to be back here today, and this time you are in the Chair. Last time, it was

Senator Feinstein when I testified here with Senator Rudman in November of last year. I would like to be able to submit my testimony into the record and maybe just make a couple of, I think, important points to inform our process here.

One, overall, of course, a conclusion of the Hart-Rudman task force report that I had the privilege to direct was that America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil, and in all likelihood the next attack will result in even greater casualties and widespread disruption to American lives and the economy.

The need for immediate action is made more urgent by the prospect of the United States going to war with Iraq and the possibility that Saddam Hussein might threaten to use weapons of mass destruction on America. We said that in October. In my view, that chilling finding still holds true today. It speaks to the enormous importance of what this Committee is looking at here today because we know the new front-line warriors in this new challenge that we are confronting turn out to be these rather mundane folks, in the traditional sense of things—INS agents, Border Patrol, Coast Guard men and women, now all put together under this new department.

The scale of the challenge, of course, is enormous, as has been cited by the figures here today. Secretary Ridge put it well when he assumed his new mantle as Secretary: getting right the job about a billion times a year. When we are talking about the total numbers of front-line field agents, the folks who are really doing the meeting and the greeting and the checking, we are talking about a number of people that is smaller than the NYPD, if we take the TSA portion out of it.

I mean, this is an incredible challenge and if we are not seriously talking about the issue of resources, we really are just engaged in talking, because this is an issue of such vital nature and it requires clearly a long-term investment that I don't believe we are pursuing with the level of zeal that we must.

Just by putting it in context, Secretary Rumsfeld testified last month before the House Appropriations Committee that he is spending $5 billion protecting U.S. bases from a would-be terrorist attack. He also said that 20 percent of those bases he didn't even need because he doesn't have the force structure to fill them. So he said we are spending about $1 billion a year protecting bases essentially that he doesn't need.

We are talking in the area of seaport security, for instance, in this upcoming bill on the order of $100 to $150 million. We are not really getting the scale right. This Nation depends on trade and commerce, and it depends on being a globally engaged, open society. The folks who are at the front lines of managing the risk of that at our ports of entry are woefully understaffed, working with obsolete technologies, inadequate support for training, and are just simply not up to the challenge, not because of desire, but because of the commitment of the national Treasury, frankly, that we haven't put at their disposal.

Now, how do we get a handle on this job when it is a billion a day? And this is a key point that I guess I want to drive home. It shouldn't be a balance, security versus trade; the two are sym-

biotic. The heart of this enterprise, when you have a billion checks to make, is about risk management, but how do you do risk management?

Risk management is fundamentally about having sufficient intelligence so that you can basically detect what is high-risk versus low, and having the opportunity to act on that intelligence. The primary tool used in enforcement and the regulatory world is what is called pattern recognition; it is the ability to be able to pick something out that doesn't look right.

What we saw about the 9/11 folks is that they tried to blend in. I spent 10 years looking at the problem of smuggling from the Caribbean up and across the southwest border, and what you find about good, capable smugglers is they try to blend into the real estate. The ability to pick that up is often not based on intelligence. It is based on a sharp front-line person who says, you know, these goods are coming in on Friday, the farmer's market is on Saturday, it takes 3 days to get to the market, there is something wrong here. Those are the tools.

Now, let's get to this key point—commerce and security. If the system is inefficient, the border is inefficient, it makes the border less policeable. If, because of lack of infrastructure, we have bottlenecks in traffic, a fragmented trucking industry and virtual chaos, you can't detect, which is the only tool we can bring on, given these numbers, the aberrant activity.

So this means that the only way you get toward security is to improve the efficiencies at the border, which is about building the roads, building the bridges, improving the inspection facilities, numbering them with the right number of people so that you can detect them out of the normal rhythm of commerce.

What we know about capable terrorists and criminals is they try to act like market actors, but they usually never get it quite right because they are not market actors. Markets are complex places and you can pick them out. It will be the key tool, but only if there is sufficient transparency within the border setting, and ideally upfront capability, are we going to get to that point.

So it comes down also to this issue of technology, how important it is that it must be integrated in an overall functional systems approach to managing our borders. If the technology is layered on without being adequately prototyped and tested and creates inefficiencies that essentially add to the chaos of the environment, then those eyes and ears of inspectors, the human judgment that is so essential, is just awash with numbers.

I mean, I stood at San Ysidro with INS agents and with Customs agents, and I have been across the border with the Border Patrol and I have been to Laredo and I have been to El Paso and I have been to McAllen, Texas, and Brownsville. In all those places, it is the human judgment that still remains key, though they need the enablers of the technology.

In the chaos of San Ysidro—75,000 people herding across the border to go work in San Diego—if you can't find the means to filter the bad from the good, we are just not going to get to where we need to go. So the point, I guess, I would make and I hope we can explore a little more in the questions is technology is a critical

enabler, but it must be looked at by an overall investment that rationalizes the way our borders and ports of entry work.

We built our national transportation system for internal development, Canada and the United States especially, to "go west, young man." All of a sudden we changed that, post-NAFTA, onto an axis that went north-south, and the infrastructure simply is not there to support that. That contributes to the opportunity for organized crime and terrorists to exploit. So this is not an either/or; this is a must.

The conversation going on over transportation, about building new roads and building the ports, must have a security component in it. An intelligent transportation system can get us where we need to go, and a part of the tool, a collective approach, versus just simply dropping in specific applications—radiation detectors or whatever—must be a part of this approach.

Thank you, sir.

[The prepared statement of Mr. Flynn appears as a submission for the record.]

Chairman KYL. Thank you very much. I am going to box that testimony up and send it over to the Appropriations Committee because that is exactly the kind of point, it seems to me, that we need to make to those who are responsible for appropriating the funds for these purposes.

Those of us in border States have been trying to make this point for years that it is not only good for our business, but would enhance our security, to have an efficient port of entry system. So everything you have said makes a great deal of sense to me.

I think, as I said to Secretary Hutchinson, we need to take a look at the Customs report of 3 years ago and advance forward to today's requirements, have them update that and see what they think we need in terms of infrastructure. We have all talked about the relationship between people and technology, and everybody acknowledges we need both and they have to work together.

It seems to me the key challenge is this, and this is the question I would really like to pose to all three of you and let me analogize here. Secretary Rumsfeld saw early on that if he was to develop an effective missile defense system to protect the United States, as President Bush asked him to do, he would be long dead and gone by the time it ever even got up and running, let alone deployed, if he went through the usual system of procurement and acquisition that the military relies on.

So he decided to take what we had, put it together as quickly as possible, field a couple of those units, see how they worked, at the same time that we are continuing to develop other technologies and try to integrate them into a system, so that over time we could have a deployable system, but in the meantime we would have something to protect ourselves with because the need is now and under the old method of procurement, we wouldn't have anything for another 10 or 12 years.

Now, you have testified, Mr. Flynn, to the immediate need to secure our borders. There will be more terrorist attacks and we have got to match our resources to the rhetoric. We also have to match our programmatic system around here to the timely challenge, and this is, Ms. Kingsbury, where I get to you.

You have properly said that we need to walk before we can run. There are a lot of bugs in the technology that have to be ironed out before we commit billions to a particular system in a particular place, and so on. But we don't have that time, clearly. So the question is how we square that circle, how we make the best judgments about getting things into the field as quickly as possible that are the force multipliers, the technology that we know exists and that we are beginning to use to do it in a very intelligent way, but in a way that gives us some protection in the short run, while not committing errors that become costly in the long run.

So I don't think we have the luxury of waiting. Mr. Flynn makes that point. We don't have the luxury of wasting a lot of money because this whole thing is going to cost a lot. So how do we square that circle?

Is it possible, for example, that pilot projects, things like the laser visa system that is being tried with Mexico and the United States, are some of the answers to that? I will just ask that open-ended question for all three of you to quickly respond to.

Is my time on here? I don't want to take more time that I am supposed to.

Ms. KINGSBURY. It just went green.

Chairman KYL. Yes, and I have already taken 3 minutes, so knock off 3 minutes of my time.

Let me start with you, Ms. Kingsbury.

Ms. KINGSBURY. Well, I am not sure that the analogy is altogether helpful because that system is protecting against something that is likely to be very infrequent, but nonetheless I certainly take your point.

Let me offer an example of the reason why really understanding the whole problem perhaps the way Rumsfeld understands the missile defense problem—the concept of the issue itself is pretty clear. You can have a perfect biometric—and let me make it clear none of the biometrics, including fingerprints, are perfect—but if you don't also have a pretty darn good enrollment system at the outset, with real commitment and real resources to that, you guarantee the system will fail and you will buy no security at all, for all practical purposes.

That is why we think the concept of operations is really so important. But once you have the concept of operations, then I think the opportunity and the technologies are there and the vendors are out there quite hungry to do something with them. The technology is there to have a lot of pilot projects and efforts of that sort, and to move fairly quickly in that regard to find out what works and what works better than something else. But I think the concept of operations is crystal clear and I think you have about said the same thing.

Chairman KYL. Mr. Flynn?

Mr. FLYNN. We are a great big, wealthy Nation. We have a lot of threats and we can afford to take them on, but one of the realities of pursuing the Strategic Defense Initiative without dealing with these issues is if you solve the problem up there, you push the problem down into legitimate trade lanes. So you have to be dealing with, even in that concept world, both of these issues concur-

rently because the threat is a weapon of mass destruction. It is a launch vehicle. A truck can be the delivery vehicle.

We are faced in this overall homeland security problem—I describe it sort of crassly as a bit like trying to, in the United States context, take a raised ranch and make it handicap-accessible. It is ugly, it is expensive, and it doesn't work very well. We are struggling with taking basically this great big, open society, with a lot of emphasis on facilitating moving, getting stuff forward with not a whole lot of people in the way, and now suddenly trying to craft it virtually overnight into dealing with this new threat environment.

