AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 107–1043

# TOOLS AGAINST TERROR: HOW THE ADMINISTRATION IS IMPLEMENTING NEW LAWS IN THE FIGHT TO PROTECT OUR HOMELAND

## HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

OCTOBER 9, 2002

**Serial No. J–107–110**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
88–868 PDF WASHINGTON : 2004

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

PATRICK J. LEAHY, Vermont, *Chairman*

| | |
|---|---|
| EDWARD M. KENNEDY, Massachusetts | ORRIN G. HATCH, Utah |
| JOSEPH R. BIDEN, JR., Delaware | STROM THURMOND, South Carolina |
| HERBERT KOHL, Wisconsin | CHARLES E. GRASSLEY, Iowa |
| DIANNE FEINSTEIN, California | ARLEN SPECTER, Pennsylvania |
| RUSSELL D. FEINGOLD, Wisconsin | JON KYL, Arizona |
| CHARLES E. SCHUMER, New York | MIKE DEWINE, Ohio |
| RICHARD J. DURBIN, Illinois | JEFF SESSIONS, Alabama |
| MARIA CANTWELL, Washington | SAM BROWNBACK, Kansas |
| JOHN EDWARDS, North Carolina | MITCH MCCONNELL, Kentucky |

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

---

## SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairperson*

| | |
|---|---|
| JOSEPH R. BIDEN, JR., Delaware | JON KYL, Arizona |
| HERBERT KOHL, Wisconsin | MIKE DEWINE, Ohio |
| MARIA CANTWELL, Washington | JEFF SESSIONS, Alabama |
| JOHN EDWARDS, North Carolina | MITCH MCCONNELL, Kentucky |

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

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS


| | Page |
|---|---|
| Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin | 11 |
| Feinstein, Hon. Dianne, a U.S. Senator from the State of California | 1 |
| Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah, prepared statement | 123 |
| Kyl, Hon. Jon, a U.S. Senator from the State of Arizona | 3 |


## WITNESSES


| | |
|---|---|
| Edson, Stephen A., Acting Deputy Assistant Secretary of State for Visa Services, Bureau of Consular Affairs, Department of State, Washignton, D.C. | 23 |
| Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C. | 5 |
| Fisher, Alice, Deputey Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C. | 8 |
| Hastings, Scott, Associate Commissioner for Information Resources Management, Immigration and Naturalization Service, and Michael Cronin, Assistant Commission for Inspections, Immigration and Naturalization Service, Washington, D.C. | 21 |
| Lormel, Dennis, Chief, Terrorist Financing Operations Section, Counterterrorism Division, Federal Bureau of Investigation, Washington, D.C. | 10 |
| Wu, Benjamin, Deputy Under Secretary for Technology, Department of Commerce, Washington, D.C. | 25 |


## QUESTIONS AND ANSWERS


| | |
|---|---|
| Responses of Mr. Edson to questions submitted by Senators Feinstein and Kyl | 36 |
| Responses of Mr. Hastings and Mr. Cronin to questions submitted by Senators Feinstein and Kyl | 52 |
| Responses of Mr. Wu to questions submitted by Senators Feinstein and Kyl | 74 |


## SUBMISSIONS FOR THE RECORD


| | |
|---|---|
| Cronin, Michael, Assistant Commission for Inspections, Immigration and Naturalization Service, Washington, D.C., prepared statement | 78 |
| Edson, Stephen A., Acting Deputy Assistant Secretary of State for Visa Services, Bureau of Consular Affairs, Department of State, Washignton, D.C., prepared statement | 90 |
| Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C., prepared statement | 99 |
| Fisher, Alice, Deputey Assistant Attorney General, Criminal Division, Department of Justice, Washington, D.C., prepared statement | 108 |
| Hauer, Jerome M., Acting Assistant Secretary for Public Health Emergency Preparedness, Department of Health and Human Services, Washington, D.C., prepared statement | 125 |
| Lormel, Dennis, Chief, Terrorist Financing Operations Section, Counterterrorism Division, Federal Bureau of Investigation, Washington, D.C., prepared statement | 130 |
| Wu, Benjamin, Deputy Under Secretary for Technology, Department of Commerce, Washington, D.C., prepared statement | 144 |

# TOOLS AGAINST TERROR: HOW THE ADMINISTRATION IS IMPLEMENTING NEW LAWS IN THE FIGHT TO PROTECT OUR HOMELAND

---

**WEDNESDAY, OCTOBER 9, 2002**

UNITED STATES SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 10:10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, Chairman of the Subcommittee, presiding.

Present: Senators Feinstein, Feingold, and Kyl.

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

Chairperson FEINSTEIN. Good morning, ladies and gentlemen. It is a pleasure for me to welcome you to this hearing of the Technology, Terrorism and Government Information Subcommittee.

I would like to welcome the Ranking Member, Senator Kyl, from Arizona, with whom I have worked now for 7 or 8 years either as chairman or ranking of this Subcommittee, and also the distinguished Senator from Wisconsin, Senator Feingold. We are delighted to have you with us this morning as well.

The September 11 terrorist attacks were a wake-up call for our country. In the aftermath of those attacks, it quickly became apparent that our approach to combating terrorism was, to put it simply, broken.

In response to the failures that led up to September 11, Congress passed a number of key legislative initiatives to beef up—well, we are working on beefing up homeland security, giving law enforcement a greater ability to go after potential terrorists, and improving the protection of our borders.

Two of the most important of those initiatives were the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act, each of which passed within just a few months of the terrorist attacks and each of which contained a number of key provisions and deadlines to enhance homeland security. It is these pieces of legislation that are the topic of today's hearing.

We are here to ask a number of questions of some very distinguished panelists. Are the new laws working? Are there things we left out? Are there improvements we should make? And most im-

portantly, what progress is being made by the administration to implement these new items?

The USA PATRIOT Act was passed by the full Judiciary Committee with the knowledge that it had been drafted and negotiated rather quickly—only 6 weeks elapsed between proposal and passage—and that Congress would need to exercise vigorous oversight to prevent abuses and solve unintended problems. That is one reason why some of the tools in the USA PATRIOT Act will sunset in a few years.

If the new tools of this Act are working well and are effective, clearly we should keep them, and perhaps if needed, even strengthen them. If they are being abused, we should eliminate them or add new safeguards.

The reforms in the USA PATRIOT Act were spurred by the fact that key agencies in our Government had information about the hijackers and their plans before they attacked, but didn't share this information and didn't act on it. These failures reveal fragmentation of anti-terrorism efforts and the need for better information-sharing.

The lack of investigative and intelligence authority was another problem. As Judiciary and Intelligence Committee hearings have revealed—and both Senator Kyl and I sit on these joint Intelligence hearings—the FBI was unable to obtain a search warrant for the computer of accused terrorist Zacarias Moussaoui, who was detained by the FBI and the INS in August of 2001 after his enrollment in flight simulator training for jumbo jets raised considerable suspicion.

Hearings also demonstrated that the terrorists made ample use of e-mail and the Internet in planning these attacks. The Government clearly needed and still needs adequate tools to monitor electronic communications.

Senator Kyl and I worked together on the encryption issue. And yesterday at the hearings, Senator, you might be interested to know that I asked the question of former FBI Director Louis Freeh as to whether the informal arrangements that he had made as a product of some meetings I organized were adequate, and he said clearly, no, they are not adequate.

There are some voluntary agreements between large computer companies and the FBI and other security organizations with respect to the key issue, but there were real problems and this remains a major point of American vulnerability. So I think this is something that this committee really should take another look at at a future hearing.

Finally, the disclosure that hijackers entered the United States on legal visas showed a need for immigration reform. So the PATRIOT Act was an effort to solve some real problems.

One issue is the ability of agencies to utilize the tools we gave them. The FBI can best use these new tools if it has a road map to ensure that it knows the nature, the likelihood, and the severity of the terrorist threat we face, as well as intelligence gaps that still remain.

The DOJ Inspector General will testify today that the FBI has not yet performed a comprehensive written assessment of the ter-

rorist threat facing the United States. That came out yesterday in our Intelligence hearings as well.

I don't want to go on and on, but with respect to the Border Security Act, there are some things that are important.

First, enhancing our intelligence capacity is key to increased security. Second, our most effective security strategy is to keep out those who do us harm, while admitting those who come to build America and be good residents.

There still are five areas of vulnerability in our immigration system. We still have an unregulated visa waiver program in which 23 million people arrive with little scrutiny from 29 different countries. Now, there are 28; Argentina is out of the program. Abuse of the visa waiver program is real and there are examples of it.

Second, we have an unmonitored non-immigrant visa system in which 7.1 million tourists, business visitors, foreign students, and temporary workers arrive. To date, INS does not have a reliable tracking system. We need to know how progress is going because this remains a huge loophole. We don't know if people leave, we don't know where they are in the country, and that is 7 million visitors.

Third, the porous nature of our borders, along with INS' unreliable recordkeeping, have contributed to the agency's inability to keep out criminals and terrorists. We need to continue to strengthen the border, and it can be done.

Fourth, this is an era where terrorists use satellite phones and encrypted e-mail. The INS, our Nation's gatekeeper, is considered by many observers to still be in the technological dark ages. The agency is still using paper files, archaic computer systems, often non-functioning. They don't communicate with each other and they do not integrate well with other law enforcement systems.

Fifth, about 50 to 70 percent of the estimated 7 to 9 million illegal immigrant population are visa overstayers. So people who come here illegally, 50 percent of them come with visas and then just simply disappear.

In particular, I am going to be interested in learning more about the progress of the State Department, INS, and the National Institute of Standards and Technology in, one, establishing tamper-resistant visas and passports; two, establishing a non-immigrant tracking system using biometric data to verify the identity of persons seeking to enter the United States—I very deeply believe this becomes a key and critical tool in deterring terrorists from entry—three, upgrading the information technology systems; and, four, building the necessary technology infrastructure so we can better protect our ports of entry.

So this is a big agenda, and I want to stop here and see if our distinguished Ranking Member has some comments that he might wish to make.

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

Senator KYL. Thank you very much, Senator Feinstein. First of all, I am very interested in getting answers to the same questions that you have just propounded. Let me add to that that I will be asking at least on the first panel some questions about what addi-

tional tools law enforcement may need. The question you asked about the FBI analysis of the threat, I think, is an important one to get an answer to. I will be curious about the assessment of the sunset provisions in the USA PATRIOT Act.

On panel two, we were going to be talking about the response to the various requirements that we established in the law. You identified them, but we need to have some very forthright assessments of the features of the Border Security Act; for example, whether the deadlines in the Act are going to be met, where we are in the process of creating the interoperable data system that everybody agrees we need.

As a matter of fact, I note that just this month there is a 171-page report by the Brookings Institution and Center for Strategic and International Studies that concludes that we have to have an interoperable data system, the same one that we actually already require in the Act.

How is the State Department responding to the visa issue requirement as it pertains to individuals from terrorist-sponsoring nations? How are INS and the State Department responding to the requirement that upon notification, stolen passport numbers must be entered into all relevant systems and to the requirement that INS must determine that any alien who is to be admitted at a port under the visa waiver system also be checked against relevant lookout data bases? Those and other questions we hold this hearing to determine answers to.

I also would like to conclude my opening remarks by referring to a report that was just out today. It is in the National Review magazine, the very latest issue. It is called "The Terror Visas" and it says, "The applications of the September 11 hijackers should have been denied on their face, but the State Department approved them. Why?"

The article goes on to note that in violation of our own provisions, Section 214(b), which essentially provides a presumption against the granting of visas for would-be immigrants, or puts the burden of proof, I should say, on the non-immigrant visa applicant to show that he has ties to his own country, that he has a stated purpose for the visa, a reason for coming back to his country so that he won't be staying in the United States and be one of that 50 percent that you identified—notwithstanding that presumption, the visa application forms of 15 of the 19 September 11 terrorists that were studied—all of the applicants among the 15 reviewed should have been denied visas under that provision on their face.

The article goes into a lot of detail. I will just mention two because they are names we know. Hani Hanjour was first denied a visa. He conveniently changed many of the answers on the next application. Just 2 weeks later, he got a visa. Khalid al-Mihdhar, one of the terrorists who obtained a visa through the Visa Express program, simply listed "Hotel" as his U.S. destination—something that should have prompted the personnel in Saudi Arabia to inquire further.

The bottom line is that apparently, according to this report, about 2 percent of the visas were denied, notwithstanding this presumption against their granting, for the Saudi nationals in the 12

months prior to September 11. The worldwide refusal rate for temporary visas is about 25 percent.

Now, obviously, things have changed. So how about in the 12 months following September 11, Madam Chairwoman? It has gone from 2 percent to 3 percent, according to this article. We will want to know from our witnesses why, according to the State Department's own documents with the letterhead of the embassy in Saudi Arabia, its refusal rate for Saudi nationals in the 12 months following September 11 is a mere 3 percent. That is something that we have got to get into, so I hope that those of you who haven't had a chance to review this can do so and provide us your comments on it.

Thank you, Madam Chairman.

Chairperson FEINSTEIN. Thank you very much, Senator Kyl.

Senator Feingold has indicated that he has to leave at 10:45 and so I will ask him to go first for questions. But do you have a brief opening statement?

Senator FEINGOLD. In light of that, I will just wait and I appreciate it.

Chairperson FEINSTEIN. All right, happy to do it.

Let me quickly introduce the panel. The first panelist is Glenn Fine. He is the Department of Justice's Inspector General. He is a Rhodes Scholar, a graduate of Harvard Law School. He was an attorney specializing in labor and employment law prior to going to Justice. He has prosecuted more than 35 criminal jury trials, handled numerous grand jury investigations, and argued cases in the District of Columbia and the United States Court of Appeals.

He and his staff have made a tremendous contribution to the Subcommittee's work in developing the Enhanced Border Security and Visa Reform Act, and I want to thank you for your cooperation.

The second person is Alice Fisher, of DOJ. She serves as the Deputy Assistant Attorney General of the Criminal Division. In that capacity, she supervises several Criminal Division litigating sections, including the Terrorism and Violent Crime Section. That Section has handled all investigations and prosecutions relating to the 9/11 terrorist attacks.

The next person is Dennis Lormel, of the FBI. He joined the FBI 26 years ago as a special agent and he now serves as Chief of the Terrorist Financing Operation Section of the Counterterrorism Division. Immediately following the 9/11 attacks, he was given the responsibility for establishing and coordinating the FBI's comprehensive terrorist financing initiative. He also oversees the Multiagency Terrorist Financial Review Group, which is responsible for tracking and investigating terrorists' financial abilities. So he can update us on that.

Why don't we begin with you, Mr. Fine? If you can possibly truncate your statements into 5 minutes, it will give us more of a chance to have a discussion back and forth.

Welcome.

## STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. FINE. Chairwoman Feinstein, Senator Kyl, members of the Subcommittee, thank you for inviting me to testify today regarding

the Office of the Inspector General's recent audit of the FBI's counterterrorism program.

Last week, our full 131-page classified audit was provided to the FBI and congressional committees, including this Subcommittee, and we publicly released an unclassified executive summary that highlighted our major findings and recommendations.

Our audit was part of a series of reviews that we have undertaken regarding Department programs that affect counterterrorism and national security issues. The audit examined aspects of the FBI's management of its counterterrorism resources, focused specifically on, one, the FBI's progress toward developing a comprehensive written risk assessment of the terrorist threat to the United States; two, the FBI's strategic planning as it relates to counterterrorism; and, three, the amount of resources dedicated to the FBI's counterterrorism program over the past 7 years.

It is important to note at the outset of my remarks that our audit does not purport to assess all aspects of the FBI's counterterrorism program or how the FBI handled information that may have been related to the September 11 attacks. We have initiated a separate review that is examining aspects of the FBI's handling of certain intelligence information related to those attacks, including the Moussaoui case, the Phoenix electronic communication, and other issues.

The audit that we released last week contains several important findings. We determined that the FBI has not developed a comprehensive written assessment of the risk of a terrorist threat facing the United States, despite its statement to Congress in 1999 that it would. We concluded that such an assessment would be useful not only to define the nature, likelihood, and severity of the terrorist threat, but also to identify gaps that need to be addressed. A comprehensive written threat and risk assessment would also be useful in determining where to allocate attention and resources on programs and initiatives to combat terrorism.

By September 2001, the FBI had developed a draft of what it called a terrorist threat report. This report described terrorist organizations and state sponsors of terrorism, but the draft report did not assess the threat and risk of a terrorist attack on the United States.

Among the report's many omissions were assessments of the training, skill level, resources, sophistication, specific capabilities, intent, likelihood of attack, and potential targets of terrorist groups.

Nor did the draft report discuss the methods that terrorists might use. For example, there was no analysis of terrorists' progress toward developing or acquiring chemical, biological, radiological, and nuclear weapons, or any discussion of what the FBI had learned from its past terrorist investigations.

We identified a number of causes for the FBI not adequately addressing these issues. First, no single individual at the FBI was accountable for managing the assessment.

Second, some FBI officials said the FBI lacked the analytical capability or resources to complete such a broad threat assessment.

Third, the FBI did not have a system of management controls that ensured compliance with GAO or OIG recommendations. Also,

FBI counterterrorism managers had a tendency to rely on their own experience and professional judgment regarding the overall terrorist threat and did not value a formal written assessment that used a structured methodology.

We believe that completing the national-level written threat assessment is critical to the FBI's counterterrorism efforts. This assessment must also include an evaluation of the likelihood that specific weapons of mass destruction will be acquired or used against American targets and citizens.

Fully assessing the threat, probabilities, and likely consequences of a terrorist attack by different methods will be of significant benefit not only to the FBI in allocating resources, but also for domestic preparedness efforts and counterterrorism programs at all levels of government.

Our audit also found that the FBI's strategic planning has not been guided by an overall strategic-level assessment of the threat and risk of terrorist attacks on the United States. The FBI's strategic plan has not been updated since 1998 and does not conform to the counterterrorism priorities in the Department's November 2001 strategic plan, the FBI Director's new priorities, or the FBI Counterterrorism Division's approach to developing the maximum capacity to deal with the terrorist threat.