The initial phase is not likely to look all that pretty. The key is, I think, some investment in resources at the outset because you have just got to get by. The long-term approach is that we have to understand this broader system prospect, and I think the key to getting there right away is the pilot programs.

I have been a big advocate of something that has developed that is called Operation Safe Commerce. The initiative, which is $28 million and has gone out to the ports of L.A., Long Beach, New York, New Jersey, and Seattle-Tacoma, is to go and basically recruit retailers, carriers, terminal operators from the point of origin of where goods come from and see if we can track and if we can monitor the integrity of shipments from the point of origin all the way through.

Now, when you talk about mandating that tomorrow, it is a herculean task. But just stepping out and beginning to do it is a bit like a 1,000-piece jigsaw puzzle. Once you start doing it, patterns start to emerge and you start to get going and the relationships come together and you understand it.

But the key is use the strength of federalism, drill down, get the money out of Washington down to the local levels and enlist the local Federal representatives along with Governors and mayors and their Chambers of Commerce. They can recruit often better than the feds can those retailers and those carriers, and so forth. And let's begin the process of validating low risk.

On the other set of issues, we have some very good programs. The SENTRI program, for instance, can work very well. But when I was on the San Ysidro border, I found with the SENTRI program that it took over 9 months to get into the program because INS didn't have enough people to fill at the entry, and plus it was a pretty hefty fee for a Mexican. Our security improves when we take those frequent travelers and put them in a lane. So don't charge a fee. It would be a relatively modest thing so you can do the prescreening and get those people going.

There were 4.2 million trucks that came across the Laredo border in 1999, but it was 88,000 trucks that actually did those movements. And this is the key. I would push those one-stop concepts, one stop like the Brits and French do at the base of the Chunnel. One stop is Americans and Mexicans working alongside, away from the bridge where there is plenty of real estate, and then you could have long-haul truck meet long-haul truck. Now, you have taken thousands of trucks out of the mix and the result is you have a more efficient border. You have a more policeable system to operate from, less environmental congestion, and so forth.

That is the kind of thinking that we need to push, and we can do it in a pilot kind of way virtually tomorrow. Use the Columbia Bridge or use a border-crossing in Arizona. I haven't had the privilege yet to get to Nogales and across your entry, sir, but that is the kind of thing I think we need to move on.

Chairman KYL. Thank you.

Mr. Stana, I haven't given you any opportunity. Please take an opportunity and then I will call on Senator Craig.

Mr. STANA. OK, let me be brief, then. I agree with what has been said by the other panel members here. I would like to take it down to the front line, the few thousand men and women who really form our line of scrimmage at the border, and what they need to do to assess the risk of the individual that they have 15 to 20 seconds, on average, to evaluate.

I agree that they do a very good job, particularly those that are well-trained, but we are talking about our national security hinging on somebody's gut feel, no matter how well-intentioned they are. So they do need the tools to help them do it better.

If you are talking about short run, I would concentrate initially on getting the intelligence systems in shape so there is not a lot of noise in the system, get the intelligence shops at the ports to filter out the noise that happened downstream, northern border, so that they are not burdened, frankly, with understanding and absorbing intelligence that doesn't pertain to them.

I would focus on the IT systems so that they don't have to log on and off six different times, and they might only go to five because they don't have the time. I would also concentrate on the procedures that would have them check more than just the license plate of a vehicle, since most of the traffic is vehicular, and get to the individual driver and the passengers to assess risk more on a random basis, not only on a gut feel basis.

Chairman KYL. Thank you very much.

Senator Craig?

Senator CRAIG. Probably only a comment, and I thank all of you for your testimony and your insight.

Mr. Flynn, I think you have said it well and said it right. Historically, we were an east-west-moving people until NAFTA came along, and then we decided we would go north-south. Clearly, the greatest growth in commerce and activity over the next couple of decades could well be the north-south traffic.

The greater growth will probably be in the U.S.-Mexican relationship, but the growth with Canada will be continuous and progressive. There is just no question about that, and whatever we do there we have got to do it right and we have got to do it with that eye for growth and the ability to handle large flows because large flows will also attract, as you have suggested, the individual who might try to access by acting as if he or she were a part of that. I thank you for that.

We are seeing that in my State now. The traffic out of Canada into the United States through Idaho nearly doubles every year, and it has since NAFTA—tremendous traffic. We can see it by the forcing of us to improve our roads and widen them. But once across that border and into the culture, into the economy, it is a different story.

Clearly, the ability to do as you last suggested, to prototype some things, to see how we can handle volumes, my guess is is going to be tremendously important because the lines entering Arizona, the lines entering Texas are phenomenal and they will stifle commerce. And it shouldn't have to happen if we can go it smartly.

Any additional reactions to that comment, I would welcome them, but it is more of a comment. I think some of us realize it. I don't think our country yet realizes that all of a sudden it started looking north and south a good deal more than it is looking east and west. The east and west traffic is commerce that will continue and will grow, but the greater growth will probably be north-south.

Mr. FLYNN. Thank you for that, Senator. The only thing I might say real briefly is if there is anything I learned from a 2-year project of marching along both the northern border and the southern border, it is there is no one-size-fits-all with regard to our borders. So part of the value of this prototyping is learning the unique challenges and the strengths and opportunities that each of our jurisdictions pose.

Another critical point I want to come back to is what Ms. Kingsbury has said about the value of international cooperation and private sector cooperation. There will never be enough eyes and ears. So on the intelligence function, it is going to be coming from sharing with our allies the forward information, the trade partners, and also getting the private sector willing to share when they see things wrong.

Again, if we do security measures that undermine that spirit of cooperation—the old axiom in the security business is if you look at everything, you see nothing. So if they find themselves robbed of intelligence with just volumes, it is a needle-in-a-haystack exercise.

Thank you, sir.

Chairman KYL. Thank you. Let me just ask one last very specific question and make one last point.

Mr. Stana, do you happen to know the status of the implementation of the reader programs under the laser visa program with Mexico, or should I just get an answer to that for the record?

Mr. STANA. I believe they have demonstration projects at about a half a dozen ports and 250-or-so individuals who have been caught. I don't know when the full fielding is expected to happen.

Chairman KYL. What we need to figure out is what, if any, additional money we need to put toward that, and therefore how quickly that might get done. To the extent you could help us with that, I would appreciate that.

Mr. STANA. Perhaps we can pursue that later.

Chairman KYL. Let me just make a general comment. Just because of the strictures of time here, we are going to move on, but I think that this is a very, very important panel because it really sets up the dilemma well.

What Mr. Flynn bringing his expertise here has pointed out I don't think any of us can argue with. The question is how we get it done and committing ourselves to apply the resources that you quite properly indicate we are going to have to apply if we are really serious about this.

The $5 billion that we spend to protect the military bases, for example—obviously, we are protecting a lot of people there, too, and there are some potential threats out there for that. But that is something we have learned to do well. We know we need to protect the bases. We have learned how to do it and we are willing to spend the resources for it. This new problem, however, is not something we have gotten used to, and we haven't gotten used to spending the kind of resources that we are going to have to.

I would ask Ms. Kingsbury and the folks at GAO to help us out by not—and I am not suggesting this has been done, but what we need to do is not just focus on the dollars and cents, but accept the public policy commitment to provide as much security as we possibly can, as quickly as we can, and evaluate programs in that context.

It is easy for us to sit back and make it perfect 30 years from now after the horse is long gone from the barn. Your point is, unless we do a good job here, we could waste an awful lot of money and we don't have the money to waste on it. So your point is very well taken, but we are going to need to do a lot more, a lot more quickly, than we would ordinarily be used to doing, and we need to find the fiscal ways of doing that in a responsible way.

I think that is the challenge before us, and maybe in another year or so we can get back with all of you and see where we are at that point, having taken advantage of your expertise.

I want to thank all of you for being here. Again, as with the first panel, we will leave the record open for any further questions for the record for all of you. Thank you very, very much.

With that, Senator Craig, unless you have anything else, this hearing will be adjourned.

[Whereupon, at 12:19 p.m., the Subcommittees were adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

"The Role of Border Technology in Advancing Homeland Security"

Written Testimony before

a joint hearing of the

U.S. Senate Judiciary Subcommittee on
Technology, Terrorism, and Government Information
and
the U.S. Senate Judiciary Subcommittee on Immigration

on
"Border Technology: Keeping Terrorists Out of the United States – 2003"

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies and
Director, Council on Foreign Relations Independent Task Force
on Homeland Security Imperatives

Room 226
Dirksen Senate Office Building
Washington, D.C.

10:00 a.m.
March 12, 2003

Chairman Kyl, Senator Feinstein, Senator Kennedy and distinguished members of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information and Subcommittee on Immigration. I am the Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations where I recently directed the Independent Task Force on Homeland Security, co-chaired by former Senators Warren Rudman and Gary Hart. In June 2002, I retired as a Commander in the U.S. Coast Guard after 20 years of active duty service. I am honored to be appearing before you this morning on the issue of Border Controls, Technology, and Terrorism.

We find ourselves in paradoxical times. On the one hand, our prosperity and that of our neighbors and international trade partners depends on an open global system that facilitates the free movement of people and goods. On the other, appropriate concern about our ongoing exposure to catastrophic terrorist attacks have fixated Washington's attention on the nation's borders. Consequently, there is a potential train wreck in the making. Moving in one direction are those who have been keen to make national borders as porous as possible so as to spawn greater economic integration. From the other are officials charged with the new homeland security mandate who look to the border to hold back would-be terrorists, contraband, criminals, and illegal migrants.

Now that September 11 attacks have let the catastrophic terrorist genie out of the bottle, the United States is rightly concerned about its security at home. Just this past November, I was privileged to testify before this subcommittee with former Senator Warren Rudman on our homeland security task force report. In that report we concluded that: "America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil. In all likelihood, the next attack will result in even greater casualties and widespread disruption to American lives and the economy. The need for immediate action is made more urgent by the prospect of the United States going to war with Iraq and the possibility that Saddam Hussein might threaten the use of weapons of mass destruction (WMD) in America." In my view, that chilling finding holds true today.

Yet, however compelling the homeland security imperative may be, it should not mean a derailment of the continental engine of free trade and travel. U.S. prosperity—and much of its power—relies on its ready access to North American and global networks of transport, energy, information, finance, and labor. It is self-defeating for the United States to embrace security measures that end up isolating it from those networks. In addition, there is little value to focusing singularly on bolstering the defenses of only those parts of those networks that lie within on at the borders of U.S. jurisdiction. Such an approach is much like building a firewall only around the computer server physically nearest to a network security manager, while leaving the remaining more remote servers unprotected.

Further, the experience over the past decade of stepped-up enforcement along the Mexican border suggests that U.S. efforts aimed at hardening its borders can have the unintended consequence of creating precisely the kind of an environment that is conducive to terrorists and criminals. On the face of it, an emphasis on tighter border controls appears logical. Stopping threats at the frontier is better than trying to cope with them once inside the

country. Customs inspectors and immigration officials also have the strongest legal authority for inspecting and searching people and goods. But, draconian measures to police the border invariably provide incentives for informal arrangements and criminal conspiracies to overcome cross-border barriers to commerce and labor movements. In addition, unilateral measures pursued on one side of the border create political impediments for enforcement cooperation on the other. The result is that the border region becomes more chaotic which makes it ideal for exploitation by criminals and terrorists.

The alternative is to look beyond national borders as a line of defense. Terrorists and the tools of terrorism do not spring up at the border. Instead, they generally arrive via hemispheric and international trade and travel networks. Advancing a continental approach to deterring, detecting, and intercepting illicit actors seeking to exploit those networks would accomplish two things. First, it would provide some strategic depth for responding to a threat before it arrived at a critical and congested border crossing. Second, it would allow the ability to segment risk so that the cross-border movements of people and cargo deemed to present a low-risk could be facilitated. Then limited enforcement resources could be targeted more effectively at those that present a high risk.

Based on a two-year project that I directed from 1999-2001 that involved field research all along the U.S.-Canada and U.S.-Mexican border, I am convinced that the 21st century imperatives that fuel both the incentives for advancing hemisphere economic integration and satisfying the new homeland security mandate do not inevitably involve trade-offs. On the contrary, the shared risks of loss of life and massive economic disruption presented by the catastrophic terrorist threat should provide the basis for trilateral cooperation that can remove many longstanding barriers to continental commerce precisely because those barriers themselves can elevate security risks. For example, the longstanding neglect of the border in terms of limited infrastructure investment and tepid efforts at customs and immigration modernization and harmonization made no sense in purely economic terms. But the resultant inefficiencies that carry substantial commercial costs also create opportunities that thugs and terrorists can exploit. Thus, there is a national security rationale to redress those inefficiencies. The agendas for both promoting security and greater continental commerce can be and must be mutual reinforcing.

That brings me to the issue of border technology which is the basis of the hearing today. Let me begin by citing a caveat contained in our "Hart-Rudman" Task Force report: "*Proceed with caution when embracing technological security 'fixes':* Technology can often serve as an enabler, but it must belong to a layered and dynamic system of defense that incorporates the contribution of human intuition and judgment. Any proposed technological "solution" must be evaluated against the costs and consequences if it should be compromised. In the end, security is not just about protecting American lives. It is also about sustaining systems that support our way of life in the face of designs to exploit or target those systems. This means that the security protocol must be able to manage any suspected or real terrorist breach without imposing costs so high as to compromise the very network it is designed to secure. Ultimately, the end game must be to continue to live and prosper as an open, globally engaged society, not to become a nation trapped behind the modern versions of moats and castles."

But the complexity of the border control agenda highlights the difficulty of placing excessive reliance on border technology to keep terrorists at bay, especially at the nation's border crossing and maritime ports of entry. Substantial investments in technologies such as (1) deploying non-intrusive inspection equipment and radiation detection devices; (2) using transponders and proximity cards in programs such as SENTRI, and NEXUS, and (3) incorporating biometric devises into identify coduments as a part of the Exit-Entry program, will be helpful only if pursued as a part of a comprehensive approach that is mindful of four facts of border control life:

First, ports of entry cannot be separated from the international transport system to which they belong. Border crossings and seaports are for all practical purposes, simply nodes in an international network that moves people and cargo. Therefore, border controls must be pursued as a subset of a broader commitment to transportation and cargo security. In other words, efforts to improve security at the border require that parallel security efforts be undertaken in the rest of the transportation and logistics network. If security improvements are limited to the border, the result will be to generate the "balloon effect"; i.e., pushing illicit activities horizontally or vertically into the transportation and logistics systems where there is a reduced chance of detection or interdiction.

Take the case of the Loredo, Texas—the busiest commercial border crossing on the U.S.-Mexican border. In 1999, 2.8 million trucks crossed the border there, up from 1.3 million in 1993. Many of these trucks operating at the border are old and poorly maintained and owned by small mom-and-pop trucking companies. The drivers of these short-haul rigs tend to be younger, less skilled, and are paid only nominal wages—as little as $7 to $10 per trip—since waiting hours at a border crossing in order to make a 20-mile round trip, with an empty trailer on the return, is not a lucrative business. Not surprising the turnover-rate among these drivers is also extremely high.

The prevalence of a fragmented, semi-anarchical trucking sector to service the border is itself a direct consequence of the delays associated with crossing the border. Long-haul truck companies like Yellow and Roadway Express simply cannot afford to run their state-of-the-art rigs near the border. As a consequence, trailers are usually offloaded at depots near the border. In the case of south-bound traffic, a short-haul truck is then contracted to move the freight to a customs broker who will then order another short-haul truck to transport the freight to another depot across the border. A long-haul truck will then pick up the load and carry it into the interior. All this conspires to create almost ideal conditions for organized criminal networks to exploit.

Now if there were no real delays at the border, state-of-the-art long-haul trucks with experienced drivers that are easier to regulate and monitor would be responsible for these cross-border flows. There would be less congestion at the border so the border would become easier to police. In other words, the more efficient the border crossing—which is a an outcome of their being adequate infrastructure on both sides of the border—access roads, bridges, state-of-the-art inspection facilities, and the more efficient the inspection processes,

the more secure the border will become. Alternatively, pursuing improvements in only one of these areas without parallel efforts in the other will have suboptimal—maybe even counterproductive outcomes.

Second, since the bridges and seaports that link the United States to its neighbors and the world are among America's most critical infrastructure, they should not be viewed as a primary line of defense in an effort to protect the U.S. homeland. The last place we should be looking to intercept dangerous cargo on a truck or bridge is in a busy, congested, and commercially vital seaport or at the base of a bridge. For instance, the Ambassador Bridge that links Detroit, Michigan to Windsor Ontario is the lifeline of the U.S. automotive industry. This bridge alone carries more trade into the United States than all the trade that arrives by sea from China. Thus, initiatives such as the Container Security Initiative and the next generation of the Computer Assisted Passenger Prescreening System (CAPPS-II) that push the border inspection out towards the port of origin should be pursued with a greater sense of urgency.

Third, inspections processes at a port of entry must be an exercise in *risk management*. There will never be enough inspection resources and it would prove self-defeating to subject every person, conveyance, and cargo to the same inspection regime. An age-old axiom in the security field is that if "you have to look at everything, you will see nothing." At its heart, risk management requires quickly clearing the inspection queues of traffic that is deem low risk so that limited enforcement resources can focus on that which is deemed to be high risk. But, ultimately determinations of low or high risk are only as good as the integrity of the information, the targeting algorithms and intelligence that underpin them.

The assessment of a person as low or high risk is best done when an application is first made for a visa or passport. A good assessment of the baseline documents that prove an applicant's identify can be supported by technology, but the quality of the interview conducted by a U.S. consulate officer is likely to be more an issue of the time that officer has available to meet with the applicant plus his or her training and experience. An investment in this human resource intensive part of the application process deserves equal billing with vast expenditures on new technologies such as biometrics.

The assessment of the relative risk of an inbound conveyance and cargo is dependent upon verifying the integrity of that conveyance from its point of origin to its arrival at the port of entry. It does not matter that a truck or cargo container originated from a legitimate company or that its paperwork is in order if there is no way to verify that the vehicle and shipment were not compromised once it left the loading facility. Technologies that can track the vehicle and ensure that neither it nor the freight is carries has been tampered with will be essential to confirming that these shipments are indeed low risk. Thus, initiatives such as "Operation Safe Commerce" that look to embed technologies into the transportation and logistics system at large should be pursued with the same vigor as efforts to advance inspection technologies at the border crossings themselves.

A determination that a person, conveyance, or freight shipment deserves to be considered as high risk is dependent on good intelligence. Good intelligence, in turn, is heavily dependent upon close coordination and cooperation with the stakeholders who are vested in legitimate trade and travel. Incentives are key—there must be rewards for good behavior. Accordingly, technology or any security measure which is indiscriminately applied across a particular sector or that singles out a particular population group will almost certainly backfire by undermining the basis for information sharing and cooperation. For instance, a rush to deploy the Exit-Entry system at our borders is likely to produce considerable disruption and angst among the overwhelming majority of the people who are perfectly legitimate. Their frustration will translate into less cooperation, making the exercise of policing them more daunting for border inspection officials. The better approach is to draw frequent travelers and shippers into programs like NEXUS, SENTRI, and the INSPASS that offer facilitation across the border as a reward for undergoing vigorous pre-screening.