We also found that the FBI had not developed a system for capturing and using lessons learned from past terrorism incidents and operations to improve the FBI's counterterrorism capabilities. In addition, the FBI has not established a core training curriculum and proficiency standards for these new agents working in counterterrorism.

Our report details the level of resources that the FBI has dedicated to counterterrorism and related counterintelligence over the last 7 years. While the FBI has indicated that the exact figures are classified, I can say that those resources have tripled between 1995 and 2002.

I want to be clear that our findings are not intended to criticize the expertise of FBI employees and managers who work on counterterrorism matters or the extensive knowledge they have developed through their casework and regular discussions with the FBI and the intelligence community.

Our findings also should not be interpreted to mean that the FBI has not taken important steps during the past year to improve its counterterrorism program. After the September 11 attacks, the FBI identified as a critical weakness its ability to analyze intelligence and has begun taking steps to improve its capabilities in this area.

But we believe the FBI can and must do more. Our audit report offers a total of 14 recommendations to help improve the management of the FBI's counterterrorism program, including recommendations that the FBI prepare an authoritative, written, national-level threat and risk assessment of terrorism; identify the chemical and biological agents most likely to be used in a terrorist attack; develop criteria for evaluating incoming threat information and establish a guide for the distribution of threat information; build a core of professional trained and experienced intelligence analysts for assessing and reporting on threats at both the strategic and the tactical levels; and close the gap between FBI planning

and operations by establishing an effective system of performance measures and holding FBI managers at all levels accountable for achieving those performance goals.

The FBI responded that it concurred with our recommendations and that they provide constructive guidance. It described the steps it has taken to address the recommendations. We are pleased that the FBI has agreed with our recommendations and we look forward to monitoring the FBI's progress toward implementing them.

We believe these recommendations will aid the FBI in making the changes set in motion by the FBI Director to move the Bureau from a reactive, post-crime investigatory culture to a more proactive organization that seeks to identify and deter terrorists before they can strike.

This concludes my statement and I would be pleased to answer any questions.

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

Chairperson FEINSTEIN. Thanks, Mr. Fine, and again thanks for your help to this Subcommittee. We appreciate it.

Ms. Fisher?

**STATEMENT OF ALICE FISHER, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.**

Ms. FISHER. Thank you, Chairman Feinstein, Senator Kyl, Senator Feingold. Thank you for providing me the opportunity to testify on behalf of the Department of Justice to inform the Subcommittee about the Department's implementation and use of the important anti-terrorism provisions in the USA PATRIOT Act.

I want to thank this Subcommittee's members who helped to develop and enact the USA PATRIOT Act so swiftly in the wake of last September's attacks on our Nation. As Deputy Assistant Attorney General in the Criminal Division, I am personally involved in using the tools myself and in working with others in the Department in seeing that the tools Congress provided in the Act have been used as intended, to enhance the ability of law enforcement to bring terrorists to justice.

The unprecedented and heinous attacks on our Nation, in which over 3,000 innocent civilians were killed, occurred just over 1 year ago. At that time, the President pledged to the American people that we would not relent until justice was done and our Nation secure.

Members of this committee and the Congress in general joined the President as key partners in this important undertaking. Congress' swift and comprehensive response was to develop and pass the USA PATRIOT Act, which provided law enforcement with vital new tools and updated those tools already at our disposal that have been instrumental in our efforts to combat terrorism and the most extensive criminal deeds in history.

One year later, I am pleased to report that we have used these tools effectively, aggressively, and I believe responsibly. As the Attorney General told this committee in July, the Department's single overarching goal since September 11 has been to prevent future attacks on the United States and its citizens.

In furtherance of that goal, we have been aggressively implementing the USA PATRIOT Act from the outset. Law enforcement uses the tools in our ongoing cooperative effort to identify, disrupt, and dismantle terrorist networks. We are expending every effort and devoting all available resources to intercept terrorists and defend our Nation.

Never was this so apparent as last Friday—as the Attorney General describing it, a defining day in the war on terrorism—when law enforcement neutralized a suspected terrorist cell in Portland, Oregon, convicted attempted suicide bomber Richard Reid, and saw John Walker Lindh, an American captured fighting for the Taliban in Afghanistan, sentenced to 20 years in prison.

In the last 6 weeks, we have charged 17 individuals involved in terrorist-related activities. In addition to Portland, we have charged an individual with attempting to set up an Al-Qaeda training camp in Oregon. Tools authorized by the USA PATRIOT Act, such as information-sharing provisions and enhanced penalty provisions, have been critical in all of these cases.

The PATRIOT Act has aided law enforcement efforts in the war on terrorism in four key areas. First, it updated the law to reflect new technology. Second, it removed obstacles to investigating terrorism. Third, it strengthened criminal laws and enhanced penalties. And, fourth, it facilitated increased intelligence-sharing, gathering, and analyzing.

As examples, over the past year the Department has used the following important new authorities and tools provided by the Act. We have charged a number of individuals under 18 U.S.C. 2339A and 2339B, which prohibit providing material support to terrorists or terrorist organizations and now carry enhanced penalties.

We have used, newly streamlined authority to use trap and trace orders to track communications of a number of criminals, including the terrorists, kidnappers, and murderers of journalist Danny Pearl, as well as identity thieves and a four-time murderer.

We have used new authority to subpoena information about Internet users' network addresses to track down terrorists and computer hackers. We have used newly authorized nationwide search warrants for terrorist investigations at least three times, including during the ongoing anthrax investigation.

We have used, on many occasions, provisions in the Act to foster an unprecedented level of cooperation and information-sharing between Government agencies. For example, we have disclosed grand jury information on at least 40 occasions.

We have saved precious time and resources through a provision that permits officials to obtain court orders for electronic surveillance pertaining to a particular suspect rather than a particular device. We have used the provision allowing Internet providers to disclose records to law enforcement in emergencies preventing risk of life. This authority allowed us to track down a student who posted electronic bulletin board threats to bomb his high school and shoot a faculty member. We have also made sure that the prosecutors in the field know what valuable tools Congress has provided them by training and through guidance.

I would like to conclude by thanking the members once again of your committee for your efforts in so swiftly giving us these tools.

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

Chairperson FEINSTEIN. Thank you very much, Ms. Fisher.

Mr. Lormel, welcome back to the committee.

**STATEMENT OF DENNIS LORMEL, CHIEF, TERRORIST FINANCING OPERATIONS SECTION, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.**

Mr. LORMEL. Thank you, ma'am. I also appreciate the opportunity to participate in this forum today. I have submitted a formal statement for the record and I would just like to augment that with some comments, and particularly to stress the importance of interagency cooperation. Clearly, that is important in our mission.

I would like to commend the Treasury Department, who aren't here, for their outstanding efforts in furtherance of methodologies being developed for use of the PATRIOT Act and working with us, and particularly David Offhauser for his leadership role in the Policy Coordinating Committee on Terrorist Financing.

I would like to focus my comments on the progress that we are making in terrorist financing investigations and the operational benefits that we have specifically derived from the PATRIOT Act. I think that will be important for your benefit.

First, our mission is two-fold. We were formed to investigate the events around the 19 hijackers and identify the financial infrastructure and flows. We have pretty much completed that, and at the same time we set up a template for investigations in the future to be much more proactive and progressive and predictive. We have adopted a centralized approach. We are looking outside the box to develop new methodologies in our approaches, and clearly the PATRIOT Act really helps us in that regard.

Our strategies are to conduct full financial analysis of terrorist suspects and their financial support structures; disrupt and dismantle terrorist funding mechanisms; coordinate the joint participation and liaison and outreach efforts to exploit financial investigative resources of private, government, and foreign entities; utilize the FBI and LEGAT expertise in reaching out and fully exploiting those relationships; work jointly with the law enforcement, regulatory, and intelligence and business communities to develop predictive models based on terrorist cell financial traits; and conduct data-mining analysis to proactively identify terrorist suspects. We are also providing financial investigative components to the Counterterrorism Division and the overall mission. We are a support component of the Counterterrorism Division.

Our investigative initiatives include support to significant terrorism investigations and deployments, and strategic investigative targets that we are going after, which include Al-Qaeda cells and other cells of Hamas and Hezbollah, in particular.

We are looking at financial institutions, particularly non-banking financial institutions, the hawalas, the money services businesses and others. Clearly, in that regard, the PATRIOT Act is a big help to us. We are looking at NGO's and charities, fundraisers, facilitators, couriers, and donors.

We are conducting a number of data-mining initiatives. We are looking at undercover possibilities and platforms, clearly looking at

the Internet, and we have established a 24/7 financial monitoring capability where we have a network of over 411 financial institutions involved. Clearly, human intelligence and outreach are important.

We are striving to disrupt the flows of funding to terrorists by going back to the donors and forward to the strike teams. There are clearly three or four tracks, and I will come back to that in questions, if you like, as to how we are proceeding in that regard.

Again, I would like to reiterate the importance of our cooperation and coordination particularly with the CIA and Treasury, and FinCEN in particular is an important partner for us with regard to the PATRIOT Act and the utilization of the provisions.

The benefits that we have derived from the PATRIOT Act—clearly, on the financial side, the enhanced reporting requirements regarding suspicious activities, particularly with the non-banking financial institutions; registration requirements for licensed money remitters, and this provides us with a broader data-mining and investigative avenue to go after information.

The authority to seize terrorist assets has been beneficial. The ability to seize foreign bank accounts, or funds in foreign bank accounts through correspondent accounts here in the U.S. has been helpful. The ability to prosecute unlicensed money remitters is going to be very important to us; more timely access to reports on currency transactions in excess of $10,000; authority for the service of administrative subpoenas on foreign bank accounts concerning records of foreign transactions.

Clearly, the sharing of intelligence information and the criminal information between us and the CIA, in particular, has been very important. The mandated FinCEN establishment of the secure network is going to be a tremendous benefit. I believe that our operation will be the primary beneficiary from that.

There are some other things, Senator, but in deference to time and Senator Feingold, I will stop here. Again, I can expand on this during questioning.

Thank you very much.

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

Chairperson FEINSTEIN. We certainly want you to. Thank you.

Senator we will turn to you.

## STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator FEINGOLD. Thank you, Madam Chairman, and I want to commend you and Senator Kyl for holding this very important hearing and your tremendous courtesy in letting me go first. I really do appreciate that. My opportunity to speak on the Iraq resolution is at eleven, so I am grateful.

One of the most vital tasks Congress has is to ensure that the powerful tools we give to law enforcement are used effectively and appropriately. I hope that this hearing will become part of a vigorous and consistent review of the tools Congress has given law enforcement.

On July 24, I sent a letter to the Attorney General requesting a full report on the implementation of the USA PATRIOT Act, and

asked specific questions about the business records, computer trespass, and FISA roving wiretap provisions. I still have not received answers to my questions about the use of the business records, computer trespass, and FISA roving wiretap provisions of the USA PATRIOT Act.

These provisions deserve close congressional oversight because of, among other reasons, the enormous potential chilling effect on the First Amendment rights of innocent Americans who simply want to buy a book from an online retailer or borrow a book from a local public library.

Nevertheless, I have received the Department's unclassified responses to a House Judiciary Committee letter that requested information on the USA PATRIOT Act. The Department answered in response to many of the questions posed by Chairman Sensenbrenner and Ranking Member Conyers that the information would be shared with the House Intelligence Committee, but not the Judiciary Committee.

This is not a response, in my view. There is no reason why the Department should not share with me or my colleagues on this committee or the House Judiciary Committee information like the number of times the Government has requested records from public libraries, bookstores, or newspapers.

Congress has an important responsibility to exercise our oversight of the Department's application of the USA PATRIOT Act, a law that significantly expands the Federal Government's power to intrude in the lives of law-abiding Americans. To the extent the responses are classified, of course, we have well-tested procedures for handling that type of information in this committee.

I am still hopeful that I will receive a full and complete response to my July letter, as well as copies of the responsive material that the Department has apparently conveyed to the House Intelligence Committee but has so far refused to share with the House and Senate Judiciary Committees.

I would like to just ask a couple of questions.

Ms. Fisher, I have heard that the Justice Department is gathering proposals from various divisions from within the Department for a possible sequel to the USA PATRIOT Act. Could you please describe what efforts are being made within the Department to seek to broaden the powers of the USA PATRIOT Act through additional legislation and what other changes to existing law you anticipate the Justice Department will propose?

Ms. FISHER. Thank you, Senator. We have been internally within the Justice Department looking at potential proposals following up on the PATRIOT Act for new tools, and we have also been working with different agencies within the Government and they are still studying that. Hopefully, we will continue to work with this committee in the future on new tools that we believe are necessary in the war on terrorism.

Senator FEINGOLD. Can you give us some sense of what you are looking at?

Ms. FISHER. At this point, I can't. I am sorry. They are studying a lot of different ideas and a lot of different tools that followup on information-sharing and other aspects.

Senator FEINGOLD. I would ask you and the Department to provide us with some sense of where they are heading on this as soon as possible so that we are not confronted again—and it was more understandable last time, of course—with such a brief period of time in which to review such a significant series of proposals.

Ms. FISHER. Yes, Senator.

Senator FEINGOLD. Listening to the witnesses, I am struck by the tools being used in the war on terrorism that are not being spoken about today. Since September 11, the Justice Department has declared and imprisoned two U.S. citizens as enemy combatants, and detained people as material witnesses. In each of these instances, the Justice Department has opposed judicial review and refused to answer congressional questions about the affected people.

I think the rules under the Constitution are pretty simple. If you have evidence of criminal misconduct, then you should provide people with attorneys, bring them into a courtroom and prosecute them. And if you don't have evidence, the Constitution dictates that you cannot hold them indefinitely.

Given the successes that you just, I think, reviewed that DOJ has had in criminal cases arising from the war against terrorism, what is it about the criminal justice system that leads the Justice Department to fear criminally charging the accused and prosecuting them in a courtroom?

Ms. FISHER. I take it that is directed at me.

Senator FEINGOLD. Please, yes.

Ms. FISHER. The Justice Department does not fear bringing of criminal charges, but it is important to understand that these are two separate tracks. "Enemy combatant" is something that comes under the President's authority as Commander-in-Chief of our country and it provides the military—and this has been upheld by the Supreme Court—with the authority to detain combatants that would cause harm to our country.

Therefore, a determination is made on a case-by-case situation whether someone—for example, if you are referring to Mr. Padilla or Mr. Hamdi—should be detained as enemy combatants under those powers or should be charged in an Article III Court. But I will say that even if they are held as enemy combatants, they are not held indefinitely, as you suggest. In fact, they are held for the duration of the conflict.

Senator FEINGOLD. Well, why was the choice made not to charge them in a criminal proceeding? What is it about them that means that they can't be charged in a criminal proceeding?

Ms. FISHER. Well, I wouldn't comment on saying that they can't be charged. It often may be the case that you could qualify as both an enemy combatant and be charged in a criminal Article III proceeding, such as John Walker Lindh.

However, in this case when the Department and other aspects of the Government looked at the facts and looked at the national security interests and the information available, it was the Commander-in-Chief power utilized by the President to detain these two individuals as enemy combatants.

Senator FEINGOLD. I understand that is the decision, but let me just say that I think it is deeply troubling to many Americans to not really understand why the decision was made. I understand

that the decision was made, but given the lack of rights and procedures that are associated with this rather startling enemy combatant concept, I think that it would be in the interests of the administration to provide a better explanation of why this rather unusual procedure is used.

Finally, Mr. Fine, pursuant to Section 1001 of the USA PATRIOT Act, your office submitted a report concerning complaints alleging abuses of civil rights and civil liberties by employees and officials of the Justice Department covering the period from October to June 2002.

According to the report, there were 458 complaints suggesting a USA PATRIOT Act-related civil rights or civil liberties connection. These complaints included charges of excessive force, illegal detention, and a denial of the right to counsel.

What is the status of the IG investigation and what can you tell us about the merits of the complaints that you have investigated?

Mr. FINE. Senator Feingold, I can tell you that we have a number of ongoing investigations, both criminal and administrative. We have also referred several of the allegations to other agencies, including the FBI, which is reviewing and investigating some of them.

In addition to the individual ongoing investigations, we also have a review that tries to look at it in a systemic way. So we have looked at the treatment of special-interest detainees at two facilities, the Metropolitan Detention Center in Brooklyn and the Passaic, New Jersey, facility, looking at issues such as their access to counsel, the conditions of confinement, the timing of charging decisions. We are pretty far along in that review and we hope to have a comprehensive review done in the near future. So we are working hard on that and look forward to having findings soon.

Senator FEINGOLD. You don't have any comment on the merits of the complaints at this point?

Mr. FINE. I wouldn't want to comment on an ongoing investigation.

Senator FEINGOLD. My time, I think, has expired, but I would ask the Justice Department—Ms. Fisher, I really hope you can get an answer to my letter of July, and if there is any information that needs to be presented in a classified manner, so be it. I have that clearance; others on my staff do. I surely think that the members of the Senate and the House Judiciary Committees are entitled to answers to those questions.

I do thank all the witnesses, and I especially thank the Chair for letting me do this.

Chairperson FEINSTEIN. Thanks, Senator.

My first question is of Ms. Fisher and I want to just sort of set this question in some context, if I might. In June, the Department of Justice announced that a man was being held. His name was Abdullah al-Muhajir. He was 31, a former Chicago gang member who was born Jose Padilla, in Brooklyn. He was raised as a Roman Catholic, but he converted to Islam and began using a new name.

Mr. Padilla traveled to Pakistan and received training from Al-Qaeda in the wiring of explosives, intelligence officials have said. While he stayed at an Al-Qaeda safehouse in Lahore, he conducted research on radiological devices on the Internet.

Now, in the PATRIOT Act we changed the definitions of pen register and trap and trace devices to include devices that track dialing, routing, addressing, or signaling information. For that might be interested, pen registers and trap and trace devices are like called I.D. on a telephone. They record the date, the time, and the phone number of outgoing and incoming calls, but they don't reveal their content.