A final border control fact of life is that people matter. Any conversation about investing in new technologies at the border must not be divorced from a concurrent discussion about investing in the quantity and quality of the people who work at the border. Identifying and intercepting criminal or terrorist activity at the border places a premium on the people who populate the front-lines agencies that are tasked to do this. We must be candid in acknowledging that these agencies have been sorely neglected in recent years. This neglect has translated into limited personnel training and advancement opportunities. Most of the inspectors who work along the border have traditionally relied heavily on "on-the-job-training" and promotions from within on the basis of time-in-grade. This approach is clearly out of step with the much more complicated and technology-intensive border management environment of today and tomorrow. Today's inspectors and managers must have the same kind of formal training and education opportunities that we provide our military services. Failing to do that means that large investments in border technologies will end up being essentially white elephants.

Conclusion

Ultimately a focus on border technology in isolation from a broader national and trilateral conversation that reexamines the very ends and means of border control is self defeating. Accordingly, we should not fall into the trap of simply pursuing technologies that support traditional border management practices, particularly is those practices end up introducing delays at our already congested border crossings.

Instead the post-9/11 focus on our borders should be seen as an opportunity to reinvent our borders with our neighbors. Such an exercise is long overdue. The evolution of commercial and social patterns of interaction throughout North America that have made our continental relationships more dynamic, organic, and integrated should have long ago raised the issue of border management to the top of the national agenda. Our aim must be to invest in the kind of "smart border" initiatives being embraced on the northern border, not to try and replicate the inherently flawed and self-defeating approach that we pursued along the southwest border in the 1990s.

The outline for transformed border management is clear. It requires a risk management approach to policing cross-border flows which includes the close collaboration of the major beneficiaries of an increasingly open North American continent—the United States' neighbors to the North and the South, and the private sector. The stakes of getting this right are also clear. Transforming how the border is managed is an essential step towards assuring the long-term sustainability of hemispheric economic integration within the context of the transformed security environment of the post-9-11 world.

Thank you and I look forward to responding to your questions.

Statement of
The Honorable Orrin Hatch
United States Senator
Utah

March 12, 2003

PRINTABLE VERSION

I want to thank the Chairmen and Ranking Democrat Members of both of the Subcommittees convened here today for holding this hearing. I particularly want to thank Senators Kyl and Feinstein for their long and tireless efforts in the Border Security and Technology areas. I also want to thank Senator Chambliss, our incoming Chairman of the Senate Judiciary Subcommittee on Border Security, Immigration, and Citizenship, for his subcommittee's participation in this hearing. We can be assured that he will provide effective leadership and diligent service to this subcommittee.

The issues that we will discuss today are of the utmost importance. We accomplished several good legislative efforts in the 107th Congress to keep our country safe from terrorists. One of these was the Enhanced Border Security and Visa Entry Reform Act, of which I was an original cosponsor. The legislation provided many crucial tools, now, it is crucial that Congress and the Department of Homeland Security work together to evaluate what progress has been made and to ensure that the measures set out in the Border Security Act are appropriately implemented.

Securing our nation's air, land, and sea borders is a critical yet difficult task. Each year, more than 500 million people cross the borders into the United States, some 330 million of whom are non-citizens. The lessons of September 11 teach us that those who would come here to do harm will be innovative in their attempts to circumvent our immigration laws. It is essential that our country remain vigilant against terrorists, and the Department of Homeland Security must be prepared to intercept terrorists before they enter our country.

At the same time, we must remember that our nation was founded by those who immigrated to our shores. Historically, immigrants have richly contributed to our country's culture, learning, and progress. It was never the intent of the Enhanced Border Security Act to stymie lawful immigration and it would be a real setback if we applied it in such a perverse manner. America always gains strength by welcoming a diversity of peoples and ideas. We need to ensure that our immigration laws continue to provide the promise of America to all those who lawfully seek to become Americans.

In passing the Enhanced Border Security and Visa Entry Reform Act, Congress attempted to remove the barriers that had, in the past, inhibited our security by forbidding comprehensive data sharing between various governmental agencies.

We also provided for the use of biometric technology to enhance our ability to confirm the identity of those desiring admission into our country. These are just some of the measures included in the bill to enable the Department of Homeland Security to promptly process the requests of those seeking lawful entry into our country and, at the same time, deny entry to terrorists and criminals. It is important for us to understand how the Department of Homeland Security plans to implement these measures. It is also important for Congress to learn what other areas exist that might require further action.

With this in mind, I want to thank the witnesses for appearing today and look forward to hearing their testimony into this important area of national security.

###

- TOP OF THIS PAGE
- RETURN TO HOME

PRINTER FRIENDLY VERSION

STATEMENT

OF

THE HONORABLE ASA HUTCHINSON
UNDER SECRETARY
FOR
BORDER AND TRANSPORTATION SECURITY
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SENATE SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY
AND THE
SENATE SUBCOMMITTEE ON BORDER SECURITY, IMMIGRATION, AND CITIZENSHIP
COMMITTEE ON THE JUDICIARY

"BORDER TECHNOLOGY: KEEPING TERRORISTS OUT OF THE UNITED STATES"

MARCH 12, 2003, 10:00 AM

226 DIRKSEN SENATE OFFICE BUILDING

MISTER CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE, thank you for providing a forum to discuss using technology to protect our borders and fight terrorism. This is my first opportunity to appear before the Congress as our nation's first Under Secretary for Border and Transportation Security, and I am pleased to discuss with you the critical steps we are taking to improve our ability to determine which people and what materials are entering our country.

As you are aware, the United States Customs Service and Immigration and Naturalization Service – agencies with primary jurisdiction over the laws that govern the entry and exit of people and goods into and from the United States – were transferred to the Department of Homeland Security on March 1, and were re-grouped among two newly-formed Bureaus within the Border and Transportation Security Directorate. Immigration and Customs inspections and border enforcement functions have been placed in the new Bureau of Customs and Border Protection, or BCBP, and Immigration and Customs investigations and interior enforcement functions were placed in the new Bureau of Immigration and Customs Enforcement, or BICE. We believe this reconfiguration will enable us to streamline the activities of the Inspectors, Border Patrol Agents and Investigators in the two bureaus and reap benefits in enhanced screening of people and goods, and enforcement of our immigration and customs laws.

I mention this because prior to March 1, at the direction and with the support of Congress, the INS and Customs Service were working to develop and deploy technologies that would enhance their ability to perform their missions. Now that they are part of the Department of Homeland Security, they will have the benefit of being able to rely on expertise and resources vested within the Department's Directorates of Science and Technology (S&T), and Information Analysis and Infrastructure Protection (IAIP), to

enhance the systems already in place, and develop and deploy new technology and information sharing tools to aid in the completion of their missions. The President and Secretary Ridge have identified a very qualified candidate, Dr. Charles McQueary, to lead the S&T Directorate, and are working diligently to identify the right candidate to lead the IAIP Directorate. I look forward to working with them once they are confirmed.

Let me quickly lay out how I will proceed with my testimony this morning. I will first address our efforts to use technology to ensure we know the "who" and "how long" of people entering the U.S., and highlight the status of three very important tools in this arena: the Entry-Exit System (EES), the National Security Entry Exit Registration System (NSEERS), and Biometric Verification System (BVS). Next, I will cover briefly the status of our efforts to ensure we know what is entering the U.S., including Non-Intrusive Inspection Devices, Advance Information Systems, and Information Sharing systems. Finally, I will discuss some of the needs we have identified and will work with the S&T and IAIP Directorates to meet.

Knowing who has entered and who has departed our country in real time is an important element in enforcing our laws. Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), requires the development of an automated entry and exit control system to collect records of arrival and departure from every alien entering and leaving the United States. The Data Management Improvement Act, passed in 2000, requires the INS to develop a fully automated integrated entry-exit data collection system (EES) by the end of 2005. The legislation also requires a public and private sector task force to make recommendations on development of the system and methods to ensure that trade and tourism is not harmed. The Enhanced Border Security and Visa Entry Reform

Act, as well as the USA PATRIOT Act, added the complexities of biometrics to the implementation of the EES – it is an addition which will bolster our security.

The Departments of Justice and State have reported to Congress on the issues to be considered in adding biometrics to the entry exit process, as required by the USA PATRIOT Act and the Enhanced Border Security Act and Visa Entry Reform Act. These reports outline many issues that will need to be considered in undertaking such an endeavor. A November 2002 GAO report entitled "Using Biometrics for Border Security" cited privacy rights, international relations, feasibility, cost and effectiveness as further considerations before biometrics can be implemented effectively at the border. In March 2002, an Entry Exit Program Team comprised of all appropriate Department and Agency representatives was chartered to improve the processes, policies, workforce, and systems utilized to manage the pre-entry, entry, stay, and exit of international travelers through established air, land, and sea ports-of-entry (POE's).

The EES will be able to strike the appropriate balance between enhanced border security and the facilitation of legitimate international trade and travel. This will integrate real-time, transaction-level biometric and watch list data, improving systems interoperability, and enhancing interfaces with related government partners. The system will include a number of software and hardware enhancements to further strengthen border management processes.

Specifically, the Entry Exit System will:

- Provide improved access to data relevant to determining visa eligibility;
- Improve detection of fraudulent documentation through automated capture and processing of data contained in travel documents;

- Capture and process biometric data in order to improve precision of traveler identification, and;
- Improve data integration and sharing among agencies in terms of accuracy, consistency, completeness, and timeliness.

We share Congress' desire to field the Entry Exit System capability as soon as possible while ensuring we have a well-defined project plan. We look forward to working with Congress toward that end over the next two months. The Directorates of Science and Technology and Information Analysis and Infrastructure Protection will be actively involved as we put this system in place.