This change allows the tracking of e-mail and Internet usage rather than just phone calls. However, e-mail routing information and Web addresses provide a lot more information than a telephone number. The e-mail address johnsmith(at)yahoo.com identifies a person, not a fixed piece of equipment, and a Web address such as www.plannedparenthood.com provides information about a person's thoughts and interests. To solve this problem, the PATRIOT Act requires that pen registers and trap and trace devices do not capture the content of any communication.

My question to you is how extensively has DOJ been using pen registers and trap and trace devices to track e-mail and Internet usage, and how do you ensure that these devices do not capture the contents of any communication?

Ms. FISHER. Thank you, Senator. We do share your concern about content and we have not used the tools, as we should not, to gather content information. But the pen/trap and trace statute and the tool authorized by the PATRIOT Act has been used on several occasions.

Although I don't have the particular number of times at my fingertips, it was used in the Danny Pearl case. It was used with regard to other terrorist conspirators, one major drug distributor investigation, identity thieves, an investigation to track down a four-time murderer, as well as a fugitive who was fleeing using a false passport.

So we have been using this tool and we have been cautious not to get into content or the Web addresses, as you suggest.

Chairperson FEINSTEIN. So it has been a successful tool?

Ms. FISHER. Absolutely.

Chairperson FEINSTEIN. Do you see any violations of privacy?

Ms. FISHER. No. In fact, I am not aware of any violations of privacy. This tool has been used very carefully. The Deputy Attorney General issued a memo clearly delineating the Department's policy with regard to avoiding over-collection and avoiding the collection of content in the use of this authority.

Chairperson FEINSTEIN. Thank you.

Mr. Lormel, I want to give you an opportunity to expand on the strike aspect that you spoke about in your opening comments, and this, of course, relates to Title III of the PATRIOT Act which focuses on money laundering. The title provided for increased information-sharing. It allows suspicious activity reports received by the Treasury Department to be shared with intelligence agencies, and it authorizes the sharing of surveillance information between law enforcement and intelligence agencies.

Perhaps you can bring us up to date on any new activities that you are taking in that regard, how well this is working and what you are finding.

Mr. LORMEL. Yes, Senator. Some of our agents are assigned over the CIA Counterterrorism Center, and conversely they have got people assigned with us. As I mentioned, we work very closely with FinCEN, and in that regard the sharing of information back and forth between us and the CIA has been outstanding.

I don't have any anecdotes that I can really get into in this forum.

Chairperson FEINSTEIN. You don't have any nuggets like you had last time you appeared before us?

Perhaps I should ask about that. Have banks done anything about the hijackers?

Ladies and gentlemen, six of the hijackers went into a bank to open an account, Mr. Lormel informed us at one of our earlier hearings, and in doing so they just made up Social Security numbers.

Mr. LORMEL. Well, in regard to the Social Security numbers, let me clarify that. The numbers that were used weren't necessarily made-up numbers, but they were on the application in the Social Security field itself. So they are numbers that for automation purposes they had to fill in, and in a couple of instances Social Security numbers were listed which may have been FAA numbers, as opposed to Social Security. But in the instances where the banks themselves listed the numbers, it was basically for administrative purposes in the use of those particular numbers.

But going to the greater question of the cooperation with the banks, a comment I wanted to make was some observations, Senator, that I have seen in implementation of the PATRIOT Act. In anticipation of the implementation between the banking community, and particularly the non-banking financial institutions, their concern about consequence and their concern about doing the right thing in terms of reporting and working closer with us has been outstanding.

That includes forums that we have had through FinCEN, and independent of FinCEN where we are trying to promote the use of the PAC system that FinCEN is implementing. We believe that that is going to enable us in terms of the data-mining to get information in an electronic format that we will have more timely access to and more timely responsiveness in terms of following up on leads in investigations.

Chairperson FEINSTEIN. To date, tell us what you are able to do with respect to the hawala method of transferring funds to terrorist organizations.

Mr. LORMEL. In regard to that, let's go beyond the specific hawala, but into that whole informal mechanism. The fact now that there are licensing or reporting requirements helps us tremendously. We are going to have a conference in the next few weeks where we are bring prosecutors together with our agents to determine the best vehicles out there for proceeding with prosecutions.

We have had some success in the disruption of money flows, and I think there are intelligence reports that will support that. In terms of the actual hawalas and that informal networking, the registration requirements through FinCEN are enabling us to identify who is a licensed money remitter that is outside the normal banking confines and who are unlicensed and perhaps illegal. It enables

us to set up strategies and methodologies on both of those tracks, so we are proceeding accordingly.

Chairperson FEINSTEIN. My time is up.

Senator Kyl?

Senator KYL. Let me begin with Mr. Fine. The threat assessment with regard to terrorism that you strongly suggest the FBI should get on with producing, you said, was hampered to some extent by, at least according to the FBI, a lack of analytical capability within the FBI. Is that correct?

Mr. FINE. Yes.

Senator KYL. What would it take to correct that deficiency for the FBI?

Mr. FINE. I think the FBI needs to focus attention and energy on developing a core of trained professional analysts. They have some, but they need more, and I think the FBI recognizes that. In the past, it has not valued it as much as it perhaps could have and should have.

There has been a focus in the past on reactive crime-solving. Agents' work has been valued, but the more strategic, analytical, overarching analysis that needs to be done and should be done hasn't received as much attention in the past. I think it needs to receive more attention in the future.

Senator KYL. I know FBI Director Mueller immediately brought some CIA analysts over to the FBI. I know he doesn't want to raid the CIA, but that kind of thing could at least in the short term help to augment his cadre, could it not?

Mr. FINE. Yes, it could. He has brought over 25 CIA analysts as detailees that can help in the short term. In the long term, I think the FBI needs to develop its own permanent professional analyst capabilities.

Senator KYL. If they were able to engage in this analytical discipline, it would also require the integration of their field office personnel and the information that they derive from that with the other aspects of the intelligence community, including the CIA, because you can't do analysis without a full knowledge integration. So that in itself would be a useful exercise for further analytical capability at the FBI, would it not?

Mr. FINE. Absolutely. The FBI can't do it on its own. It needs to use intelligence and information from throughout the Government and elsewhere to factor into its analysis. It did try, as we indicated in our report, to look into the threat of weapons of mass destruction, but it didn't do it with all the information that it should have. It has to reach out outside the FBI for expertise that can help them in this area.

Senator KYL. I think we are all aware of the fact that the FBI had some really good nuggets of information, but they weren't brought together in a central place. This call that you are making for an analytical document which would then presumably be ongoing is a very important thing.

I want to ask Mr. Lormel, I gather the FBI has acknowledged the need for this. I suspect that you are not in a position to tell us why it hasn't been fully implemented, but at least perhaps you could confirm to us that you will help convey the message to those with whom you work that we think this is an important thing to

do, to move on with very quickly, and to let us know what you need, if anything, that Congress can help to provide in order to get this done.

Mr. LORMEL. In that regard, Senator, I am aware that we are taking steps to move forward. For instance, we have, I believe, 240 analysts in some stage of backgrounds to come on board. Clearly, the Director deserves a lot of credit for his vision to integrate the analytical component with the operational component, and also the third leg, the financial component. Our financial analysts and things are going to be integrated into that process.

There are strategic reports that are now being drafted that the analytical component, the people from the agency, are involved in in finalizing which will be going forward, I believe, in the very near future.

Senator KYL. Well, just to conclude this point, be sure and convey to those with whom you work our view that this is a very important aspect of the FBI's contribution to the war on terror. The recommendations of the Inspector General should be closely examined and if there is any disagreement with any of that, let us know. Otherwise, we will expect that it will be done with some alacrity.

Mr. LORMEL. Again, Senator, if I may, we embrace those recommendations and I know that the Director is looking to continuously improve our performance.

Senator KYL. Let me just make one other point. We heard testimony yesterday from Louis Freeh, and I remember him coming before this very Subcommittee three and 4 years ago asking us for authority and Senator Feinstein and I supporting those authorities. We couldn't get total cooperation from other members of the Senate and the House, and as a result it wasn't until after September 11 that a lot of what he was asking for was actually done, like the trap and trace, for example, was a good example, the roving wiretap. Those are authorities he asked for long ago.

He also asked for more agents. He asked for something like 1,800 agents and I think we gave him 76 over a 3-year period, or at least numbers in that general realm. So part of the problem is us not necessarily providing what is needed and if there is something needed here to get this job done, we expect to be told.

The red light is on. Let me just close with one question for Ms. Fisher.

In response to Senator Feingold, you indicated that there was an ongoing review of needs within not just the Department of Justice but other agencies of the Government to augment what has already been done in the USA PATRIOT Act, and that that study would produce a set of recommendations, hopefully early so that we can act on that very early next year. That last part I am adding to your testimony.

In this regard, I am especially interested in having you look at the provisions—I think there are some 14 of them in the PATRIOT Act—that will sunset in 3 years. Unless you are aware of specific problems that have arisen with the application of those provisions, several of which are very important, I would hope that you could assess the desirability of making those provisions permanent as part of the recommendations for legislative reform.

Your comment?

Ms. FISHER. We certainly will. As we all know, we don't expect the war on terrorism to sunset in the near future, unfortunately, and we certainly are using all the tools and we don't believe that they should sunset. We have put them to good use, and so making that part of our recommendations, I think, is a very good idea.

Senator KYL. All right. Then, finally, I am kind of catching you off guard here, but Senator Schumer and I have an amendment that we would like to get adopted sometime before Congress adjourns that would slightly modify the FISA warrant procedure to add to the definition "a foreign person."

This perhaps would pertain to Moussaoui, but I don't ask for your comment on that. Where you have an individual you believe is engaged in terrorism, but you can't necessarily connect him to a specific terrorist organization or foreign power, it would still permit the warrant to be obtained to investigate further.

Previous witnesses representing the Department of Justice or the FBI have testified in favor of that. Is that still the position of the Department?

Ms. FISHER. Absolutely. The Administration supports your bill on that. We think that it is an important and needed fix.

Senator KYL. Thank you.

Chairperson FEINSTEIN. To you, Ms. Fisher, I need to say one thing. I authored legislation that was signed into law in 1999 that mandates up to 20 years in prison for anyone who distributes bomb-making information, knowing or intending that the information would be used for a violent Federal crime. That is 18 U.S.C. 842P.

This law has been on the books for 3 years. It has not been enforced. We know that bomb-making information has been found. We know that in Afghanistan and we know that it has been found from the Internet. We know that its intent is clearly for terrorists to use it to violate a Federal law.

Federal prosecutors have only charged a single person under the statute, and then these charges were quickly dropped for lack of evidence. I see this as an indispensable supplement for anti-terrorism tools. Terrorist groups, we know, are not only actively searching out bomb-making information, but they are even distributing it for recruitment and instructional purposes. If they do that, you have got them for 20 years.

Why don't you use the law?

Ms. FISHER. Well, Senator, you raise a good point. Clearly, you are right. We do know that there are individuals out there that are doing this kind of activity with regard to bomb-making materials. I can't speak to the one case where it was used and dropped. We can certainly take a fresh look at that statute and, where appropriate, charge it.

Chairperson FEINSTEIN. One Al-Qaeda videotape consisted of a lab session showing the materials and processes needed to make TNT and high-explosive bombs. So you have a cause, and this ties in with my second question and I was very surprised to see this.

My staff did some research and according to an analysis of DOJ records by the Transactional Records Access Clearinghouse, associated with Syracuse University, from October 2001 to March 2002, Federal prosecutors turned down 55 percent of referrals in inter-

national terrorism cases and 46 percent of referrals in domestic terrorism cases.

What is surprising about this is the likelihood was to decline prosecution for terrorism cases to a much greater extent than for other cases. The declination rates for referrals in non-terrorism cases during the same period was 32 percent.

Why is that?

Ms. FISHER. Well, Senator, a couple of points on that. First, over the past year, and certainly since September 11 when I think you said the data started, I have been involved in overseeing terrorism prosecutions. Terrorism prosecutions, regardless of where they are in the U.S. Attorney's office, come up for approval through Main Justice and I am not aware of one terrorism case that we have declined.

Chairperson FEINSTEIN. Can I ask that perhaps you then research it and give the committee a response in writing? I will be happy to give you the question in writing right now.

Ms. FISHER. Sure.

Chairperson FEINSTEIN. Perhaps you would answer it in writing within the next week.

Ms. FISHER. OK. I am aware that there is a definitional issue of how the FBI characterizes what is a terrorism case, and I know that the FBI is working with the Executive Office of U.S. Attorneys on these statistics to figure out what the definitions are.

It may be that included in those numbers are intelligence cases which don't necessarily go to the Criminal Division because they are continuing as intelligence operations. It also may be that something is catalogued as a terrorist investigation initially, but later it is determined that it has no links to terrorism and it is some other type of charge, and so therefore it is not pursued as a terrorism case.

But it is important to note that I am not aware, and I don't think that the people at Main Justice are aware of any terrorism cases, certainly no international terrorism cases where we have declined prosecution or stepped away from that. We are very aggressively pursuing those cases, and I will be happy to look at your question and get back to you with an answer.

Chairperson FEINSTEIN. Thanks so much.

Senator do you have anything else?

Senator KYL. No.

Chairperson FEINSTEIN. Well, let me just thank the panel very much. You have been very gracious with your time and also with your expertise, and we appreciate it. Thank you.

We will now go to the Visa Reform and Border Entry Act, and I will introduce the witnesses. We have Scott Hastings, from INS. Scott is the Associate Commissioner for the Office of Information Resources Management with INS. He is responsible for the information technology programs, including all electronic enforcement technology programs. He is also responsible for examining the role of Federal information technology organizations and their future configurations and structure.

Michael Cronin, also of INS, serves as Assistant Commissioner for Inspections. He is responsible for program and policy development relating to INS operations at our Nation's ports of entry. He

is the principal point of contact between the INS and other Government agencies active at ports of entry as well as numerous foreign governments.

Stephen A. Edson from the State Department began his work with State in 1981. He now serves as the Acting Managing Director of the Visa Services Directorate with the Department's Bureau of Consular Affairs. He has served in the State Department all over the world, including Thailand, India, and Japan.

Mr. Benjamin Wu represents the Commerce Department. He is the Deputy Under Secretary for Technology at that department. In that role, he supervises policy development and direction among numerous Federal offices that work on technology policy, including the National Institute of Standards and Technology, which was directed in the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act to work with INS and the State Department to develop a biometric standard for immigration documents. Clearly, we want to know where that is today.

So if I might, perhaps I could begin with you, Mr. Hastings. If you gentlemen would confine your remarks to 5 minutes, go right down the line, and then we will be able to ask you some questions.

**STATEMENT OF SCOTT HASTINGS, ASSOCIATE COMMISSIONER FOR INFORMATION RESOURCES MANAGEMENT, IMMIGRATION AND NATURALIZATION SERVICE, WASHINGTON, D.C.; AND MICHAEL CRONIN, ASSISTANT COMMISSIONER FOR INSPECTIONS, IMMIGRATION AND NATURALIZATION SERVICE, WASHINGTON, D.C.**

Mr. HASTINGS. Madam Chairman, the INS has prepared a single statement and Mr. Cronin will summarize, so I will defer to him.

Chairperson FEINSTEIN. That is fine. Thank you.

Mr. CRONIN. Thank you, Madam Chairwoman, and Senator Kyl. Thank you very much for the opportunity to participate in this hearing concerning coordinated information-sharing among Federal agencies in the war on terrorism.

Since September 11, INS has witnessed an unprecedented increase in information flow among agencies. We strongly recognize our need for vital enforcement and intelligence data, and we are committed to providing accurate and timely immigration data to other agencies that require it.

We are also strongly committed to the use of this data in a fashion that improves the security of our borders, while limiting disruption to legitimate travel and trade. We appreciate the support and the leadership of the Congress for this information-sharing effort, especially as embodied in the USA PATRIOT Act and the Enhanced Border Security Act.

The Office of Homeland Security, in conjunction with the Office of Management and Budget, is leading critical initiatives to improve and monitor information-sharing among key Federal agencies, and to ensure the timely provision of critical data to State and local law enforcement and emergency management agencies. We are also working internationally to develop new and better ways of sharing information that will support intelligence and enforcement efforts.

INS has been engaged in broad-based information-sharing efforts since long before the terrorist attacks of September 11. For more than a decade, INS has joined with the U.S. Customs Service in development and management of the Interagency Border Inspection System, or IBIS, which is the principal border lookout system containing data from more than 20 Federal agencies, as well as real-time linkage to the National Crime Information Center, or NCIC.

Since the late 1990's, INS has been working with the Department of State to develop and expand the Data Share Project, under which visa data is transmitted electronically through IBIS to our ports of entry. In January 2002, the Consolidated Consular Data base was made available to ports of entry. Through use of this system, inspectors can access non-immigrant visa information, as well as a photograph of a rightful bearer of a visa.

Before and after September 11, INS has worked with the U.S. Marshals Service and the Federal Bureau of Investigation to include wanted persons' fingerprint data in the INS fingerprint system, IDENT. For nearly a decade, INS has received data from the State Department TIPOFF data base of suspected terrorists. Each of these systems and projects has led to significant enhancement of the security of our borders through the interdiction or apprehension of numerous terrorists and criminals.

Also related to and supported by the USA PATRIOT Act and the Enhanced Border Security Act are several key programs designed to manage and track the entry, stay, and departure of foreign visitors.

INS has formed an interagency project team with representatives from the Departments of State, Treasury, Transportation and Justice to effect the creation of the statutorily mandated entry/exit tracking system. This effort has led to implementation of electronic tracking of the arrival and departure of visa waiver program travelers as of October 1 of this year, with full implementation for all foreigners arriving by air anticipated as of January 1, 2003. This information will be fed automatically into the Arrival Departure Information System, ADIS, which will be the repository for arrival and departure data, eventually replacing the current non-immigrant information system.