As we were working on the comprehensive Entry Exit System, the events of September 11th propelled the Administration into launching the National Security Entry Exit System. This system, otherwise known as "NSEERS," is a response to strategic intelligence assessments that warranted the rapid development of a more rigorous process than had been employed in the Special Registration Program since 1995.

The goal of NSEERS is to secure our borders, by intercepting terrorists and criminals at Ports of Entry, identifying aliens who deviate from their stated purposes once they enter the country, and identifying instantly aliens who overstay their visas. NSEERS promotes several important national security objectives:

- The NSEERS program will allow the United States to screen aliens effectively by matching individual biometric data against a database of known terrorists and criminals during the initial and continuing registration processes.
- The NSEERS module permits computerized review of warehoused data, allowing it to be utilized as new information relating to terrorist activities is developed.

- NSEERS enables us to determine instantly whether an alien has overstayed his or her visa.
- NSEERS enables us to verify that an alien is acting according to stated plans while in the United States, and ensure that he or she is not violating our immigration laws

The NSEERS process has operated since September 11, 2002, with registration of 88,989 enrollees from 149 countries as of March 4, 2003. We have learned and applied lessons with the intent to minimize delays and inconvenience to registrants, while balancing the security objectives of the program.

Non-immigrant aliens entering, present in, and departing the United States, who fall under the NSEERS program, may interact with BTS through four distinct processes:

- Point of Entry (POE) registration
- Domestic or Call-In Registration
- Continuing Registration Requirements
- Departure Verification

With Respect to POE registration, NSEERS requires certain non-immigrant aliens from designated countries to be fingerprinted, photographed, and interviewed at the POEs at the same time they apply for admission to the United States. In addition, other aliens who are identified from intelligence sources or who match certain pre-existing criteria determined by the Attorney General or the Secretary of the State may be enrolled in NSEERS at the POE.

Call-in registration relates to the class of aliens known as "Domestic Registrants," who are subject to special registration. Domestic Registrants are certain nonimmigrant aliens who were admitted to the United States prior to the inception of the new border registration program, have remained in the United States, and who, when designated by the Attorney General, must report to an identified Interviewing Office for Special Registration to be

registered. The Attorney General has designated individuals from 25 different countries as subject to domestic registration requirements. The purpose is to gather the same information that may have been collected at the POEs had those aliens arrived after the effective date for NSEERS.

Aliens subject both to POE registration and Domestic Registration must also appear to fulfill their continuing registration requirements, based upon length of stay in the United States. Finally, aliens registered either through the POE or the Domestic Registration must complete a departure check when they leave the United States.

As of March 4, 2003, 88,989 individuals have been registered in NSEERS, a number divided evenly between POE registrations and Domestic registrations. The total number of registrations, including POE registrations, the follow-up or continuing registrations of aliens registered at a POE, and domestic registrations, is 133,017. The NSEERS program has led to the identification and apprehension of 8 suspected terrorists, and the initiation of 40 investigations of registrants suspected of terrorist activity. We have apprehended or denied admission to more than 555 aliens with warrants or other criminal violations.

Likewise, through the domestic registration program, as of March 4th, 4,825 individuals in violation of our immigration laws are awaiting removal from the United States. Since its implementation, fifteen aliens have been arrested for explicit violation of their status related to NSEERS requirements, after they failed to appear for their continuing registration interviews. NSEERS is also providing DHS with information to target enforcement activities and coordinate with other law enforcement components to prevent those aliens seeking to do harm to the United States from remaining in this country for extended periods of time. Our NSEERS experience reflects the importance of having a comprehensive,

requirements-based technology solution to ensure compliance with the immigration laws for the millions of visitors to this country every year.

I will now briefly discuss the Biometric Verification System. Since 1998, the Department of State and the former INS have produced over six million Border Crossing Cards that include biometrics, based on a mandate included in Section 104 of IIRAIRA. The Border Crossing Card has two fingerprints and a digital photograph imbedded in an optical stripe on the back of the card. With the passing of the fiscal year 2002 Counter Terrorism Supplemental Appropriations Act, the INS received 10.6 million dollars to purchase readers that can decode those imbedded biometrics for comparison with the person presenting the card. A recent pilot program which ran for three weeks at six locations shows the value of a Biometrics Verification System. More than 250 imposters were detected.

Two other tools we are developing and using will ensure the integrity of the immigration and visa issuance processes -- the SENTRI and NEXUS programs. These programs allow pre-screened, low-risk travelers to be processed in an expedited manner via a dedicated lane at our land borders with minimal or no delay, thereby enabling BCBP staff to focus their attention on those crossing our borders who are relatively unknown. SENTRI is deployed at 3 southwest border crossings: El Paso, San Ysidro and Otay Mesa. The NEXUS program is deployed at 6 northern border crossings: Pacific Highway, Peace Arch Bridge, Port Roberts, Port Huron, Detroit and Buffalo

We must also ensure the integrity of our borders between ports of entry, including remote areas of the Northern and Southern Borders. Today we have over 10,000 Border Patrol Agents, now a part of BCBP, deployed at our nation's borders. We will deploy an additional 285 Agents with funds provided by the Congress in the FY 2003 Appropriations Bill. In addition, the Border Patrol is employing a number of force-multiplying

technologies, including aerial surveillance equipment, infrared surveillance scopes and other sensor technology. We will deploy similar technologies for use on the Northern Border, and work closely with the Science and Technology Directorate to identify and deploy other technologies to augment those capabilities and better secure those borders. We will also continue to work with the Department of State and other agencies on cooperative "smart border" international programs implementing the 30-point U.S.-Canada Smart Border Action Plan and 22-point U.S.-Mexico Border Partnership.

I will now outline the technology we are using to inspect commercial goods to detect potentially dangerous or threatening materials coming across our borders. The BCBP has deployed, and must continue to develop the technology necessary to inspect arriving and departing conveyances and cargo at our ports of entry rapidly and comprehensively to prevent the smuggling of weapons, narcotics and other contraband. This technology permits enhanced security without unduly impeding the flow of legitimate commercial traffic. We are:

- Expanding deployment of non-intrusive inspection technology
- Enhancing our advance targeting capability, and
- Modernizing our nearly 20-year old legacy trade system.

The BCBP has deployed 112 large-scale Non-intrusive inspection (NII) systems at our Nation's air, sea and land border ports of entry to further enhance our non-intrusive inspection capability while facilitating the flow of legitimate trade and traffic. Additional systems have been ordered.

The BCBP is also testing and deploying other technologies that will assist inspectors to conduct high-confidence, non-intrusive inspections quickly and efficiently. These systems include portal monitors and isotope identifier devices that are capable of detecting and

identifying radiation. Over 6,000 personal, pager-sized radiation detectors have already been deployed to our ports of entry to allow inspectors to monitor their vicinity for radioactive sources.

We are employing and refining our risk-based targeting systems, to incorporate intelligence information and enable us to target unusual, suspect or high-risk inbound and outbound shipments for intensive examinations. We are also working with the Department of Transportation to test different tracing and tracking technologies that enable commercial carriers to maintain contact with their fleets and cargo.

In accordance with the Trade Act of 2002, BCBP is working to promulgate regulations by October 2003, which will mandate the advance electronic information for all modes of transportation, both inbound and outbound. The BCBP, formerly U.S. Customs, already issued regulations requiring advance manifest information – 24 hours before lading of oceangoing cargo containers bound for U.S. ports. These regulations will allow BCBP sufficient time to determine whether a particular shipment is high risk or warrants closer scrutiny. In fact, access to advance information on all cargo shipments expands on our successful efforts to require airlines to submit passenger manifests to our Advanced Passenger Information System (APIS) prior to departure.

The Automated Commercial Environment, or ACE, BCBP's first major modernization project, will improve both the collection and sorting of trade data to expedite trade across our borders and enhance our targeting of high risk cargo. The new system will help overcome information stovepipes and enhance border security by providing interagency information sharing, and real-time, cross-government access to more accurate information. Shipment information will be analyzed prior to arrival, allowing advanced inter-agency

assessment of risks and threats. Results will determine if, upon arrival, a shipment is to be examined or cleared for release.

The trade community currently files its data with numerous government agencies to comply with approximately 400 laws and regulations. The BCBP is working with these other government agencies to coordinate efforts and leverage information and resources through ACE.

The International Trade Data System (ITDS), initiated as a project to streamline government and provide a single interface for the submission of import and export data to the U.S. Government, will be a fully integrated part of ACE. We continue to work closely with other government agencies and the trade community, to ensure requirements are incorporated into, and are compatible with, ACE.

Technology is a critical tool that enables the hard-working men and women of the Department of Homeland Security to properly balance our national security imperative with the free flow of goods and peoples across our Nation's borders. We look forward to working together with the Congress, within the Executive Branch, and with our state, local, and private partners to provide the American people with the level of security that they deserve.

Thank you for this opportunity to appear before your Subcommittees today. I look forward to your questions.

United States General Accounting Office

GAO

Testimony

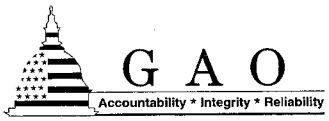
Before the Subcommittee on Terrorism, Technology, and Homeland Security and Subcommittee on Border Security, Immigration, and Citizenship, Committee on the Judiciary, United States Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday March 12, 2003

BORDER SECURITY

Challenges in Implementing Border Technology

Statement of Nancy Kingsbury, Managing Director
Applied Research and Methods



GAO-03-546T

Mr. Chairmen and Members of the Subcommittees:

I appreciate the opportunity to participate in today's hearing on border technology. The Department of Homeland Security (DHS) faces enormous challenges to protect the nation from terrorism.[1] One of the primary missions of the new department focuses on border control – preventing the illegal entry of people and goods into the United States. Part of this mission is controlling the passage of travelers through official ports of entry into the United States. Facilitating the flow of people while preventing the illegal entry of travelers requires an effective and efficient process that authenticates a traveler's identity. Generally, identifying travelers at the ports of entry is performed by inspecting their travel documents, such as passports and visas, and asking them questions. Technologies called biometrics can automate the identification of individual travelers by one or more of their distinct physiological characteristics. Biometrics have been suggested as a way of improving the nation's ability to determine whether travelers are admissible to the United States. Today, I will discuss the issues and challenges associated with using biometrics in border control systems and the significant management challenges we identified during our ongoing work at land ports of entry.

My testimony today is based on a body of work we completed last year examining the use of biometrics for border control and on preliminary observations related to our ongoing work examining the inspection of travelers at land border ports of entry. In our report on the use of biometrics, we discussed the current maturity of several biometric technologies, the possible implementation of these technologies in current border control processes, and the policy implications and key considerations for using these technologies.[2] We are also in the process of reviewing immigration inspections at land border ports of entry, where our work has included examining the integrity of the inspections process, programs to segregate low-risk travelers, the technology and equipment

[1] We recently designated the implementation and transformation of DHS as a high-risk area due in part to the inherited operational and management challenges faced by the department. See U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington D.C.: Jan. 2003).

[2] U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington D.C.: Nov. 15, 2002).

used to conduct inspections, immigration intelligence information, and inspector training issues.

In brief, biometric technologies are available today that can be used for border control. However, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. Before implementing any biometric border control system, a number of other issues would have to be considered, including the system's effect on existing border control procedures and people, the costs and benefits of the system, and the system's effect on privacy, convenience, and the economy. Furthermore, technology is only part of the solution. Effective security requires technology and people to work together to implement policies, processes, and procedures. At land border ports of entry, DHS faces several challenges including ensuring that the inspections process has sufficient integrity to enable inspectors to intercept those who should not enter our country, while still facilitating the entry of lawful travelers; ensuring that inspectors have the necessary technology, equipment, and training to do their job efficiently and effectively; and providing inspectors the access to necessary intelligence information.

Background

The United States essentially relies on a two-step process to prevent inadmissible people from entering the country. The Bureau of Consular Affairs in the State Department is responsible for issuing international travel documents, such as passports to United States citizens and visas to citizens of other countries. On March 1, 2003, the Bureau of Customs and Border Protection in the Department of Homeland Security assumed responsibility for inspecting travelers at and between ports of entry. Inspectors from the Immigration and Naturalization Service (INS), the U.S. Customs Service, and the Animal and Plant Health Inspection Service (APHIS) were brought together in this new bureau.

In fiscal year 2002, there were about 440 million border crossings into the United States at over 300 designated ports of entry (see table 1). Of the more than 358 million border crossers who entered through land ports of entry, almost 50 million entered as pedestrians. The rest entered in more than 131 million vehicles, including cars, trucks, buses, and trains. Further, the State Department processed about 8.4 million nonimmigrant visa applications and issued about 7 million passports.

Table 1: Number of Inspections at U.S. Ports of Entry, Fiscal Year 2002

Type of port	Number of inspections
Sea	12,369,035
Air	69,679,190
Land	358,373,569
Total	**440,421,794**

Source: GAO analysis of INS data.

The term biometrics covers a wide range of technologies that can be used to verify a person's identity by measuring and analyzing his or her physiological characteristics, based on data derived from measuring a part of the body directly. For example, technologies have been developed to measure a person's finger, hand, face, retina, and iris. Biometric systems are essentially pattern recognition systems. They use electronic or optical sensors such as cameras and scanning devices to capture images, recordings, or measurements of a person's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics.

Using biometrics as identifiers for border security purposes appears to be appealing because they can help tightly bind a traveler to his or her identity by using physiological characteristics. Unlike other identification methods, such as identification cards or passwords, biometrics are less easily lost, stolen, or guessed. The binding is dependent on the quality of the identification document presented by the traveler to enroll in the biometric system. If the identification document does not specify the traveler's true identity, the biometric data will be linked to a false identity.

Applying Biometrics to Border Control

In our work last year, we examined several different biometric technologies and found four to be suitable for border control systems: fingerprint recognition, facial recognition, iris recognition, and hand geometry. Other biometric technologies were determined to be impractical in a border control application because of accuracy or user acceptance issues. For example, speaker recognition systems do not perform well in noisy environments and do not appear to be sufficiently distinctive to permit identification of an individual within a large database of identities.

We defined four different scenarios in which biometric technologies could be used to support border control operations. Two scenarios use a biometric watch list to identify travelers who are inadmissible to the United States (1) before issuing travel documents and (2) before travelers

enter the country. The other two scenarios help bind the claimed identity of travelers to their travel documents by incorporating biometrics into (1) U.S. visas or (2) U.S. passports. Linking an individual's identity to a U.S. travel document could help reduce the use of counterfeit documents and imposters' fraudulent use of legitimate documents.

Biometrics have been used in border control environments for several years. For example, the INS Passenger Accelerated Service System (INSPASS), a hand geometry system first installed in 1993, has been used in seven U.S. and two Canadian airports to reduce inspection time for trusted travelers. Since April 1998, border crossing cards, also called laser visas, have been issued to Mexican citizens that include their photograph and prints of the two index fingers.[3] The Automated Biometric Fingerprint Identification System (IDENT) is used by DHS to identify aliens who are repeatedly apprehended trying to enter the United States illegally. IDENT is also being used as a part of the National Security Entry-Exit Registration System (NSEERS) that was implemented last year.[4]

Laws passed in the last 2 years require a more extensive use of biometrics for border control.[5] The Attorney General and the Secretary of State jointly, through the National Institute of Standards and Technology (NIST) are to develop a technology standard, including biometric identifier standards. When developed, this standard is to be used to verify the identity of persons applying for a U.S. visa for the purpose of conducting a background check, confirming identity, and ensuring that a person has not received a visa under a different name. By October 26, 2004, the Departments of State and Justice are to issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. At the same time, Justice is to install at all ports of entry equipment and software that allow the biometric comparison and

[3] Border crossing cards allow Mexican citizens to enter the United States for the purpose of business or pleasure without being issued further documentation and to stay for 72 hours or less within 25 miles of the U.S./Mexican border.

[4] Under NSEERS, certain nonimmigrants, who may pose a national security risk, are being registered, and are fingerprinted and photographed when they arrive in the United States. These nonimmigrants are required to periodically report and update, when changes occur, their registration information, and record their departure from the country.

[5] See the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public Law 107-56, §403(c) and §414, Oct. 26, 2001) and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173, May 14, 2002).

authentication of all U.S. visas and other travel and entry documents issued to aliens and machine-readable passports.

Challenges and Implications to Applying Biometrics at the Border

While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. In addition, before implementing any biometric border control system, a number of other issues would have to be considered including:

- The system's effect on existing border control procedures and people. Technology is only part of an overall security solution and only as effective as the procedures within which it operates.
- The costs and benefits of the system, including secondary costs resulting from changes in processes or personnel to accommodate the biometrics.
- The system's effect on privacy, convenience, and the economy.

Introducing Technology Affects People and Procedures

The successful implementation of any technology depends not only on the performance of the technology but also on the operational processes that employ the technology and the people who execute them. The implementation of biometrics in border security is no exception. Further, the use of technology alone is not a panacea for the border security problem. Instead, biometric technology is just a piece of the overall decision support system that helps determine whether to allow a person into the United States. The first decision is whether to issue travelers a U.S. travel document. The second decision, made at the ports of entry, is whether to admit travelers into the country. Biometrics can play a role in both decisions. Sorting the admissible travelers from the inadmissible ones is currently conducted by using information systems for checking names against watch lists and by using manual human recognition capabilities to see if the photograph on a travel document matches the person who seeks entry to the United States. When enabled with biometrics, automated systems can verify the identity of the traveler and assist inspectors in their decision making.

However, a key factor that must be considered is the performance of the biometric technology. For example, if the biometric technology that is used to perform watch list checks before visas are issued has a high rate of false matches, the visa processing workload could increase at the embassies and consulates. If the same biometric solution were used at the

ports of entry, it could lead to increased delays in the inspection process and an increase in the number of secondary inspections.

Exception processing will also have to be carefully considered. Exceptions would include people who fail to enroll in the biometric visa system or are not correctly matched by it. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole. Failure of equipment must also be considered and planned for. Further, to issue visas with biometrics, an appropriate transition strategy must be devised to simultaneously handle both visas with biometrics and the current visa that could remain valid without biometrics for up to the next 10 years.

Weighing Costs and Benefits

Before any significant project investment is made, the benefit and cost information of the project alternatives should be analyzed and assessed in detail. A clear statement of the high-level system goals should drive the overall concept of a U.S. border control system. System goals address the system's expected outcomes and are usually based on business or public policy needs, which for a border control system could include items such as binding a biometric feature to a person's identity on a travel document, identifying undesirable persons on a watch list, checking for duplicate enrollments in the system, verifying identities at the borders, ensuring the security of the biometric data, and ensuring the adequacy of privacy protections. The benefits gained from a biometric border control system should be based on how well the system achieves the high-level goals.

A concept of operations should be developed that embodies the people, process, and technologies required to achieve the goals. To put together the concept of operations, a number of inputs have to be considered, including legal requirements, existing processes and infrastructure used, and known technology limitations. Performance requirements should also be included in the concept of operations, such as processing times. Business process reengineering, such as new processes to conduct inspections of passengers in vehicles or to maintain a database of biometric data, would also be addressed in the concept of operations.