INS has also very quickly implemented the National Security Entry/Exit Registration System, under which certain non-immigrant aliens who may potentially pose a national security risk are fingerprinted and interviewed upon arrival in the United States and registered periodically if they remain in the United States for a period of 30 days, and again if they remain for more than 1 year. Registration information is also updated in the event of changes of address, employment, or schools, and again upon departure from the United States.

The legislation we are discussing today mandates use of biometrics in various documents and processes. INS is awaiting the results of evaluation and development of biometric standards by the National Institute of Standards to proceed to develop approaches to this statutory direction.

In the interim, we are working with the Departments of Justice and State to design and evaluate processes and technologies which could potentially be used in the integration of biometric checks and

border operations. Next week, we will begin deployment of border-crossing card readers to selected ports of entry for test and evaluation prior to a large-scale procurement of readers for all ports of entry.

The INS has made significant progress in development and implementation of the Student and Exchange Visitor Information System, and we are confident that we will meet the January 1, 2003, deadline for full implementation established in the USA PATRIOT Act, with gradual, incremental implementation of use of this system by schools throughout 2003.

In May 2000, INS initiated a project to develop a business-driven enterprise architecture. The result is a multi-year modernization plan which provides a blueprint and build-out plan for modernizing information systems and technical infrastructure.

This clearly has been a broad brush over a great deal of activity in the area of systems development and information-sharing. Once again, we thank the committee for this opportunity to testify on these important issues and we welcome any questions.

[The prepared statement of Messrs. Hastings and Mr. Cronin appears as a submission for the record.]

Chairperson FEINSTEIN. Thank you very much. I appreciate it.

Mr. Edson, do you have comments?

**STATEMENT OF STEPHEN A. EDSON, ACTING DEPUTY ASSISTANT SECRETARY OF STATE FOR VISA SERVICES, BUREAU OF CONSULAR AFFAIRS, DEPARTMENT OF STATE, WASHINGTON, D.C.**

Mr. EDSON. Madam Chair, Senator Kyl, thank you for allowing me to speak this morning concerning the progress of the Department of State's efforts to implement the provisions of the Enhanced Border Security and Visa Entry Reform Act of 2002.

In implementing the immigration laws of the United States, the Department of State has no higher priority than our national security. We participate with the border security agencies and the broader law enforcement and intelligence communities in a wide range of activities, including but not to limited to the visa process, to ensure the greatest possible cooperation in our joint efforts to secure our borders and fight terrorism.

Although these relationships are longstanding, they have been significantly expanded in the past year. We are dedicated to meeting the opportunities provided by the Enhanced Border Security and Visa Entry Reform Act, both to build on our efforts to date and to break new ground in our common search for a safer United States.

In my written remarks, I have provided a comprehensive review of our efforts by section in the implementation of the Act. Now, I would like to just provide some highlights.

Significant progress has been made in the past year to increase the amount of information available to visa officers overseas, and conversely to INS and other law enforcement and intelligence agencies in the United States. The State Department's Consular Lookout and Support System, CLASS, is a principal example of this progress.

We have been able to leverage the provisions of the Enhanced Border Security Act and the USA PATRIOT Act to make CLASS an evermore effective tool for fighting terrorism. CLASS uses sophisticated search algorithms to match lookout information to individual visa applicants. Every single applicant is run through this system. CLASS is only as good, however, as the data it contains, and I am happy to report that post-9/11 this situation has improved dramatically.

CLASS records have doubled in the past year. More than 7 million names of persons with FBI records have been added to CLASS by August of 2002, augmenting the 5.8 million name records that we already had from State, INS, DEA, and intelligence sources. These NCIC records include the FBI's Violent Gang and Terrorist Data base, a particularly valuable resource.

Twenty thousand Customs serious violator name records have been added to CLASS since September 11, 2001. CLASS now has over 78,000 name records of suspected terrorists, up 40 percent in the past year. Most of this information has entered CLASS through TIPOFF, a program run through the Department's Bureau of Intelligence and Research that acts as a clearinghouse for sensitive intelligence information provided by other agencies. Since September 11, 2001, approximately 20,000 new terrorist lookouts have entered CLASS through TIPOFF alone.

Chairperson FEINSTEIN. Say that again, would you?

Mr. EDSON. Twenty thousand new entries into CLASS concerning terrorists that we have gotten through TIPOFF in the past year.

The State Department's CLASS lookout system has used for some time now linguistically sensitive algorithms for checking Arabic and Russo-Slavic names. A Hispanic algorithm is developed and ready for implementation, and an algorithm for East Asian languages is under study. We have been a leader in the development of linguistic logic for search purposes, and we are actively engaged with other U.S. Government agencies to help share this expertise as we work to expand those language algorithms.

The State Department currently shares electronic data with other agencies, including INS, and is rapidly expanding information-sharing arrangements through the law enforcement and intelligence communities. Our CLASS data base is already interoperable with the Interagency Border Inspection System, IBIS, that INS uses. In fact, we have been sharing information between CLASS and IBIS since 1995.

The Department's systems use open, flexible architecture consistent with industry standards in order to facilitate information-sharing. All non-immigrant and immigrant visa activities at all of our posts worldwide are replicated back to a consular consolidated data base in Washington at 5-minute intervals, providing the Department, INS, and other U.S. Government agencies with a near-real-time window into this work.

We in the State Department are actively participating in the design and the development of the Student Exchange and Visitor Information System, SEVIS, the permanent system that will contribute to our national security as it adds integrity to the student and exchange visa-issuing process.

At the same time we are working on SEVIS implementation in response to a separate legislative mandate, the Department has launched the Interim Student and Exchange Authentication System, ISEAS, which will provide for electronic verification of student and exchange visitor visas until SEVIS is fully implemented.

As of October 7, nearly 3,000 educational institutions and exchange program sponsors had entered approximately 72,000 records into ISEAS. Two hundred and thirteen visa-issuing posts around the world had used this system to verify 9,000 cases. ISEAS has provided both the Department and INS a better system to verify incoming foreign and exchange students until SEVIS becomes fully operational.

This concludes my testimony and I would be happy, of course, to take any questions.

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

Chairperson FEINSTEIN. Thank you very much.

Mr. Wu?

**STATEMENT OF BENJAMIN WU, DEPUTY UNDER SECRETARY FOR TECHNOLOGY, DEPARTMENT OF COMMERCE, WASHINGTON, D.C.**

Mr. WU. Good morning, Madam Chairwoman and Ranking Member Kyl. I appreciate the opportunity to update you on the Department of Commerce's implementation of the USA PATRIOT Act and the Enhanced Border Security and Visa Reform Act, of which the bulk of the work is performed by our Technology Administration's National Institute of Standards and Technology.

NIST is our Nation's oldest Federal laboratory and the only laboratory with the express mission of working closely with industry to develop measurements, standards, and a variety of technologies. Consequently, NIST has been working with the biometrics industry and other Federal agencies for years, and has especially been in very close collaboration over the past year in meeting its statutory requirements to develop a biometric standard for visas and passports.

In this Congress, Congress provided by statute appropriate tools required to intercept and obstruct terrorism in our country. These laws call for the Departments of Justice and State, working with NIST, to develop and certify technology standards to be used in visa control systems.

NIST has responsibility to develop and certify a technology standard that can be used to verify the identity of persons applying for a U.S. visa or using a visa to enter the country. The Department of Justice and the Department of State also expect NIST to certify the accuracy of specific government and commercial systems being considered for use in the visa system.

At this time, biometrics that are included in NIST studies are face and fingerprints, including the ten-finger rolled fingerprint system, the flat fingerprint matching system, and also a single flat fingerprint for verification as well as face-based verification.

NIST has received large-scale data bases from both the INS and the State Department, and is conducting tests to be used for set-

ting standards for certifying the accuracy of proposed fingerprint and facial biometric technologies.

NIST is also establishing interoperability standards for use between systems for both identification and verification functions. This is being done jointly with industry through the——

Chairperson FEINSTEIN. Can I just stop you there? We heard testimony, oh, maybe a year ago about all these biometric cards that went on to the border between our country and Mexico; I think 5 million, but no readers for those cards.

Is the biometric system that you are now talking about the same as the system that is on those cards, or is this a different one?

Mr. WU. The system that we are using could be used. My understanding is that it could be used for implementation with the system that we already have, but I am not clear as to whether or not it is the exact same system that you are referring to. But we can certainly check on that.

Chairperson FEINSTEIN. It seems to me you would want one system that is used all over so that all readers can gibe with the system.

Mr. WU. That is the goal ultimately to have one system that is interoperable that can be used with multi-systems, and ideally even using these standards and applying them internationally so we have a worldwide network for verification and authentication for visas and border control.

Chairperson FEINSTEIN. Please continue.

Mr. WU. Thank you.

This is being done jointly with industry through the International Committee for Information Technology Standard's Biometric Committee in trying to achieve this international interoperable standards system.

NIST has also contributed greatly in laying the foundation for interoperable data exchange for one of the primary biometric technologies, and that is fingerprint technology. NIST, working closely with the FBI, State and local law enforcement agencies, and product vendors of fingerprint classification systems, recently completed a joint American National Standards Institute, ANSI, and NIST standard for the data format for exchange of fingerprint information. This standard promotes the exchange of fingerprint data among different law enforcement agencies using systems from different vendors.

NIST is also spearheading the Face Recognition Vendor Test 2002 which is evaluating automated facial recognition systems that eventually could be used in the identification and verification processes for people who apply for visas who visit the United States.

The significance of the Face Recognition Vendor Test 2002 is evident by its large number of sponsors and supporters. This includes 16 Federal Government departments and agencies. The current evaluation builds on the success of NIST personnel who have had success in evaluating face recognition systems over the past decade.

This evaluation methodology developed for FRVT 2002 will become a standard for evaluating other biometric technology and we will learn precisely how accurate and reliable these systems are. Fourteen companies are currently participating in FRVT 2002, and we deliberately designed a tough test that involved matching ex-

tremely challenging real-world images that require participants to process a set of about 121,000 images and match all possible pairs of images to this image set. In other words, this required some 15 billion matches. As you can imagine, this generated a mountain of data and we are crunching all the numbers to see how well this system worked.

Also, open consensus standards and associated testing are critical to providing higher levels of security through biometric identification systems. Throughout the years, NIST has worked in partnership with U.S. industry and other Federal agencies to establish formal groups for accelerating national and international biometric standardization.

The Biometric Consortium which NIST is leading serves as the Federal Government's focal point for research and development testing, evaluation, and application of biometric-developed personal identification and verification technology. This Consortium has grown to more than 900 members, including 60 Government agencies. NIST and the National Security Agency co-chair the Consortium.

NIST has collaborated with the Consortium, the biometric industry, and other biometric organizations to create the CBEFF, the Common Biometric Exchange File Format. This format already is part of a Government requirement for data interchange and is being adopted by the biometric industry.

The specification is a candidate for fast-track approval as an ANSI standard and as an international standard for exchange by many types of biometric data files, including data on fingerprints, faces, retinas, palm prints, and iris and voice patterns.

Later this year, also, NIST expects to submit a report, as required by the Acts, on our work to the State and Justice Departments for transmittal to the U.S. Congress. The due date, I believe, is November 10. The report will make a recommendation on which biometric or combination of biometrics would best secure the Nation's borders. The report will also address interoperability standards and tamper-resistant standards.

Madam Chairwoman, I want to thank you and the committee for the passage of the Act, not just because it has made our country safer, but also it allows for NIST to cooperate closely with several Government agencies in the development of biometric standards and testing. This cooperation has really been successful and allowed for us to determine appropriate test scenarios for biometrics and exchange of very large data sets of fingerprints and face images obtained under operational conditions. As a result, we believe that the underlying science and technology for biometrics will greatly benefit, and the overall biometrics industry will also benefit as well.

We thank you and Congress for providing legislative tools to allow us to achieve this goal, and I thank you for the opportunity to testify this morning.

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

Chairperson FEINSTEIN. Thanks very much, Mr. Wu.

I am going to try and shorten my questions. I have a number of them and I think I would like to send them to you in writing, if I might, and hopefully you could respond within a week.

I have a big concern over the visa waiver program, largely because it is so huge. Twenty-three million people a year come in and I recognize why it is necessary. On the other hand, I recognize that it is a very easy thing to abuse.

Now, as I understand it, in our bill, by October 26, 2004, every person participating in the visa waiver program should have a machine-readable passport, I assume, with biometric data.

Will you meet that date? You are on the record, Mr. Cronin or Mr. Edson.

Mr. EDSON. Yes.

Chairperson FEINSTEIN. Say that, "yes."

Mr. EDSON. Yes. Many of the visa waiver countries have had machine-readable passport programs at varying degrees of implementation for some time now. We used the passage of the legislation to sort of heat up discussions with them on this issue.

The EU countries have indicated to us that they are planning on a uniform standard within the European Community for the biometric to be adopted. ICAO is proceeding apace with work on a sort of a triple standard, and it is our understanding right now that the ICAO members would be allowed to choose one of those three.

Although no one is committing to us to definite deployment plans right now in these foreign governments, it looks as if they will have some biometric that is accepted by ICAO within the time allotted.

Chairperson FEINSTEIN. Well, I might say both Senator Kyl and I worked very hard on some of these aspects of the bill and this is very important to us, so we are going to be watching with glasses on.

To what extent are you able to develop a pre-screening for visa waiver passport-holders so that you know who is coming into that program ahead of time?

Mr. CRONIN. If I may, Senator, basically that is done through the collection of data on departure by airlines. When flights depart for the United States, a manifest is provided to the U.S. Customs Service and to INS. We use the data provided while the flight is in the air to screen the names of the individuals on the flight to identify persons who may be the subjects of lookouts.

We do analysis on that data to identify persons who might fit broad criteria that would indicate that they should be examined more closely for criminal reasons, for terrorism reasons, for reasons relating to migration issues or customs issues.

Chairperson FEINSTEIN. Does the manifest alone contain sufficient data to do that?

Mr. CRONIN. It provides us the name, the date of birth, the nationality, passport number of the individuals who are coming, as well as other data.

Chairperson FEINSTEIN. And that is in operation now?

Mr. CRONIN. Correct.

Chairperson FEINSTEIN. And is it observed one hundred percent of the time?

Mr. CRONIN. I can't say we are at—we are very close to one hundred percent. Both INS and Customs are working closely with the

carriers to ensure that we are hitting one hundred percent as to both the data in the system and the accuracy of the data.

That is going to continue to be an issue. I mean, we will always be faced with keying errors to some degree in the check-in process or similar aspects of error that can't be avoided, but we are very, very close to a hundred percent in terms of working with the carriers.

Chairperson FEINSTEIN. That is good news.

Now, the 7.1 million non-immigrant visas—what is being done to assure that it is properly filled out, that it isn't falsified, and that the exit date is carried out?

Mr. CRONIN. In terms of departure data, we are basically using the same system of gathering data from the airlines to close out the departures of persons who have arrived. The data is all coming to us electronically based on airline manifests.

The way the system functions is the airline provides a departure manifest based on check-in information. They provide a subsequent departure manifest based on boarding gate information to verify that all persons that have checked in have, in fact, departed.

We are going to have to continue to work with the airlines in terms of the integrity of the system to ensure that there aren't elements of fraud introduced into the system, persons using other identities. At this point, we are still relying on provision of data from the airlines, albeit in electronic form.

Chairperson FEINSTEIN. At this point, it could all be fraudulent data.

Mr. CRONIN. Sure.

Chairperson FEINSTEIN. You would have no way of knowing?

Mr. CRONIN. We are relying on data provided at check-in to the airlines. The airlines are required to check documentation when the individual checks in. By and large, as part of the statutory scheme, they are required to check that documentation and we get that data from them.

I would distinguish, then, the national security entry/exit registration system where we are tracking select individuals. Those individuals on departure will be interviewed by an immigration officer. Their biometric will be verified against the data collected when they arrived and their departure will be recorded by an immigration officer. But, again, that is a select group of people that are subject to national security entry/exit registration.

Chairperson FEINSTEIN. I want to turn to Senator Kyl, but can you give me a percent compliance of the airlines with this?

Mr. CRONIN. I would prefer to go back and give that to you for the record. I am not sure off the top of my head that what I would give you would be accurate, but I am certainly happy to do that.

Chairperson FEINSTEIN. Fine, thank you.

Senator Kyl, I know you have to leave.

Senator KYL. Thank you, Senator Feinstein. I would like to submit some questions for the record to the entire panel here, but because of the timeliness of this article, I would really like to focus there.

Primarily, I suspect, Mr. Edson, these questions will go to you. You did not choose to be the subject of my questioning this morning and I don't mean this in any way personally, but I would like

to start by reading three paragraphs from the beginning of this article to set the stage for it.

"On June 18, 2001, Abdulaziz Alomari filled out a simple, two-page application for a visa to come to the United States. Alomari was not exactly the ideal candidate for a visa. He claimed to be a student, though he left blank the space for the name and address of his school. He checked the box claiming he was married, yet he left blank the area where he should have put the name of his spouse. This 'student' indicated that he would self-finance a 2-month stay at the 'JKK Whyndham Hotel' and evidently provided no proof, as required by law, that he could actually do so."

"Despite the legal requirement that a visa applicant show strong roots in his home country (to give him a reason to return from America), Alomari listed his home address as the 'AlQUDOS HTL JED,'" in Saudi Arabia. "Alomari didn't even bother filling in the fields asking for his nationality and sex, apparently realizing that he didn't need to list much more than his name to obtain a visa to the United States. He was right. He got his visa."

"When he arrived in the United States, he connected with his friend Mohamed Atta. And less than 3 months later, on September 11, he helped smash American Airlines Flight 11 into the north tower of the World Trade Center. Alomari never should have gotten the visa that allowed him to be in the United States on that day, and neither should at least 14 of the other 9/11 terrorists."