As we have noted, the desired benefit is the prevention of the entry of travelers who are inadmissible to the United States. More specifically, the use of a biometric watch list can provide an additional check to name-based checks and can help detect travelers who have successfully established separate names and identities and are trying to evade detection. The use of visas with biometrics can help positively identify

travelers as they enter the United States and can limit the use of fraudulent documents, including counterfeit and modified documents, and impostors' use of legitimate documents.

However, the benefits gained by using biometric have several limitations. First, the benefit achieved is directly related to the performance of the biometric technology. The performance of facial, fingerprint, and iris recognition is unknown for systems as large as a biometric visa system that would require storage and comparison against 100 million to 240 million records. The largest facial, fingerprint, and iris recognition systems contain 60 million, 40 million, and 30,000 records, respectively.

The population of the biometric watch list is critical to its effectiveness. Policies and procedures would need to be developed for adding and maintaining records in the watch list database. Key questions that have to be answered include who is added to the watch list, how someone is removed from the watch list, and how errors could be corrected. Successfully identifying people on the biometric watch list is also dependent on the effectiveness of the law enforcement and intelligence communities in identifying individuals who should be placed on the watch list.

Issuing visas with biometrics will only assist in identifying those currently required to obtain visas to enter this country. For example, Canadians, Mexicans with border crossing cards, and foreign nationals participating in the visa waiver program do not have to have a visa to enter the United States. The issuance of visas with biometrics is also dependent on establishing the correct identity during enrollment. This process typically depends on the presentation of identification documents. If the documents do not specify the applicant's true identity, then the travel document will be linked to a false identity.[6]

Further, biometric technology is not a solution to all border security problems. Biometric technology can address only problems associated with identifying travelers at official locations such as embassies and ports of entry. While the technology can help reduce the number of illegal immigrants who cross with fraudulent documents, it cannot help with

[6] We have previously reported on weaknesses in the visa issuing process. See U.S. General Accounting Office, *Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*, GAO-03-132NI (Washington D.C.: Oct. 21, 2002).

illegal immigrants who cross between the ports of entry. INS has previously estimated that up to 60 percent of the 275,000 new illegal immigrants a year do not present themselves at a port of entry to enter the United States. In addition, biometrics cannot help to identify foreign nationals who enter through ports of entry and are properly admitted by an inspector but may overstay their visit.

The costs of any proposed system must be considered. Both initial costs and recurring costs need to be estimated. Initial costs need to account for the engineering efforts to design, develop, test, and implement the system; training of personnel; hardware and software costs; network infrastructure improvements; and additional facilities required to enroll people into the biometric system. Recurring cost elements include program management costs, hardware and software maintenance, hardware replacement costs, training of personnel, additional personnel to enroll or verify the identities of travelers in the biometric system, and possibly the issuance of token cards for the storage of biometrics collected for issuing visas. While specific cost estimates depend on the detailed assumptions made for the concept of operations, the costs are significant.

Effect on Privacy, the Economy, and International Relations

The Privacy Act of 1974 limits federal agencies' collection, use, and disclosure of personal information, such as fingerprints and photographs. Accordingly, the Privacy Act generally covers federal agency use of personal biometric information. However, as a practical matter, the act is likely to have a more limited application for border security. First, the act applies only to U.S. citizens and lawfully admitted permanent residents. Second, the act includes exemptions for law enforcement and national security purposes. Representatives of civil liberties groups and privacy experts have expressed concerns regarding (1) the adequacy of protections for security, data sharing, identity theft, and other identified uses of biometric data and (2) secondary uses and "function creep." These concerns relate to the adequacy of protections under current law for the large-scale data handling in a biometric system. Besides information security, concern was voiced about an absence of clear criteria for governing data sharing. The broad exemptions of the Privacy Act, for example, provide no guidance on the extent of the appropriate uses law enforcement may make of biometric information. Because there is no general agreement on the appropriate balance of security and privacy to build into a system using biometrics, further policy decisions are required. The range of unresolved policy issues suggests that questions surrounding

the use of biometric technology center as much on management policies as on technical issues.

The use of biometric technologies could potentially impact the length of the inspection process. Any lengthening in the process of obtaining travel documents or entering the United States could affect travelers significantly. At some consular posts, visas are issued the day applications are received. Even without biometrics, the busiest ports of entry regularly have delays of 2 to 3 hours. Increases in inspection times could compound these delays. Delays inconvenience travelers and could result in fewer visits to the United States or lost business to the nation. Further studies will be necessary to measure what the potential effect could be on the American economy and, in particular, on the border communities. These communities depend on trade with Canada and Mexico, which totaled $653 billion in 2000.

The use of biometrics in a border control system in the United States could affect the number of international visitors and how other countries treat visitors from the United States. Much visa issuance policy is based on reciprocity—that is, the process for allowing a country's citizens to enter the United States would be similar to the process followed by that country when U.S. citizens travel there. If the United States requires biometric identifiers when citizens of other countries apply for a visa, those countries may require U.S. citizens to submit a biometric when applying for a visa to visit their countries. Similarly, if the United States requires other countries to collect biometrics from their citizens and store the data with their passport for verification when they travel here, they may require the United States to place a biometric in its passports as well.

As more countries require the use of biometrics to cross their borders, there is a potential for different biometrics to be required for entering different countries or for the growth of multiple databases of biometrics. Unless all countries agree on standard biometrics and standard document formats, a host of biometric scanners might be required at U.S. and other ports of entry. The International Civil Aviation Organization plans to standardize biometric technology for machine-readable travel documents, but biometric data-sharing arrangements between the United States and other countries would also be required.

Issues Raised in Joint Report from Justice, State, and NIST

In January 2003, as required by the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act, the Attorney General, the Secretary of State, and NIST jointly submitted a report that focuses on specific legislative requirements related to interoperable databases, biometric identifiers, and travel document authentication for entry only.[7] The report discusses the current border control process, the need for a new approach, and identifies several issues that need to be addressed to make a more extensive use of biometrics in automated border control systems.

As a part of this report, NIST developed technical standards for biometric identifiers and tamper-resistance for travel documents. NIST reported that facial recognition and fingerprint recognition are the only biometric technologies with sufficiently large operational databases for testing at this time. NIST concluded that while iris recognition is a promising candidate, it requires collection of a large test database to test the uniqueness of iris data for large samples. NIST recommends that 10 fingerprints be used for background identification, and a dual biometric system using 2 fingerprint images and a face image may be needed to meet projected system requirements for verification. For tamper-resistance, NIST recommended the use of a public key infrastructure to authenticate the source of travel documents. According to the report, the Attorney General and the Secretary of State have agreed to use a live-capture digital photograph and fingerprints for identity enrollment, background checks, and identity verification. However, the exact number of fingerprints required at enrollment has not been finalized.

The report identifies several issues and considerations that need to be further evaluated and resolved. The resolution of these issues will have significant operational, technical, and cost implications. According to the report, if the various stakeholders of this cross-agency effort do not work out these details before major investments are made, the estimated cost and expected results of the investment will be at risk. Further, the report states that due to the size and complexity of the effort, the deployment schedule will need to be delayed at least 1 year from the October 26, 2004, target date established in the legislation.

[7] The Attorney General, Secretary of State, and the National Institute of Standards and Technology, *Report to the Congress: Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents* (Jan. 2003).

Many of the issues identified in the report are consistent with the challenges we identified in our work last year. For example, the report discusses the need to change the end-to-end business process to incorporate the enrollment and verification of biometric information from travelers. Further, the report cites the need to improve border security without a major adverse effect on tourism, commerce, and border traffic flow. Privacy issues and the effect on international relations are also addressed. Exception processing is discussed. According to the report, approximately 2 percent of the population cannot provide good fingerprint images. As a result, an alternate enrollment and identification procedure will be required for these people. To develop the biometric border control system, the report estimates it would cost about $3.8 billion including initial and recurring costs over a six-year period.

The report cites a number of steps that need to be taken by a cross-agency project team to clarify the scope, costs, benefits, and schedule required to implement the legislative requirement. For example, the report cites the need to develop a cross-agency concept of operations for the entire end-to-end process that would guide the scoping, requirements definition, and trade-off analyses required to develop and deploy the system. The concept of operations would also help determine how the proposed solution can balance identity verification and efficient traffic flow objectives at land borders. The report also discusses the need to update the overall costs and benefits of the solution to confirm that the effort will achieve the benefits desired at an acceptable cost. Steps will also need to be taken to align U.S. biometric standards with those of other countries, particularly visa-waiver countries, in a manner consistent with the concept of operations. Finally, the report cites the need to define and establish a cross-agency program management and governance structure to drive the business change and deployment associated with this effort.

Current Inspection Challenges at Land Ports of Entry

As the Department of Homeland Security and other agencies consider a biometrics-based border security concept of operations, they may need to address current challenges that we have observed during our ongoing work at land ports of entry. At a minimum, these challenges represent potential implementation issues that could affect the security benefits intended by the new border security system. These challenges include:

- **Integrity of the Inspections Process.** The need to balance the dual objectives of identifying those who should not be permitted entry into the country and keeping traffic and trade flowing through the ports creates potential weaknesses in the process that biometrics can help

resolve but not entirely. For example, we recently reported on our ability to enter the country at ports of entry with erroneous answers to inspector questions and counterfeit identification.[8] Also, at land ports of entry, computer checks are made on the vehicle that travelers arrive in but not on the driver and passengers unless inspectors suspect wrongdoing. Moreover, we observed that new security procedures aimed at increasing process integrity were not consistently followed. With respect to alternative inspection programs, various trusted traveler programs, intended to process large numbers of pre-screened travelers quickly so that inspectors can devote more time to travelers whose risk is unknown, can be strengthened through wider use of biometrics. Some current programs are not attractive to many travelers because the cost of participation does not ensure time savings when crossing the border.