Now, I discussed in my opening statement some of the other facts that are in this story that relied upon the analysis of six experts, people who were in the State Department or INS looking at these applications. Their conclusion was unanimous that of those that they reviewed, none of the individuals should have been granted a visa.

With that as the background, let me just confirm some information and then ask the questions.

Is it correct that Section 214(b) has always been determined to create a presumption that the immigrant has the burden of proof of demonstrating that he will return to the country of origin and not remain in the United States?

Mr. EDSON. Yes, the non-immigrant visa applicant, yes.

Senator KYL. And I should have stated these are for non-immigrant visas, of course, yes.

And that is a relatively high burden that consular officers are trained to try to cause the applicant to meet?

Mr. EDSON. Yes.

Senator KYL. Ordinarily, with the kind of application that I read to you, if you assume those facts to be true, there should have been an oral interview, should there not, to inquire into the reasons why the information was left blank that was left blank and to inquire further as to what the applicant could say that would cause the consular officer to believe that he would return to Saudi Arabia?

Mr. EDSON. That is a harder question to answer just because we cannot tell from—well, we can't tell how much of the article is accurate at this point. I just read it this morning. But we also can't tell from looking at the applications whether or not an interview took place, whether or not additional evidence was submitted with

the application and returned to the applicant, questions asked over the phone and answered.

Senator KYL. That is unclear, although let me get back to my question. Ordinarily, wouldn't an application of the kind that I read you be followed up with an oral interview? The visa wouldn't just be granted on the basis of that information on its face, would it?

Mr. EDSON. Not on the basis of that information on its face.

Senator KYL. OK. If there had been an oral interview, wouldn't it be probable that that application, the two pages or the face page of it, would have had some notation of an oral interview?

Mr. EDSON. It should have. Our instructions would be that the officer should have annotated the application.

Senator KYL. OK, so either interviews were not held or the instructions to annotate the interview application were not done. In either case, the consular officers should have done something that apparently was not done, is that correct?

Mr. EDSON. Yes. They could have done what they did better, it seems.

Senator KYL. By the way, let me say I am not blaming any consular officers here. The article itself notes that they are not implicated in the problem. The problem was the culture that had been created by their superiors.

Since the time is getting beyond us here, let me turn right to the penultimate point I wanted to make that these individuals should be demonstrating that they have a means of financial support, that they have a destination in the United States that is clear, that they have a specific reason for being in the United States, especially if they are young, single men—and every one of these applicants were single and none was even 30 years old, by the way—and that they be able to demonstrate to the consular officers that they will, in fact, return to their country of origin, in this case Saudi Arabia.

Those are all of the kinds of things that the consular officers should have looked at, is that correct?

Mr. EDSON. Yes.

Senator KYL. Now, the last point that I want to make is this: According to the article—and I will ask you if you have any reason to believe that this is not true—the consulate in Jeddah where many of the terrorist visas were issued refused applications for fewer than 2 percent of the Saudi nationals in the 12 months prior to September 11, whereas the worldwide refusal rate for temporary visas is approximately 25 percent.

Do those numbers sound reasonable to you, or would you have any reason to know?

Mr. EDSON. We track refusal rates based on the source of the application, the nationality of the applicants, and the type of visa being issued. So it is very difficult to speculate and I would much rather answer in writing concerning the refusal rates because they could be comparing rates against two different populations.

Senator KYL. Sure. One thing I would like to ask is if you or someone at the Department could get these statistics for us and could respond to the allegations in the article as to whether or not these statistics are true or, if there are some other statistics, what they are. I think that would be very useful to us.

That answer probably then also applies to the 12 months following September 11, where the article asserts that according to documents bearing its letterhead, the embassy there in Saudi Arabia, the refusal rate for Saudi nationals in the 12 months following September 11 is a mere 3 percent. I gather you would have the same answer with respect to that.

Mr. EDSON. Yes. I need to check and see what they were counting.

Senator KYL. Just as a matter of visceral reaction, if these numbers are correct, would it seem to you that they are highly out of balance with the probability that Saudi nationals, especially those under 30 years of age, males, could prove a likelihood of returning to Saudi Arabia, that those numbers do seem to be out of balance?

Mr. EDSON. Not necessarily. Again, not knowing what we are counting, it is difficult to speculate. But remember that much of the population we are talking about is now subject to special additional screening procedures that have been put in place since September 11, much of it throughout the U.S. law enforcement and intelligence communities. So that the ultimate refusal rate might be in that neighborhood would not necessarily surprise me, but I don't know. We will have to check on the numbers for you.

Senator KYL. Well, let me just conclude, then, with this general question. Given the fact that all of these people were under 30, single males from Saudi Arabia—we were talking about the hijackers that caused the terror on September 11—and that so many of them, according to this article anyway, obtained a visa notwithstanding those facts and notwithstanding the kind of omissions that they article reported on their applications, would it not suggest to you a need for the State Department to immediately investigate what the practices of the State Department were at the time in that location, as well as other Middle Eastern countries that might be of concern to us, and to compare what the instructions are today to the consular officers with respect to how they handle such applications as a means of ensuring us that the State Department is on top of the situation and that its officers are making the right kinds of decisions with respect to people coming into this country on temporary non-immigrant visas?

Mr. EDSON. Yes. I do not agree with some of the conclusions reached by the article, but the important thing is just what you have just raised. The article raises the question that we have to ask ourselves constantly: Did we do the right thing and have we made changes since then to ensure that we are doing the best possible thing now in the visa process? That is what we do on an ongoing basis and that is what I hope that we do again in response to the article as we are looking to it and answering your questions.

Chairperson FEINSTEIN. The Senator is good enough to yield, and I would like to associate myself with his comments because I asked this question informally and I was told that every applicant goes through a special screening process now. If that is not true, then I would like to know it because I believe it should be and if we need legislation to accomplish it, we should do that.

Mr. EDSON. You are speaking to Saudi nationals?

Chairperson FEINSTEIN. In all these countries where there is a very real risk to the United States, every visa applicant from those countries goes through this special screening process.

Now, Saudi Arabia isn't on our list as a terrorist state, but maybe it should be.

Senator KYL. It is, is it not, one of the states that is subject to the special screening requirement, nevertheless?

Mr. EDSON. Correct. I assume we are talking about the visa Condor process which applies primarily to adult males in all of these states that we are talking about.

Chairperson FEINSTEIN. Every one should be specially screened.

Mr. EDSON. It doesn't apply to all of them. I ran some numbers yesterday and it is in the high 90's. The criteria are driven by intelligence community concerns and don't cover everyone as currently constituted.

Chairperson FEINSTEIN. Well, I think we need to take a look at that and see if we have some views.

Senator KYL. I concur with Senator Feinstein. I think probably with some of the questions that we will submit in writing, you can clarify some of this and we will probably need to have some additional oral testimony.

I would also like to conclude, if I could, by making one thing clear. This Section 214(b) does not relate to terrorism, per se. It rather is a standard part of our immigration policy to ensure that non-immigrant visas return to their country of origin. So this should have been standard procedure before September 11. It is not a terrorism-related filter for applicants, but rather one designed to ensure that people will comply with the laws of the United States when they seek to be our guests temporarily.

The reason this has such special meaning to me is that Senator Feinstein and I were the ones that prepared the Border Security Act and part of it was based upon testimony that we received in the Subcommittee. And I will never forget the testimony of Mary Ryan, who said we didn't have the information we needed to deny these visas.

She specifically talked about Mohamed Atta and I remember her saying it is like the person that hits the child who dashes out in front of the car in the school zone. You feel horrible about it, but there isn't anything you could have done about it.

But it appears to me that there was something that we could have done about it, not because of anything related to terrorism, but simply enforcing the laws of the United States of America. And had those laws been enforced, it is likely that most of the terrorists who committed the heinous acts of September 11 would not have been permitted into the United States, at least under the circumstances in which they were. They would have had to come back and complete their applications in a very complete way and demonstrate to consular officers that they were committed to returning to Saudi Arabia.

Of course, what they would be trying to prove is something that was utterly false, so that the likelihood is that consular officers being the good people they are would have found this out, discovered the problem, and never granted the visas to these people in the first instance.

If you have any comment, fine. It is not really a question. Again, Mr. Edson, I am in no way casting any aspersions upon you. You came here to represent the Department, really to deal with some other questions, but I hope that you will be a conduit of information because we need the answers from the State Department with respect to this.

I don't expect you to have those here this morning, but I would hope that you would be as upset as I am that when we talk about being able to prevent September 11, this perhaps could have prevented September 11 if we had just done our job, having nothing to do with terrorism, but just abided by the law of the United States. If consular officers had done their job, it is quite—and I shouldn't say "if our consular officers" because I am again not suggesting that they didn't do their job.

If the State Department had had the proper policies in place to be followed by its employees, it is possible that these terrorists would never have made it to the United States.

Chairperson FEINSTEIN. Thank you, Senator Kyl, and I know you are under time pressure. I am, as well, but I have four quick questions I must ask.

Let me just make a comment on this. One of the things that I really believe is true is that prior to 9/11 immigration policy in this country was really forged on humanitarian concerns, and then there were also economic concerns of facilitating travel. After 9/11, this has changed dramatically and national security concerns have to dominate.

So I think from the perspective of this Subcommittee which oversees technology and terrorism, and as that technology impacts each of your departments, the goal clearly has to be that national security is protected. If anybody errs, they have to err toward the conservative, not toward the other side.

I had taken a position early on in the student visa program and I have just four questions.

In the past year, how many schools have you investigated for fraud or violating the terms of the student visa program?

Mr. CRONIN. I don't know the answer to that, Senator. I would have to get that for you for the record.

Chairperson FEINSTEIN. I would like to have the answer.

How many schools have you dropped from the foreign student visa program after finding they were either sham operations, had fraudulently obtained student visas for persons not intending to attend classes, or had ceased operations?

Mr. CRONIN. Again, I apologize. That is not data that I have available.

Chairperson FEINSTEIN. How many cases of student visa fraud has the INS referred for further investigation or prosecution in the past 5 years?

Mr. CRONIN. I will have to get that for you for the record.

Chairperson FEINSTEIN. How many individuals have you deported in the past 5 years for foreign student visa violations?

Mr. CRONIN. Again, an answer I will have to provide for the record.

Chairperson FEINSTEIN. What type of institutions have you identified as high risk in terms of fraud and lack of compliance with the law?

Mr. CRONIN. I will provide that for the record, Senator.

Chairperson FEINSTEIN. What is the INS' timetable for conducting site visits to those institutions?

Mr. CRONIN. SEVIS is not under my responsibility. We will provide that answer for the record.

Chairperson FEINSTEIN. I understand, but these are the questions that we are going to ask about this program and we are going to ask them in the next 3 months, for the next 3 months. I am going to ask you to come back and I will give you a list of the questions, and I would ask you to answer them with specificity 3 months from today.

Mr. CRONIN. Absolutely.

Chairperson FEINSTEIN. Thank you very much. I thank everybody. This hearing is adjourned.

[Whereupon, at 12 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

United States Department of State

*Washington, D.C. 20520*

November 6, 2002

Dear Mr. Chairman:

Following the October 9, 2002 hearing at which Acting Director of Visa Services, Stephen A. Edson testified, additional questions were submitted for the record. Please find enclosed the responses to those questions.

If we can be of further assistance to you, please do not hesitate to contact us.

Sincerely,

Paul V. Kelly
Assistant Secretary
Legislative Affairs

Enclosure:
As stated.

The Honorable
Patrick Leahy, Chairman,
Committee on the Judiciary,
Subcommittee on Technology, Terrorism, and
Government Information,

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 1.a.:**

**Mr. Edson, to what extent is the State Department working with Visa Waiver countries to develop a pre-screening for visa waiver passport holders?**

Answer:

We are working with visa waiver countries, ICAO, and other federal agencies on initiatives to address our ability to pre-screen visa waiver passport holders.

The Visa Office of the Bureau of Consular Affairs works closely with federal inspection agencies (INS and Customs, in particular) in implementing the Advanced Passenger Inspection System (APIS), which is grounded in part in section 231 of the INA (as amended by Section 402 of the Border Security Act). We were observers at recent meetings where Customs and the airlines launched an enhanced APIS program. APIS provides advance passenger manifest information to the ports of entry prior to passengers' arrival. After the airlines transmit the biographic information on travelers to the U.S, but before they arrive at the port of entry, officials at the relevant

ports of entry screen the listed passengers, including VWP travelers. In conducting the prescreening, federal inspection officials check the State Department as well as the INS lookout systems. They regularly contact the Visa Office for further details on any travelers matching State Department lookouts.

The Passport Office and the Visa Office of the Bureau of Consular Affairs are active participants in the technical working group of the International Civil Aviation Organization (ICAO) focused on travel document standards and security. ICAO, the membership of which includes the United States and visa waiver countries, is working toward development of biometric standards for international travel documents, including passports and visas. We do not expect the ICAO biometrics standards to be formulated and voted upon prior to May 2003. Section 303(c) of the Border Security Act requires that visa waiver countries have programs in place by October 26, 2004, to comply with those ICAO standards, and that visa waiver travelers present passports that comply with those standards when entering the United States on or after that date (with an exception for passports issued prior to that date).

The Department of State also consults directly with the governments of visa waiver countries on a variety of issues in connection with the visa waiver program. The USA Patriot Act of 2001 requires that travelers from a visa waiver country use a machine-readable passport as of October 1, 2003 unless the Secretary of State finds that the country is making progress toward ensuring that machine-readable passports are available to its nationals and has taken appropriate measures to protect against misuse of non-machine-readable passports that it has issued. We are working closely with visa waiver countries on implementation of this requirement.

Our efforts to ensure that visa waiver country travelers present machine-readable passports and, ultimately, passports with ICAO approved biometrics are part of our effort to work with visa waiver countries to provide enhanced identity verification of visa waiver travelers, and improve the document interface of these travelers before they pass through APIS.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 1.b.:**

**To what extent are you finding that Visa Waiver countries are providing passports to non-citizens (for example, permanent residents and asylees)?**

Answer:

The extent to which they are doing so is very limited. The Department of State asked its embassies and consulates in visa waiver countries to approach host government passport authorities with this question and received the following information.

We have found no instance in which a visa waiver country issues regular (tourist) passports to people who are not citizens.

Some countries (including Belgium, France, Germany, Italy, Luxembourg, San Marino, Spain, and Uruguay) issue diplomatic or official passports to non-citizen spouses of their diplomats. The passports are typically limited to one-year validity, or at most to the duration of the spouse's tour abroad, and state the bearer's true

nationality, rendering the document invalid for visa waiver travel. In the case of Uruguay, the diplomat's spouse must have renounced his/her citizenship and be in the process of naturalizing as an Uruguayan in order to receive the passport.

Most visa waiver countries (including Denmark, Finland, France, Germany, Iceland, Italy, the Netherlands, Norway, Portugal, Singapore, and Switzerland) issue "travel documents," "alien passports," "immigrant passports," or similar documents to refugees, asylum seekers, or stateless persons with right of residence in the visa waiver country. Brunei plans to begin issuing such documents in the future, but has not yet established a date for doing so. These documents are usually for travel only to the issuing country, do not confer or connote citizenship, and usually do not resemble the issuing country's regular tourist passport. "Alien passports" or "immigrant passports" may be valid documents for visa issuance, but not for visa-free travel to the U.S.

Ireland, by statue, gives its Minister of Justice discretionary authority to issue Irish passports, leading to claims that Irish passports were "for sale." Although

the statute remains on the books, the practice was discontinued in 1998 and it is not thought that it will be reinstated.

In very limited circumstances, a non-Belgian being sent abroad by the government of Belgium on a diplomatic mission may be given a Belgian diplomatic passport for the duration of the mission. Belgian passport authorities have not yet identified the number of these types of diplomatic passports that have been issued, but do state that it is "very few."

The United Kingdom provides passports that distinguish between citizens (who may travel under the visa waiver program), and subjects, nationals, and citizens of dependent territories and overseas territories, most of whom are not eligible for the visa waiver program and must have visas to enter and remain in the U.K. People in Gibraltar and the Falklands are full British citizens.

We also know that at least some Italian diplomatic passports issued to non-Italian diplomatic spouses do not state the true nationality of the bearer.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 1.c.:**

**Do you believe such practices threaten the integrity of the visa waiver program? If so, what is the State Department planning to do to exercise more control over who is issued a passport from these countries?**

Answer:

As indicated in the previous answer, the issuance of passports by visa waiver countries to persons who are not their nationals is very limited. It is so limited, and done in such a way that we do not believe it threatens the integrity of the program. We find no examples of documents issued to permanent residents, refugees, or asylum seekers that confer or connote citizenship. None of these documents entitles the bearer to enter the U.S. under the visa waiver program. The practice appears limited to issuance of diplomatic passports by visa waiver governments to spouses of their own diplomatic personnel and a few exceptional cases to persons performing diplomatic missions for Belgium. Most diplomatic passports issued to spouses of foreign diplomats state clearly that the bearer is not a

citizen of that country, rendering the document invalid for visa waiver travel.

The one exception of which we are aware is Italy, where a few passports may not make the non-national spouse's true nationality clear. As a legal matter, were a diplomatic passport issued to a non-citizen spouse to neglect to state that the bearer is not a citizen of the issuing country, it still would not confer eligibility for visa waiver travel. While as a practical matter the INS would have difficulty identifying such persons unless they were asked about their nationality and explained the true circumstances, the real-world likelihood of this being an issue is extremely small. It must be evaluated in light of the facts that the individuals to whom the diplomatic passports have been given have an official relationship to the issuing government and that the visa waiver program is available only to persons entering in the "B" visa classifications (business and tourist), excluding the possibility of these passports being used by persons coming here in an official classification.

We believe that any concerns about the possibility that ineligible aliens might mistakenly enter the United States

on the visa waiver program when entering as tourists using diplomatic passports issued by visa waiver countries can be dealt with in a variety of ways. We can ask the countries concerned to inform their diplomats that this use of their diplomatic passports is not permissible; press them to ensure that such passports clearly distinguish non-nationals; and work with INS otherwise to address this remote possibility. Aside from these diplomatic passports, we have not identified any other issuance practices to non-citizens that would provide a vehicle for traveling impermissibly under the VWP.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 1.d.:**

**Are you finding that visa waiver countries are readily reporting instances of stolen or lost passports in a timely manner?**

Answer:

With regard to blank passport books, visa waiver program countries have regularly notified us of any losses, which we record in the Consular Lookout and Support System (CLASS) and pass to the Interagency Border Inspection System in near-real time. We also post lookouts on passports already issued to individual citizens and subsequently lost or stolen whenever they are reported to us by foreign governments or individuals. They are generally tracked by reports to our Embassies and subsequently entered into CLASS. We recently started sharing this data with the ports of entry.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 1.e.:**

**How quickly do you turn over such information to the INS and FBI?**

Answer:

With regard to blank passport books, reports either from U.S. Foreign Service posts abroad or from foreign government representatives in the U.S. are sent to the Visa Office's Information staff, which generally enters the data into the Consular Lookout and Support System (CLASS) on the same day reports are received. The data then passes into the Interagency Border Inspection System (IBIS), used primarily by federal inspection services including INS, in near-real time. With regard to lost or stolen individual passports, our Foreign Service posts receiving reports from individuals or foreign governments have the ability to enter the passport information directly into CLASS. CLASS data entered by posts is replicated to Washington every five minutes, and thence passed to IBIS in near-real time.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
By Senatar Kyl
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

Question 1:

The Border Security Act directs the Attorney General and Secretary of State to issue machine-readable, tamper-resistant biometric visas by October 26, 2004. Please provide an update on the timeline for meeting this deadline.

Answer:

Global deployment of a program for a visa that uses a biometric identifier other than a digitized photograph (which we have already incorporated into our visa) is a formidable challenge because non-photographic biometrics have never before been used on such a scale. The program will entail over 7,000,000 annual biometric enrollments of visa applicants, with enrollment operations in almost every country on earth. In the five months since adoption of the Border Security Act on May 14, 2002, the Department of State has invested much time and effort in considering how to meet this challenge.

Section 303 of the Border Security Act calls for the Secretary of State, the Attorney General, and the National Institute for Standards and Technology (NIST), acting

jointly, to submit to the appropriate committees of Congress by November 10, 2002, a comprehensive report assessing the actions that will be necessary, and the considerations to be taken into account, to achieve fully, not later than October 26, 2004, the implementation of that section of the law, which requires the issuance of machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. Representatives from the Department of State, the Department of Justice, and NIST have been meeting regularly to draft the required comprehensive report. We expect the report to provide a detailed exposition of the issues involved in using biometric identifiers with the full range of covered travel documents by the October 26, 2004, deadline.

Question for the Record submitted to
Acting Deputy Assistant Secretary Stephen A. Edson
By Senator Jon Kyl
Senate Judiciary Subcommittee on Technology,
Terrorism, and Government Information
October 9, 2002

**Question 2 :**

**Several months ago, the State Department conducted a staff briefing on Border Security Act requirements, including the biometric requirement for October 26, 2004. The State Department indicated in that briefing that "all nonimmigrant visas incorporate a photo that can easily be matched by INS inspectors to the database record that is available at all ports of entry." How, in the absence of reliable data capture by a U.S. Government entity, does the State Department assert that a non-digitized photograph used for nonimmigrant visas meets the biometric features requirement intended by the authors of the Border Security Act?**

Answer:

When we **indicated in that briefing that "all nonimmigrant visas incorporate a photo that can easily be matched by INS inspectors to the database record that is available at all ports of entry," we were referring to a** digital image photograph that can be and is transmitted electronically from visa issuing posts to both State and INS, to be available at all ports of entry. This visa datashare system became operational in December 2001, before the Border Security Act, but does represent an important step toward use of biometrics in visas, as contemplated by the Act. (The Department does not regard non-digitized photos as

meeting the intent of the Border Security Act.) Visa datashare, by which nonimmigrant visa issuance data is replicated from Foreign Service posts around the world directly to computers in Washington on a real-time basis (updated every five minutes), has vastly increased the security of the nonimmigrant visa. Since it became available to INS at ports of entry, this system has allowed INS inspectors to detect numerous cases of visa fraud by comparing the person presenting the visa, and the photo in the visa as presented at port of entry, with the digitized photograph incorporated into the visa when it was issued. We would be pleased to demonstrate how this system functions, and we will contact your staff to arrange a demonstration for interested parties.

For most posts, electronic visa records are available from 1996 to the present. Currently, the Consular Consolidated Database contains over 50,000,000 records of NIV data, and approximately 16,500,000 have photographs included in the record.

**Hearing before the**
**Senate Committee on the Judiciary**
**Subcommittee on Technology, Terrorism and Government Information**
**On**
**"Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland"**

**Wednesday, October 9th, 2002**
**10:00 a.m., Senate Dirksen Building, Room 226**

**QUESTIONS SUBMITTED TO PANEL II**
**BY SENATOR DIANNE FEINSTEIN**

**1. *BIOMETRIC STANDARD***

The USA Patriot Act and the Enhanced Border Security and Visa Entry Reform Act required the establishment of a biometric standard that could be shared by the INS, State Department and other relevant federal agencies. While the National Institute of Standards and Technologies (NIST) is the lead agency for this endeavor, and Mr. Wu's testimony alludes to the pending report due in November, I understand that certain biometric identifiers have been ruled out for consideration.

Reportedly, NIST decided not to consider, for example, biometric standards for hand geometry identification despite the unqualified success of INS' INSPASS system for trusted travelers over a five-year period.

***QUESTIONS:***

**a. Mr. Hastings, could you explain why the INS did not ask NIST to consider hand geometry as an identifier?**

***ANSWER:*** Although hand geometry has worked well for INS Passenger Accelerated Service System (INSPASS) in a one-to-one matching mode, it is not a unique enough biometric to be used in a one-to-many matching mode. Our understanding is that NIST is investigating biometrics that can be used in both a one-to-many and one-to-one matching mode.

**b. Mr. Wu, can you tell us why voice recognition technology is not among the biometric identifiers for which NIST will propose technology standards?**

**PANEL II:**
**QUESTIONS FOR**
**SCOTT HASTINGS AND MICHAEL CRONIN,**
**IMMIGRATION AND NATURALIZATION SERVICE**

**2. *BIOMETRIC IDENTIFIERS***

One of the most profound lessons we have learned since 9/11 is that a lack of communication can have deadly consequences. No single database can be as effective as one that is connected to other federal agencies or law enforcement authorities. Linking these technologies to lookout systems and law enforcement databases would enable your agency as well as law enforcement agencies to screen foreign nationals more closely and identify and apprehend those who pose a threat to national security.

***QUESTION***

**What is INS doing to link the biometric data and technologies to other databases and criminal lookout systems?**

***ANSWER:*** INS has been building on integrating systems and information both before and since since 9/11 through the following efforts:

- Department of State and INS implemented DataShare for Non Immigrant Visas (NIV) in December 2001. Visa issuance data including a photograph is available in the Interagency Border Inspections System (IBIS) for use in secondary inspections for NIVs issued since December 1, 2001.

- The Federal Bureau of Investigations (FBI), US Customs Service (USCS) and INS worked together to implement the Advanced Passenger Information System (APIS) Interstate Identity Index (III) queries. This project queries non-US Citizen APIS passengers against the National Criminal Information Center (NCIC) III criminal history records in addition to the NCIC wants and warrants checks that are done for every APIS query. It was first implemented at Washington Dulles International Airport in July 2002 and has an aggressive national deployment schedule which includes training from the FBI on fingerprint code identification.

- Since August of 2001, fingerprints of U.S. Marshall Service (USMS) wanted fugitives began to be systematically entered into the INS Automated Biometric Identification System (IDENT) criminal database. The FBI wants and warrant information was soon added as well. In thirteen months, this program alone has resulted in over 3,000 INS apprehensions of fugitive aliens.

- The IDENT/IAFIS Integration program will complete its third phase in the Spring of 2003. Phase One provided selected INS sites with the capability to perform independent fingerprint capture and checks of the INS IDENT database and of the FBI IAFIS

database. Phase Two is currently being deployed. This phase introduces a small form factor fingerprint scanning device, replacing the large, proprietary fingerprint capture machine. Phase Three is currently moving from the design to the development stage, intended for Spring 2003 deployment. This phase builds on the small form factor scanner introduced in phase two and combines the scanning function for an integrated fingerprint capture session which spawns searches of both IDENT and IAFIS database and returns results to the same workstation.

- INS continues to work with Department of State (DOS) on the Laser Visa program. These existing systems check applicants for a Border Crossing Card against the IDENT databases to identify criminal behavior. If no "hits" are detected, the DOS, at their discretion may issue the card to an individual. This year, the number of applications in the Laser Visa database exceeded five million.

- The NEXUS program was implemented in the Summer 2002. This program provides a Border Crossing Card to Canadian and US citizens passing between these two countries. Canadian Immigration and US INS records are checked prior to issuing this card.

### 3. *ENTRY-EXIT SYSTEM*

Section 302 of the Enhanced Border Security Act requires the implementation of an integrated Entry and Exit data system. Under the law, the Attorney General is required to develop an automated entry-exit system at all air and sea ports of entry by December 31, 2003; at the largest 50 land ports-of-entry by the end of 2004; and at all land ports-of-entry by December 31, 2005.

***QUESTIONS***

a. **Mr. Hastings, can you provide a more detailed description of the progress the INS has made in implementing this system? For example, what are the INS' plans and schedule for fully implementing the entry-exit system?**

***ANSWER:*** The INS continues to work towards the dates mandated by the statute in order to establish an automated entry-exit system. In order to effect the creation of an integrated entry-exit system in a timely manner, the Immigration and Naturalization Service established an interagency project team, comprised of members from the Departments of Justice, State, Treasury, and Transportation. The U.S. Entry Exit Program is a joint effort by these Departments whose intent is to significantly improve the processes, policies, workforce, and systems utilized to manage the pre-entry, entry, stay, and exit of international travelers through over 300 ports of entry (POE).

The interagency team has completed a Concept of Operations document and is working on a Business Case, which includes a Cost Benefit Analysis, Feasibility Study, Risk Assessment and Acquisition Strategy. Additionally, the Program has already begun to address specific policy and process-related requirements through the National Security entry exit registration System (NSEERS) project to better track nonimmigrant aliens from certain designated countries.

b. **What are the greatest challenges and risks facing the INS in meeting the timeframes? And, what is the INS doing to address these challenges and/or mitigate these risks?**

***ANSWER:*** With a Continuing Resolution in effect no funds have been appropriated to fund the entry-exit program. To mitigate risks, the INS continues to move forward with providing a spending plan to Congress. The INS briefed the Government Accounting Office on October 28, 2002 to present the adopted spending plan. Dependent upon an approved budget the INS is prepared to issue a Request for Information (RFI) to solicit information from contractors as an exploratory request to identify capabilities, interest, market information and contractor capabilities. Information gathered from the RFI will help resolve concerns regarding the feasibility of the requirements, integration of the various technologies and other industry concerns or questions related to this acquisition.

c. **What are some of the main obstacles to ensuring that the all INS officers at the ports of entry and District Office personnel in the interior have the right hardware, software and sufficient training to be able to obtain critical information about a visa applicant for a foreign national seeking entry into the United States?**

***ANSWER:*** Coordination of timelines and timely funding are critical for successful implementation of an entry exit system. The INS has an overall plan to upgrade all ports-of-entry with appropriate equipment (hardware and software) and provide training to field personnel.

d. **What plans does INS have to test the entry-exit system? What are the estimated costs of developing and implementing the entry-exit system?**

***ANSWER:*** The INS is diligently following the Systems Development Life Cycle (SDLC) process, which serves as the basis for the development of both functional and technical requirements, for implementation of the entry exit system. The estimated FY03 costs are $380M.

*5. **ENTRY-EXIT SYSTEM***

Mr. Cronin, my staff has met with several immigration inspectors who have expressed concern that the computer lookout systems at the ports-of entry are not always operational, often because the INS computer network is down. Therefore, they are unable to run name checks on individuals as they seek entry into the U.S.

***QUESTION:***

a. **Could you please explain why this is occurring and what the INS intends to do to ensure that all Immigration Inspectors have access to these critical databases at all times?**

*ANSWER:* The networks used at Ports-of-Entry are largely controlled and maintained by the United States Customs Service, which is responsible for ensuring functionality of the system. Few systems work continuously, without interruption, however, the INS has put into place procedures, and trained its staff at Ports-of-Entry, to address outages and ensure that applicants for admission are properly queried against critical databases.

**6. *FOREIGN STUDENT VISAS***

Schools are quickly approaching the time by which they will need to be ready to implement SEVIS -- the foreign student tracking system. Yet, they do not have all the information needed from the INS, such as the final rules on F and M visas, or draft rules from the State Department on J visas. The INS has pointed out that since draft regulations on the F and M visas are available, schools have a "roadmap." But this does not take into account the comments that schools have submitted to improve the tracking system. Nor does it provide concrete, specific guidance for the schools.

Regarding the J visas, final regulations may not be available until after the schools are required to be in compliance with SEVIS.

***QUESTIONS:***

a. **Mr. Hastings, what is INS' timetable for issuing final regulations on the student tracking system?**

*ANSWER:* The regulations governing the F and M programs were issued as proposed rules in May of this year. We have reviewed and addressed the comments, and the final regulation was published on December 11, 2002. The regulations governing the J programs are within the purview of the Department of State, and have been published as interim final regulations on December 12, 2002.

b. **Once the final regulations are issued, how much time could you reasonably expect a school to fully understand its obligations under the regulations, obtain the necessary software that links into the SEVIS system, and obtain and train the necessary personnel to enter the foreign student data into the system?**

**In other words, do you believe you are giving the educational schools a fair shot at complying with the foreign student tracking system requirements when it is already October and these schools still do not have clear guidelines as to their obligations under the law?**

*ANSWER:* The schools have seen the proposed SEVIS regulations since May of 2002. These set forth the program requirements, and INS has testified that the proposed rules are a very good blueprint for understanding the program. Moreover, SEVIS program information has been available to schools on the INS website, and since July 1, 2002 the system for F and M students has been available, first to selected schools, and then to all schools for use. The system is easy to use, and the information schools must collect has not changed substantially from the information

schools have always been required to keep. The difference is that the school must now enter that information into an Internet website, instead of keeping it in a paper file. Access to the system requires a simple Internet connection.

We are confident that a school that wants to participate in SEVIS can do so, and we stand ready to assist them. Congress mandated the implementation of the SEVIS program by January 1, 2003, and given that, we all must do our best to meet the deadline.

## 7. *FOREIGN STUDENT VISAS*

The INS has had more than a year's notice that Congress wanted the agency to meet the statutorily mandated deadline for getting the student tracking system up and running. That deadline is January 2003. Last year, Commissioner Ziglar indicated that the INS was in the process of developing and deploying the foreign student tracking system. At that time, he also indicated that the agency would need an appropriation up-front to move forward with the tracking system's implementation.

Congress provided the INS the $38.6 million the Commissioner said he needed to get the system in place by January 30, 2003.

*QUESTIONS*

**a. Why has it taken a full year before the INS has issued final regulations?**

*ANSWER:* Implementation of a program like SEVIS by January 2003 was an ambitious undertaking. We happily can report that we will make the deadline. The regulations are but one part of a comprehensive program, and they have been scheduled to fall in place as needed to implement the program in time to meet the January 2003 deadline. The regulations for F and M students were published as proposed regulations in May of 2002. The regulations were long and detailed and they brought much public comment. INS has spent the summer reviewing the comments, addressing them and changing the regulation as appropriate. During this same period, we issued an interim rule for SEVIS preliminary enrollment and a separate interim final rule to implement the full school certification part of the foreign student program. It was important for these rules to be promulgated first, so that the review and certification of schools could be underway well before the January 2003 deadline. Also during the summer months, we deployed the two major SEVIS software modules dealing with F and M students. Concurrently with promulgation of enrollment and certification rules, establishing the school certification process, and the F and M software deployment, we also finalized analysis of comments and drafting of the final rule for F and M students, which was published December 12, 2002. We also are in the final stages of drafting a student fee regulation, and a rule to govern the withdrawal and denial of school certifications to participate in the program. Given the variety of rules needed, the demands of developing and deploying the software, and the non-system program needs such as training and outreach, we are proud of our ability to keep everything on schedule.