- **Providing Technology and Equipment to Inspectors.** Some current border operations are time-consuming because inspectors must separately log on and off of several lookout databases that need to be checked when more intensive, or secondary, inspections are required. This could increase the risk that an inspector might overlook valuable information. Further, inspectors still perform many routine administrative processes by hand, although some ports of entry have successfully automated some of these manual processes. Once the concept of operations for a new border security system is adopted, extensive introduction of new equipment and automated processes will require extensive training and reinforcement.

- **Access to Intelligence Information.** The amount of intelligence information border inspectors currently receive in a single day can be overwhelming, and inspectors report that they do not have enough time to read it. Further, because of the need to staff inspection lanes, some ports of entry reported not having time to conduct daily intelligence and safety briefings, as required. Ensuring that intelligence information is relevant, and that inspectors have sufficient time to review and absorb it, will present a significant challenge for a new border security system.

- **Adequate and Consistent Inspector Training.** Merging INS and Customs inspectors into a single shared inspection force will be a significant challenge because INS and Customs train their inspectors at

[8] U.S. General Accounting Office, *Weaknesses In Screening Entrants Into The United States*, GAO-03-438T (Washington D.C.: Jan. 30, 2003).

two separate academies using two different curricula with little time devoted to learning each other's laws and regulations. In addition, training, particularly of new inspectors, is a continuing need after deployment of inspectors, but the pressures of inspection itself has taken precedence over both on-the-job training and formal training at some ports.

In conclusion, biometric technologies are available today that can be used for border security. However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. As we have pointed out, weaknesses in any of these areas, such as those we identified at land ports of entry, diminishes the effectiveness of the security process. We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a border control system:

1. Decisions must be made on how the technology will be used.

2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs.

3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and the economy.

A report recently issued jointly by the Attorney General, Secretary of State, and NIST agrees with these considerations. As DHS and other agencies consider the development of a border security system with biometrics, they need to define what the high-level goals of this system will be and develop the concept of operations that will embody the people, process, and technologies required to achieve these goals. With these answers, the proper role of biometric technologies in border security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

Mr. Chairmen, this concludes my statement. I would be pleased to answer any questions that you or members of the subcommittees may have.

Contacts and Acknowledgments

For further information, please contact Nancy Kingsbury, Managing Director, Applied Research and Methods, at (202) 512-2700, or Richard Stana, Director, Homeland Security and Justice, at (202) 512-8777. Individuals making key contributions to this testimony include Yvette Banks, Naba Barkakati, Michael Dino, Barbara Guffy, Richard Hung, Rosa Lin, and Lori Weiss.

Related GAO Products

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO-03-519T. Washington, D.C.: March 3, 2003.

Homeland Security: Challenges Facing the Coast Guard as it Transitions to the New Department. GAO-03-467T. Washington, D.C.: February 12, 2003.

Weaknesses In Screening Entrants Into The United States. GAO-03-438T. Washington, D.C.: January 30, 2003.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102. Washington, D.C.: January 2003.

Homeland Security: Management Challenges Facing Federal Leadership. GAO-03-260. Washington, D.C.: December 20, 2002.

Homeland Security: Information Technology Funding and Associated Management Issues. GAO-03-250. Washington, D.C.: December 13, 2002.

Border Security: Implications of Eliminating the Visa Waiver Program. GAO-03-38. Washington, D.C.: November 22, 2002.

Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information. GAO-03-188. Washington, D.C.: November 21, 2002.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO-03-297T. New York, NY: November 18, 2002.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions. GAO-03-155. Washington, D.C.: November 12, 2002.

Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool. GAO-03-132NI. Washington, D.C.: October 21, 2002.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

Identity Fraud: Prevalence and Links to Alien Illegal Activities. GAO-02-830T. Washington, D.C.: June 25, 2002.

Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy. GAO-02-861T. Washington, D.C.: June 19, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project. GAO-02-545. Washington, D.C.: May 13, 2002.

National Preparedness: Technologies to Secure Federal Buildings. GAO-02-687T. Washington, D.C.: April 25, 2002.

INS Forensic Document Laboratory: Several Factors Impeded Timeliness of Case Processing. GAO-02-410. Washington, D.C.: March 13, 2002.

Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems. GAO-02-66. Washington, D.C.: January 31, 2002.

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

Immigration and Naturalization Service: Overview of Recurring Management Challenges. GAO-02-168T. Washington, D.C.: October 17, 2001.

INS Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years. GAO-01-842. Washington, D.C.: August 2, 2001.

United States Senate
Committee on the Judiciary

Committee Information Go

HOME > HEARINGS > "BORDER TECHNOLOGY: KEEPING TERRORISTS OUT OF THE UNITED STATES – 2003."

Members
Subcommittees
Hearings
Nominations
Business Meetings
Press

Statement of
The Honorable Patrick Leahy
United States Senator
Vermont

March 12, 2003

PRINTABLE VERSION

I would like to thank Senators Kyl, Feinstein, Chambliss, and Kennedy for holding this hearing on a topic that is so critical to my state and our nation. It makes perfect sense to conduct a joint hearing because the issues really do overlap – we need to improve the technology guarding our borders so we prevent terrorists from entering, while also assuring that whatever technologies we adopt are consistent with the need to maintain an orderly flow of people and goods across our borders. If we fail to do the former, the consequences are obvious. But we must also remember that if we fail to do the latter, our economy will suffer immeasurably.

Of course, this is an area where striking an appropriate balance is exceedingly difficult, and I look forward to hearing the views of our witnesses. I would like to offer a special welcome to Asa Hutchinson, appearing for the first time before this Committee in his new capacity as Undersecretary for Border and Transportation Security at the Department of Homeland Security. I regret that we were not able to hold your confirmation hearing in this committee, but I am pleased that you are appearing before us so early in your tenure. I was also pleased to see that Stewart Verdery, a distinguished former counsel for this Committee, has been named as Assistant Secretary for Border and Transportation Security.

We know that increasing the number of law enforcement personnel at our land borders is a necessary, but not sufficient, step toward improving our nation's security. In the USA Patriot Act, Congress enacted my proposal not only to triple the number of INS Inspectors, Border Patrol agents, and Customs officers at our borders, but also to provide $100 million to improve the technology we use to monitor the Northern Border and to acquire more monitoring equipment. In the same Act, we mandated improvements in information-sharing among Federal agencies, called for a faster implementation of the integrated entry-exit data system to track foreign visitors, and required that other nations that participate in the visa waiver system develop tamper-resistant passports. The USA Patriot Act was complemented by the excellent work of Senators Kennedy, Feinstein, Kyl and Brownback in last year's Enhanced Border Security and Visa Reform Act, which I was proud to cosponsor. That law provided for further increased

investment in border security technology, as well as substantial improvements to our foreign student tracking system, the entry-exit data system, and the visa waiver program, among other things.

We have passed two major bills in the last year and a half to safeguard our borders, and it is now time for us to exercise our oversight powers to ensure their proper implementation. We have asked the executive branch and our own General Accounting Office to study what technologies make the most sense, and today we will hear from representatives of both. There seems to be no shortage of technologies from which to choose. Companies large and small from throughout our nation are responding to the increased need for security by developing new products or retooling existing ones. In Vermont, a Bellows Falls company named AngioLaz has made the Vision Stick, a surveillance tool that can monitor otherwise inaccessible areas, including borders.

Of course, it is difficult to discuss our border security without considering both the administrative challenges the new Department of Homeland Security faces and the budgetary constraints that the Bush Administration has imposed upon it. Our security depends upon the effective integration of dedicated officers who worked for 22 different Federal agencies at this time last month. I know that these employees have many questions about what the future holds for them, and I would urge Undersecretary Hutchinson, as well as Secretary Ridge, to address those questions as quickly as possible.

For me, this is an issue of both national and local importance. It is a national issue because I am concerned that performance throughout the new Department will suffer if a substantial number of employees are worried about their futures. It is a local issue because I know many dedicated people in Vermont who are new Department of Homeland Security employees. For example, there were more than 1,600 INS employees in Vermont who are now working for DHS. They protect our borders, assist in the enforcement of our immigration laws in the interior, and foster legal immigration and commerce by processing applications for immigration benefits. They are the sort of well-trained and highly-educated people we need to keep if we are going to protect our nation effectively. I would strongly encourage each of you who are here today from DHS to provide as much guidance as you can to your new employees, and to retain their expertise to the maximum extent possible.

As we hold this hearing about reducing the vulnerability of our borders, the Administration continues to engage in what House Appropriations Committee Chairman Bill Young has called "a pointless and harmful debate" with its own party in Congress to avoid blame for under-funding homeland security. I agree

with Chairman Young that we can choose either to continue this distracting debate – as the White House apparently prefers – or to "address the real issues facing first responders" and our other security needs. Mr. Young's March 6 letter to White House Chief of Staff Andrew Card – reported widely in the press – shows that the Administration knew exactly what Congress was prepared to appropriate for homeland security. If the White House wanted more funding, it had the opportunity to demand it. Unfortunately, it is completely in keeping with this Administration's record on homeland security that it offered no complaints until after the bill was passed.

First, only a few months after the September 11, 2001 attacks, the President threatened to veto additional funding of about $10 billion for new customs agents, port security, and other pressing needs, causing otherwise supportive Republican members to oppose the supplemental funding. Last summer, the President refused to spend $5.1 billion that Congress had approved on a bipartisan basis, half of which was for homeland security improvements. Now, while complaining that Congress has shortchanged our security for fiscal year 2003, the President is proposing a budget for FY 2004 that does not come close to meeting our security needs. For example, the President's budget for border security provides for less than a 3 percent increase. Our nation faces serious challenges that will not be met through incremental improvements.

Neither political rhetoric nor administrative reorganization will make us safer. I look forward today to discussing something that will – improving our technology.

#####

- TOP OF THIS PAGE
- RETURN TO HOME

PRINTER FRIENDLY VERSION