**b. Have you worked out a process by which larger universities, such as the University of California, can enter data on foreign students using batch files, rather than**

**entering information of hundreds of students one-by-one, which I imagine would be time consuming and inefficient?**

***ANSWER:*** Yes, we have made this capability available. Batch processing requires two sides to participate as partners. We published in the Commerce Business Daily and sponsored multiple vendor conferences to specifically provide SEVIS technical specifications for batch-interface as soon as practical (San Diego, CA (August 28 to 30, 2001) and Charleston, SC (September 4 to 6, 2001)). Furthermore, we sponsored an additional technical conference in the Washington, DC metropolitan area (June 13, 2002). We have published our specifications for batch processing on our website, first for comment and then as final specifications. As a result of discussions with the University of California (UCLA), we added two user-defined fields so that schools could input their own student identifier, or other element, to assist their system and business processes. INS made its side of the batch-processing mode available to schools for testing on September 23, 2003. As of October 1, 2002, we made our actual batch capability available for any school that completes testing. We are working with the schools to help them in their testing process. As an example of our coordination with schools and their software vendors, we have been working with a major university in their batch test effort. As of October 24, 2002 this university and its software vendor successfully tested all of the SEVIS batch functionality. This university's software vendor will likely take lessons learned and be able to provide functioning batch software to the other 1,000+ schools that utilize the same software product that will batch interface with SEVIS.

c. [*if yes:*] **Have you begun testing the batch processing module to minimize the potential data problems schools could encounter after the January 30, 2003 implementation deadline?**

***ANSWER:*** INS tested its side of the batch-processing module internally with our prime contractor. Next, the software was independently tested before it was made available on October 1, 2002. The INS and the SEVIS software follows best practices and adheres to Software Development Life Cycle (SDLC) provisions. Schools that are interested and ready with their own side of the process have been able to send test data to us since September 23, 2003. We are working with schools on batch testing to identify and repair any deficiencies on our side of the batch partnership before January 30, 2003. Moreover, because the January 30 deadline only involves new I-20s issued after that date, the schools may have time after January 30, 2003 to perfect their batch capabilities. Again, schools will have to make individual determinations about whether and when to implement batch processing.

d. **To what extent have you reached out to the smaller schools and begun training their officials to use the SEVIS system?**

***ANSWER:*** During the past year INS has conducted at least 90 outreach sessions for schools. These sessions were in locations throughout the country and widely attended. Over 3,000 schools were represented and over 5,000 school officials attended these sessions. Since July of this year, when SEVIS first became available, we changed our focus from generalized outreach to helping actual users. We do this primarily through a robust call center, dedicated specifically for SEVIS, that is available to all schools as they apply to use the system and throughout their use of

SEVIS. In addition to the call center, which is available to all schools, without regard to size or type of program, we have developed, and will continue to develope training materials to help users. These materials include a training DVD, as well as the INS website. We believe that our focus on assistance for actual users is particularly helpful for smaller schools that may not be able to attend conferences.

e. **I imagine that schools across the country will have numerous technical and operational questions about the SEVIS electronic system. Do you plan to set up regional meetings with the schools so they can ask questions about how to properly implement the program at their schools? If so, when? If not, why not?**

***ANSWER:*** As mentioned above, INS has conducted many regional meetings over the last year. Our present focus is to help users individually through our call center, which is very robust and designed precisely to help schools with technical and operational questions. Nonetheless, we continue to participate in regional meetings as time permits. For example, working with the American Council on Education, we have planned to staff four regional meetings in early February of 2003 to assist schools as they begin to use the system.

**8. STUDENT VISA FRAUD**

***QUESTIONS***

a. **In the past year, how many schools have you investigated for fraud or violating the terms of the student visa program?**

***ANSWER:*** INS Investigations has a system to track its formal fraud investigations, but it does not have a separate category for student or school fraud. In their tracking system student/school fraud would fall under the much broader categories of "status violators" or "benefit fraud."

While we do not have a mechanism for providing exact numbers to answer your question nationwide, we can tell you that INS has engaged in significant fraud detection efforts and initiated fraud investigations in the student and schools arena over the past year. For example, in February 2002 the Enforcement Operations Division of the Vermont Service Center completed a "Summary and Analysis of Student Fraud for F1 Students." Because of the nature of Service Center work, this analysis focused on applicants for a change of status to F1 student, and the schools involved with such transactions. The analysis included the random sampling of 270 change of status petitions filed in the Vermont Service Center, a review of nine investigative and/or intelligence reports about student/school fraud issued since 1998, forensic examination of documents and contact with numerous schools about individual cases. As a result of the Vermont analysis, at least six targets were identified for further investigation. In a similar vein, in response to recent inquiries, the Texas Service Center was able to report to us about eight ongoing or very recent fraud investigations involving students or schools, and the California Service Center reported ten. We do not present this information as a comprehensive tally of activity in the area, but rather as a sampling of the kind of activity that has taken place this year.

b. **How many schools have you dropped from the foreign student visa program after finding that they were either sham operations, had fraudulently obtained student visas for persons not intending to attend classes, or had ceased operations?**

***ANSWER:*** The Student/Schools database (the predecessor to SEVIS) contains some data about schools that have been "withdrawn" from the program by INS, but it does not contain the reasons for withdrawal. The database reflects that 14,678 schools were withdrawn from the system from 1983 to the present.

c. **How many cases of student visa fraud has the INS referred for further investigation or prosecution in the past five years? How many individuals have you deported in the past five years for foreign student visa violations?**

***ANSWER:*** As noted above, INS investigators do not separately track school or student fraud. There have been referrals and prosecutions for fraud related to the foreign student visa program in the past five years, but the Service does not have specific data whether they involve students or schools.

d. **What type of institutions have you identified as "high-risk" in terms of fraud and lack of compliance with the law? What is the INS' timetable for conducting site visits to those institutions?**

***ANSWER:*** INS has not yet identified any institutions as high risk, although our recently published school certification regulation requires us to do this in order to set priorities for our site visits to schools. We have engaged a contractor to collect data to help us to set such risk criteria. The contractor's report is due shortly, and based upon this data we intend to develop our criteria. Our school certification regulation states that we will conduct site visits to all technical, flight and language schools prior to their enrollment in SEVIS, and we would expect at the very least to visit any other schools that fall into a high risk category prior to their enrollment in SEVIS. For schools that apply by November 15, these site visits will be completed before January 30, 2003.

## 9. *INSPECTOR GENERAL'S CONCERNS ABOUT INS IMPLEMENTATION OF FOREIGN STUDENT TRACKING SYSTEM*

At a recent hearing in the House Judiciary Subcommittee on Immigration, Border Security and Claims, the Department of Justice Inspector General, Glenn Fine, expressed the following concerns about the INS' implementation of the foreign student tracking system:

- First, he doubted that the INS can complete the site visits and certification of flight, vocational, language and other high-risk schools before the January 2003 deadline;

- Second, he expressed concern about the INS' ability to adequately train and oversee the contractors who will be conducing the site visits--he believes the INS needs to develop an oversight process that will ensure the adequacy of these reviews;

- Third, the INS had not agreed to devote full-time personnel in the INS districts to SEVIS; without such personnel, the INS will not be able to devote adequate attention to their foreign student tracking duties when other priorities arise;

- Fourth, the INS must provide SEVIS training to INS adjudicators, inspectors, and investigators; and

- Finally, while the INS has held SEVIS demonstrations for school officials, these sessions were not necessarily attended by officials from smaller schools, including flight schools, who are probably in most need of training.

***QUESTION***

a. **Mr. Hastings and Mr. Cronin, could you please explain how the INS intends to address those issues?**

**First, the IG doubted that the INS could complete the site visits and certification of flight, vocational, language and other high-risk schools before January 30.**

***ANSWER:*** INS has engaged the services of three investigative contractors with nationwide networks of employees to conduct site visits of schools. November 15, 2002, was the date set by our school certification regulation, by which a school must apply to use SEVIS, if they wanted to be assured that INS would act upon their application by January 30, 2003. We had estimated this to be no more than eight thousand schools based upon the number of schools that have issued I-20 forms to students over the last three years. As of December 17, 2002, 1,562 schools have been approved to use SEVIS, and so far, only 3,227 schools have submitted their petition for SEVIS access and are under review. We believe that we have sufficient investigative resources on call to complete as many as 15,000 site visits. Accordingly, we believe that the Inspector General's doubts are unwarranted in his assessment and that we will complete the investigations by January 30, 2003.

**Second, the IG expressed concern about the INS' ability to adequately train and oversee the contractors who will be conducting the site visits – he believes the INS needs to develop an oversight process that will ensure the adequacy of these reviews.**

***ANSWER:*** The INS does intend to oversee the contractors who will conduct the site visits. First, we began by developing a checklist to guide contractors through their site reviews. We have met with the contractors on several occasions to explain and plan for the work, and now that the work has begun, we receive copies of all the contractor reports both in the District Offices, where the school application is adjudicated, and INS Headquarters, where we receive the reports for purpose of monitoring quality and performance. We think that we have a responsible plan that can be modified as necessary to ensure that we receive investigations that meet our needs given the limited allotted time.

**Third, the INS has not agreed to devote full-time personnel in the INS districts to SEVIS. Without such personnel the INS will not be able to devote adequate attention to their**

**foreign student tracking duties when other priorities arise.**

***ANSWER:*** The Service believes that the IG's recommendation that INS devote full-time personnel in the field to SEVIS is focused upon the old system rather than the new system. We intend to do much of the fraud detection, data mining, monitoring of school compliance, review of trends and administration of SEVIS centrally, with a staff in headquarters. While there always will be some role for field personnel, we expect the field role to ebb and flow depending upon the program needs. For example, during the period of initial certification of schools, the program will require a tremendous effort by the District Office personnel to review school applications and site review reports. Once this effort is completed, the District role will subside substantially, only to increase again at the two-year mark, when the recertification of schools is undertaken. The Executive Associate Commissioner for Field Operations issued an August 2002 memorandum, directing District Offices to ensure that they devote adequate resources to the SEVIS program, particularly during this period of school certification. We anticipate that in many Districts, this initial effort will require the full-time efforts of more than one person and the EAC's memo demonstrates that we are willing to commit the resources to this program that it needs. However, once the initial certification process is completed, we anticipate a substantial decline in work that needs to be completed in the field. Thus, we do not believe full-time personnel in the field would be a responsible allocation of limited human resources. District managers will have the flexibility to deploy resources were they are most needed at any particular time.

**Fourth, The INS must provide SEVIS training to INS adjudicators, inspectors and investigators.**

***ANSWER:*** We agree that training is an essential and ongoing element of any program. We have conducted training, and will continue to conduct more as the program progresses. We have focused our initial training on the adjudicators, who have the early role of conducting the school certification program. We held two training sessions for these individuals, who we believe are well trained to handle their initial program responsibilities. We have conducted some preliminary training sessions with both inspections and investigations personnel, and we are in the process of engaging a contractor to develop web-based training modules that we can use to train various categories of employees and users of SEVIS. More is always better, and we are doing as much as resources permit. When the student fee is in place and producing revenue, and we have initial deployment of the system and certification of schools behind us, we will be able to accomplish much more in the realm of training and monitoring.

**Finally, while the INS has held SEVIS demonstrations for school officials, these sessions were not necessarily attended by officials from smaller schools, including flight schools, who are probably most in need of training.**

***ANSWER:*** We are aware of the limitations of large outreach sessions and demonstrations. For this reason, in July of 2002, we changed our school support strategy to move away from large conferences, and toward individual user support. We are doing this through a very robust user call center, and the development of training materials such as a training DVD and detailed user

manual. Moreover, we have insisted upon site visits for schools in part because we want to establish a support presence in each school, and assess their training and other needs. Finally, as mentioned above, we are in the process of engaging a contractor to develop web-based training for school users, and we have under consideration a certification program for Designated School Officials before schools are recertified at the two-year mark.

**10. *INSPECTOR GENERAL'S CONCERNS ABOUT INS IMPLEMENTATION OF FOREIGN STUDENT TRACKING SYSTEM***

The Department of Justice Inspector General, Glenn Fine, observed in the same hearing that for SEVIS to be fully implemented and for the program to succeed, the INS must--

- ensure that all high-risk schools are certified through site visits by January 30;
- dedicate sufficient resources to adequately training INS personnel and school officials;
- ensure that SEVIS is available at all ports of entry, INS service centers, district offices and consular posts;
- ensure that information from SEVIS is analyzed and used to identify non-compliant and fraudulent operations; and
- follow up when the SEVIS data indicate fraud in the program.

***QUESTION:* Do you agree with this assessment? If so, what steps is the INS taking to meet these objectives?**

***ANSWER***: We generally agree with the Inspector General on these program objectives. We have described above in detail our plans for certification of schools, including high risk schools, and our training plans. SEVIS is available to authorized users through any personal computer that can access the Internet. In addition to internet access, INS has worked to arrange for data sharing with the Entry and Exit system and consular posts, to ensure that SEVIS information is available where it needs to be. We have made plans for the SEVIS program office to include a data analysis unit that will review and mine data on a regular basis. The SEVIS team is also working with INS Investigations to establish protocols for the handling of fraud and noncompliance referrals. The building of our fraud detection and investigation capacity will depend in part upon the implementation of our student fee, and future reprogramming and budget requests.

**11. *FOREIGN STUDENT TRACKING SYSTEM***

***QUESTION:***

**a. As currently devised, will a school be able to enter into the SEVIS tracking system information pertaining to a student's failure to enroll or decision to drop out of the institution?**

*ANSWER:* Yes. Schools will be required to enter a student's failure to enroll or decision to drop out of the institution.

**b. If such information is entered, what happens next? For example, how soon after such information is entered will the proper INS authorities become aware of the student's failure to show up for classes?**

*ANSWER:* School officials are required to report in the system a nonimmigrant student's failure to enroll within 30 days of the end of the registration period. Additionally, to enhance security of the system, if a student is not registered in the system as being enrolled, the system will automatically indicate that the student has failed to register and make that information available to the appropriate INS office. Authorized INS officers have direct access to SEVIS via the Internet or INS intranet, so will not need to wait or process through extra steps in order to access the data. INS will have access to the information and the ability to review much sooner than in the past. The system provides query functionality and also provides reports available to the appropriate INS enforcement offices.

**c. What kind of resources does the INS currently have to follow up on such a lead and investigate the student's whereabouts?**

*ANSWER:* To respond to this challenge the INS Investigations Program currently has less than 2,000 special agents Service-wide, including supervisors and managers. Since September 11, 2001 a significant number of productive agent hours have been dedicated to national security issues.

Therefore, resources are clearly an issue. Many of the cases we pursue are critical and must be carefully prioritized, balancing available resources with the nature of the violation, and/or the threat to public safety and national security. These cases include smuggling, trafficking, criminal aliens, Joint Terrorism Task Force, investigations, benefit and document fraud, and much more. It is not unusual for the same case to cover more than one of these categories.

Currently, the INS' Investigations Program devotes approximately 7% of investigative staff hours to "immigration status violators," including students. We are developing a prioritization hierarchy for referrals from the SEVIS system and forwarding the leads to the appropriate INS investigative unit or field office for assignment. The INS Investigations Program does not have resources solely dedicated to respond to every SEVIS status violator.

**12. *VISA WAIVER PROGRAM***

The Visa Waiver Permanent Program Act requires the Attorney General to develop and implement a fully automated entry-exit system that will collect records of arrival and departure for every alien from a visa waiver country who arrives or departs the United States by air and sea, no later than October 1, 2002.

***QUESTION:***

**a. What is the status of INS' implementation of the visa waiver entry-exit system?**

***ANSWER:*** The INS published the Visa Waiver Permanent Program (VWP) requirements regulation for 8 CFR 217 (interim rule with comments). The regulation was published on Friday October 11, 2002. Currently the INS has just begun evaluating and reviewing the VWP departure data. In a preliminary report (October 2, through October 9) of 192 air carriers that have submitted arrival data, only 15 carriers do not have departure data (13 of these carriers are charter flights). The INS will notify the air carriers that have not complied.

The INS has begun evaluating the vessel information. The majority of the vessels are transmitting the arrival and departure information. The carriers are submitting the electronic arrival and departure information for all passengers for compliance with section 402 of the Border Security Act.

**b. How will this system be integrated into the entry-exit system?**

***ANSWER:*** Currently the VWP Program is using existing systems such as, Interagency Border Information System (IBIS), Advance Departure Information System (ADIS) and Advance Passenger Information System (APIS). These systems will be integrated with the other arrival and departure systems.

**c. Is the INS currently entering data on lost or stolen passports into its lookout databases, as mandated by the Border Security Act?**

***ANSWER:*** Yes. The INS is currently entering reported lost and stolen passports into databases to prevent unauthorized use of such documents.

**13. *VISA WAIVER PROGRAM***

Last year, in his testimony before this subcommittee, Department of Justice Inspector General, Glenn Fine, observed that INS inspectors typically have, on average, less than one minute to check and decide whether to admit a foreign national into the U.S. He also found that INS inspectors did not query all visa waiver passport numbers against the INS' computerized lookout system. In addition, he noted that terrorists, criminals, and alien smugglers have attempted to gain entry into the United States through the Visa Waiver program.

***QUESTIONS:***

a. **The Border Security Act requires the INS to enter stolen passport numbers into a lookout data system within 72 hours of notification of loss and theft. Is that process now under way?**

***ANSWER:*** Yes. INS is in compliance with the 72 hour mandate of the Act.

b. **Given that immigration inspectors are the principal means of preventing illegal entry under the Visa Waiver program, what steps is the INS taking to ensure that immigration inspectors check passport numbers against information in a lookout data system?**

***ANSWER:*** In April 2002, the INS placed stickers upon computers used in primary inspection reminding immigration inspectors about performing such queries, emphasized the steps to perform these queries in trainers-training (held in April, 2002) and issued guidance to the field reiterating the importance of this part of the inspection process. The stickers read as follow:

"Intercepts Save Lives"
Query passports using IBIS in this order:
1. Perforated Document Number, **OR**
2. Pre-Printed Document Number, **OR**
3. Assigned Passport Number/MRZ

(IBIS refers to the Interagency Border Inspection System)

## 14. *ENTRY-EXIT SYSTEM*

On September 11, 2002, the INS rolled out the National Security Entry-Exit Registration System (NSEERS), the first phase of the congressionally mandated entry-exit system. Upon entry, the system will match the fingerprints of certain nationals against databases of known criminals and suspected terrorists.

***QUESTIONS:***

a. **Which legislative requirements does NSEERS address?**

***ANSWER:*** The NSEERS is authorized by the Immigration and Nationality Act, sections 262 and 265, as indicated in the Federal Register, Vol. 67, No. 114, dated June 13, 2002. The NSEERS will be integrated into the congressionally mandated Entry Exit System.

b. **What is the current status of NSEERS? Where is equipment to run the system being deployed?**

***ANSWER:*** The deployment schedule for the NSEERS application was developed according to a prioritization, with information supplied by the Office of Statistics, on the anticipated volume of

registrants. Adjustments have been made in the deployment schedule where the actual volume of registrants was greater or less than the projection. To date the NSEERS application has been deployed nationally to all sites, which includes the Ports-of-Entry, District Offices, and Sub Offices, with either new workstations or an NSEERS application CD.

**c. What kind of training is being done at the Ports-of-Entry?**

***ANSWER:*** The INS Training Office developed NSEERS training for the Inspections Officers at Ports-of-Entry using multiple delivery methods. We have Instructor-led trainings that walk Inspectors through the NSEERS procedures and the automated system functions. We have scenario-based training exercises that use a computer training database. Training was provided to a cadre of INS Trainers from every region and they are responsible for delivering it to their colleagues at their Ports-of-Entry. We also built a web-based training tool to support all INS personnel implementing NSEERS. This material is available on the INS Intranet and includes "Frequently Asked Questions," policy memorandums, and other guidance. To date there have been a total of 1,423 personnel trained from Inspections, Adjudications, Investigations, and Deportation.

**d. Do all Ports-of-Entry have access to databases, such as IDENT, needed to mach travelers' fingerprints?**

***ANSWER:*** Currently all major Ports-of-Entry have access to the databases necessary to match information presented by a special registrant. Once deployment is completed, all Ports-of-Entry will have access.

**e. Do all ports have the capability to electronically register travelers into NSEERS, or are some doing this manually?**

***ANSWER:*** As deployment has been executed, electronic registrations have increased. The Service intends all sites to have the capability to register applicants electronically. Manual registration is utilized as a back-up procedure for all ports. Manual registration forms are faxed and originals FedExed to a data entry site. Some sites will continue to use manual procedures until the deployment is completed.

## 15. *ENTRY-EXIT SYSTEM*

Current immigration law does not require all travelers, such as U.S. citizens and Canadian nationals, to present documentation when entering the U.S. at land border ports-of-entry. A concern that has been raised is that foreign nationals might falsely claim U.S. or Canadian citizenship and circumvent the entry-exit system.

***QUESTIONS:***

**a. What changes, if any, to immigration law may be required to address this potential limitation of the entry-exit system?**

***ANSWER:*** In general, United States immigration laws require all travelers, including United States citizens who are returning and Canadian citizens who are entering, to present documentation when coming into the United States. In the case of United States citizens, there is a current exemption to the requirement at section 215(b) of the INA that "[e]xcept as otherwise approved by the President . . ." all United States citizens must bear a valid United States passport when departing from or entering the United States. Currently, by State Department regulation, there is an exemption to this passport requirement for United States citizens when traveling to the United States from foreign territories within the Western hemisphere. That exemption could be rescinded by either Presidential Order or rescission of the State Department regulation. Moreover, it is noted that even with the current exemptions, United States citizens returning from travel in foreign countries within the Western hemisphere are not exempt from presenting other, albeit less secure, documentation, such as drivers license, or birth certificates, to establish identity.

The waiver for Canadian nationals from the visa and passport requirements arises from authority of the Secretary of State and the Attorney General under section 212(d)(4)(B) to waive the passport and/or visa requirements of section 212(a)(7)(B)(i)(I) & (II). The waiver was implemented by joint regulation of the Department of State and Department of Justice at 22 C.F.R. § 41.2 and 8 C.F.R.§ 212.1(a). While the INS Data Management Improvement Act of 2000 (DMIA) contains a prohibition on the imposition of new documentary or data collection requirements on any person in order to satisfy the DMIA, including implementation of the entry/exit system, the statute also specifically states that, "nothing in [the DMIA] shall be construed to reduce or curtail any authority of the Attorney General or the Secretary of State under any other provision of law." Thus, if the Attorney General and the Secretary of State determine that visas and passports are necessary in order to implement laws other than DMIA, such as other provisions of the INA, it would be legally permissible without a change in legislation.

**b. What administrative changes could be made to plug this potential vulnerability?**

***ANSWER:*** As noted above, potential vulnerabilities arising from current exemptions could be addressed by: 1) in the case of United States citizens, issuance of Presidential Order or State Department regulation rescinding the exemption for passports for travel to the United States from a foreign country within the Western hemisphere; 2) in the case of Canadian nationals, revision of the regulations establishing waiver of the passport and visa requirement.

## 16. ***ENTRY-EXIT SYSTEM***

At pedestrian lanes at Ports-of-Entry, INS has installed document readers to electronically scan documents, such as some passports.

***QUESTIONS:***

**a. Does the INS plan to install document readers at vehicle inspection lanes?**

***ANSWER:*** Not at this time. However, the INS and U.S. Customs Service will be deploying readers at one site to test and evaluate the concept.

**b. What would be the pros and cons of such action, including the costs of implementing it and its potential impact on inspection time?**

***ANSWER:*** The advantage would be the ability to determine with certainty that the individual presenting the document is the rightful owner of the card. The disadvantage is that this could result in unnecessary delays that may be caused by the increased processing times. The results of the test and evaluation will allow INS and USCS to answer these types of questions in a more complete manner.

**Hearing before the**
**Senate Committee on the Judiciary**
**Subcommittee on Technology, Terrorism and Government Information**
**On**
**"Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland"**

**Wednesday, October 9th, 2002**
**10:00 a.m., Senate Dirksen Building, Room 226**

**QUESTIONS SUBMITTED TO PANEL II**
**BY SENATOR JON KYL**

**Questions for INS:**

**1.) a.) Scanners/Readers for Border Crossing Cards and b.) October 26, 2004 Border Security Act requirement that scanners be in place at all ports of entry to read biometric visas and other documents:**
**After 1) all the money spent to actually manufacture the replacement laser visas (to replace the non-secure border crossing cards), 2) readying consular posts in Mexico and other satellite locations for application processing, and 3) after the Congress appropriated $11 million last year to provide enough funding to install readers at all Southwest and other relevant ports -- the INS has not installed any of these readers? Why? My staff informs me that INS staff indicated that there have been procurement problems and that the $11 million was only supposed to fund a pilot project. In a meeting on Capitol Hill last May, Commissioner Ziglar told me that the scanners/readers would be *fully* installed at all relevant ports (not as a pilot project) by the end of this year. Please comment on this information. Also, please provide an update on the requirement that biometric readers be installed at all ports of entry by October 26, 2004.**

**Answer:** The INS sought to procure 30 biometric verification systems to conduct a pilot to evaluate the optical stripe reader's effectiveness, the ability of its software to successfully read and match the biometrics embedded, and operational feasibility.

The INS notified Congress that a pilot of the system would be conducted during the Fall of 2002. Seventeen vendors stated that they could meet INS requirements stated in the request for proposal. Based on those responses, INS decided to proceed with a competitive bid. During the period of comment, prospective vendors requested the dissemination of the firmware, encryption, and drive technology that reads the information stored on the BCC and the Permanent Resident Card (PRC). However, the need to maintain security and integrity of the security features of these documents has prompted concerns. The encryption, firmware, and drive configuration information is not classified but is highly sensitive. The INS decided to require a pre-award demonstration, to ensure that participating vendors could actually meet the technical and security requirements of this program before releasing the encryption firmware.

The pilot is comprised of field and laboratory tests, conducted by the Space and Naval Warfare System Center, San Diego (SPAWAR), an independent contractor. The SPAWAR will conduct tests, gather the metrics, and evaluate the concept of BCC Biometric Verification Systems (BVS) at different inspection ports-of-entry and climatic environments. Included in this phase are the acquisition of the systems and testing of stand alone secondary BVS. The pilot will consist of 30 optical stripe (laser card) readers and biometric verification systems at various INS inspectional environments. The sites include small, medium and large land and air Ports-of-Entry. The designated ports are Los Angeles, San Ysidro, Nogales, Falcon Dam, San Antonio, and Atlanta.

If the BCC pilot and concept evaluation are successful, the BVS will begin deployment along the Southwest Border and ports-of-entry with high BCC traffic or fraud.

One of the components of the Entry Exit Project is the deployment of equipment and software to allow biometric comparison and authentication of US visas, and other travel and entry documents that use biometric identifiers. A comprehensive report assessing the actions that will be necessary, the considerations to be taken into account, and the expected costs of such a deployment will be delivered to Congress as expeditiously as possible.

**2.) <u>The Border Security and Visa Entry Reform Act's Chimera, the interoperable data system:</u> The Border Security Act requires a) the INS to fully integrate all of its databases and systems that contain information on aliens and b) requires the system to be a component of the government-wide interoperable system called Chimera (an update on Chimera is due on October 26, 2002). In addition, a Commission on Interoperable Data Sharing is required to be in place by October 26, 2002. In the Supplemental Appropriations bill that passed a few months ago the Justice Department/INS was given the authority to draw down from its "Working Capital Fund" (a technology fund) in order to produce a report on its plan for developing Chimera. It is my understanding that a report on the development of interoperable system is due in March 2003. Has INS used any Capital Working Fund funding to produce this report? How is this being coordinated with the Entry-Exit system development? Where is INS in producing its seamless technology system that will be coordinated with Chimera? The INS, reportedly, continues to develop a program called ATLAS, the purpose of which is to produce a seamless system but for which Congress has had no oversight. How much INS information technology funding has INS spent on ATLAS? Why haven't members been assigned to the Commission on Interoperable Data Sharing been named?**

**Answer:** The 2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States (P. L. 107-206 and the accompanying House Report (H. Rpt. 107-593) directed the Department of Justice, "to develop a plan regarding the INS 'Chimera' system for review by the Committees on Appropriations, as directed in the Senate report." Specifically, H. Rpt. 107-593 provided the following direction:

"The conference agreement also includes language that funds shall [be] derived from the Working Capital Fund to develop a plan regarding the INS `Chimera' system for review by the Committees on Appropriations, as directed in the Senate report. This project shall also be managed by JMD [Justice Management Division]. The conference agreement also adopts Senate direction regarding a briefing on lessons learned on the implementation of the Trilogy program. Centralizing the management and implementation of these systems will ensure that they will be interoperable and accessible by other relevant Federal agencies."

To date, the Justice Management Division has contracted for an independent assessment of INS information technology (IT) systems. Specifically, the contractor will document current INS IT system capabilities and shortcomings, analyze and document opportunities to leverage technical solutions developed or lessons learned, and assess the INS Atlas Program. As directed by Congress, funding has been allocated from the Working Capital Fund to finance this study.

The contractor's assessment of Chimera is scheduled to be delivered in January 2003. The report will include some general projections for the implementation of Chimera, but not a fully developed implementation plan. After we have had an opportunity to review the results of this study with the Committees on Appropriations, we will solicit their direction on how we should proceed and the extent to which the Department of Justice should continue its involvement with this project, especially in view of the transfer of INS to the Department of Homeland Security.

**3.) Justice/INS was appropriated $5.75 million in the last July's emergency supplemental bill to integrate the FBI's "most wanted list" fingerprint system, the Integrated Automated Fingerprint Information System (IAFIS) with the INS' IDENT system. Please provide an update on the progress INS has made in installing IDENT systems at ports and in integrating IDENT and IAFIS.**

**Answer:** The FBI's "Most Wanted List" has been integrated into IDENT. Approximately 91,000 FBI NCIC fingerprint records were entered into the IDENT Lookout database. U.S. Marshal fugitive records were entered as well. These records are updated on a bi-weekly basis. Since August of 2001, when this initiative began, over 3,000 fugitive aliens have been apprehended by INS agents.

The IDENT/IAFIS Integration program will complete its third phase in the Spring of 2003. Phase One provided selected INS sites with the capability to perform independent fingerprint capture and checks of the INS IDENT database and of the FBI IAFIS database. Phase Two is currently being deployed. This phase introduces a small form factor fingerprint scanning device, replacing the large, proprietary fingerprint capture machine. Phase Three is currently moving from the design to the development stage, intended for Spring 2003 deployment. This phase builds on the small form factor scanner introduced in phase two and combines the scanning function for an integrated fingerprint capture session which spawns searches of both IDENT and IAFIS database and returns results to the same workstation.

**4.) Congress is poised to appropriate some $360 million to the Justice Department in FY 2003 for the entry-exit system. During the past year, in supplemental appropriations bills, Congress has provided over $14 million for the development of the entry-exit system. When will the overall entry-exit system be deployed at all of our nation's ports? Will it be developed concurrently with the development of the interoperable data system?**

**Answer:** The following deadlines are mandated:

| | |
|---|---|
| October 1, 2002: | VWPPA at air and sea POEs |
| December 31, 2003: | DMIA integrated Entry Exit System at air and sea POEs |
| December 31, 2004: | DMIA system at 50 largest land POEs |
| December 31, 2005: | DMIA system at all POEs |

The entry exit system design must incorporate the various system development phases to fit within the projected timelines. The phases will consist of detailed design, development, implementation, testing, and quality assurance. To the greatest degree possible, the system will leverage the utility of existing legacy systems. The system will be based on an open architecture approach, promoting interoperability and commonly accepted industry standards.

**5.) A report due on November 14 of this year, to be written jointly by INS, NIST, and the State Department, will assess actions necessary for full 1) implementation of biometric visas and 2) installation of equipment and software at all U.S. ports that read and authenticate biometric documents. I will also ask your counterparts here today from NIST and the State Department B will this report be completed on time, and can you tell me what it will say?**

**Answer:** The report will cover the reporting requirements of section 303a of the Border Security Act and section 403c of the Patriot Act. We believe a single report best responds to the reporting requirements outlined in the legislation because the issues to be covered are so closely aligned. The Department of Justice Chief Information Officer has taken the lead role in preparing the report together with representatives from the Department of State, the National Institute of Standards (NIST), the Immigration and Naturalization Service (INS), the Federal Bureau of Investigation (FBI), and the Office of Homeland Security (OHS) to provide a joint response to the Congress.

**Responses to Questions from**
**October 9, 2002 Hearing**
**Regarding**
**"Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland"**
**Before the**
**Senate Judiciary Subcommittee on Technology, Terrorism and Government Information**

---

**Responses to Senator Dianne Feinstein's Questions:**

b. *Mr. Wu, can you tell us why voice recognition technology is not among the biometirc identifiers for which NIST will propose technology standards?*

Due to the time constraints imposed by the Patriot and Enhanced Border Security acts, biometrics to be initially tested and certified by NIST as being highly accurate must conform to certain conditions. First, any biometric to be considered must be an available and established technology. Second, the captured biometric image outputs from the biometric devices must be available to NIST. Finally, large-scale databases of realistic samples must be available for testing.

Biometric accuracy determination requires the use of large-scale databases for testing in order to capture the variation in subject population. Large realistic test samples of face and fingerprint images were obtained by NIST from the State and Justice Departments. These samples were obtained from operational, rather than laboratory, settings. The scale of these tests is significantly larger than any tests previously published. At this time, only fingerprints and face recognition biometrics are included in the NIST accuracy certification studies; iris-based technology was not included due to the lack of an iris database of sufficiently large sample size.

Fingerprints and faces are also the first two biometrics tested by NIST because there exist large legacy databases with which to compare new subjects for identification during enrollment. Both the INS and the FBI have large fingerprint databases to check for criminal records. The Department of State has large databases of visa face images and fingerprints. In addition, within the intelligence community, facial data is often the only biometric data that has been and is currently being captured. Face data is one key source for "watch lists," and in many situations fingerprint data cannot even be captured to use in constructing a "watch list."

The Border Security Act states that countries that participate in the visa waiver program must incorporate biometric standards consistent with the International Civil Aviation Organization (ICAO). It is therefore desirable that any biometrics used by the INS or State Department also be consistent with ICAO standards. ICAO biometrics standards include only face, fingerprint, and iris.

NIST has not considered hand geometry for several reasons. First, NIST was informed by the INS that they do not plan to continue working with hand geometry because of the identification requirements required for travel documents. Second, hand geometry is not included in the ICAO international standards. Third, no attempt to use hand geometry for large scale identification has ever been tested operationally. INSPASS is a verification system without identification capability.

Voice recognition technology is not currently being considered by NIST for several reasons. First, there are no large-scale sample databases available to NIST. Second, voice biometrics does not fit within the existing legacy databases available to the State and Justice Departments. Finally, voice biometrics are not included in the ICAO international standards.

**Question Submitted to Ben Wu**

*1.* ***Biometric Technology***

*a. What factors led NIST to determine that combination was the most reliable form as opposed to others in today's biometric technology market?*

*b. How would this biometric standards work in conjunction with other law enforcement databases such as FBI fingerprint systems?*

Due to the time constraints imposed by the Patriot and Enhanced Border Security acts, biometrics to be initially tested and certified by NIST as being highly accurate must conform to certain conditions. First, any biometric to be considered must be an available and established technology. Second, the captured biometric image outputs from the biometric devices must be available to NIST. Finally, large-scale databases of realistic samples must be available for testing.

Biometric accuracy determination requires the use of large-scale databases for testing in order to capture the variation in subject population. Large realistic test samples of face and fingerprint images were obtained by NIST from the State and Justice Departments. These samples were obtained from operational, rather than laboratory, settings. The scale of these tests is significantly larger than any tests previously published. At this time, only fingerprints and face recognition biometrics are included in the NIST accuracy certification studies; iris-based technology was not included due to the lack of an iris database of sufficiently large sample size.

Fingerprints and faces are also the first two biometrics tested by NIST because there exist large legacy databases with which to compare new subjects for identification during enrollment. Both the INS and the FBI have large fingerprint databases to check for criminal records. The Department of State has large databases of visa face images and fingerprints. In addition, within the intelligence community, facial data is often the only biometric data that has been and is currently being captured. Face data is one key source

for "watch lists," and in many situations fingerprint data cannot even be captured to use in constructing a "watch list."

The Border Security Act states that countries that participate in the visa waiver program must incorporate biometric standards consistent with the International Civil Aviation Organization (ICAO). It is therefore desirable that any biometrics used by the INS or State Department also be consistent with ICAO standards. ICAO biometrics standards include only face, fingerprint, and iris.

NIST has not considered hand geometry for several reasons. First, NIST was informed by the INS that they do not plan to continue working with hand geometry because of the identification requirements required for travel documents. Second, hand geometry is not included in the ICAO international standards. Third, no attempt to use hand geometry for large scale identification has ever been tested operationally. INSPASS is a verification system without identification capability.

Not all subjects can be easily fingerprinted with existing technology under the wide range of conditions expected in the entry/exit system. Tests by NIST using INS data show that for approximately 2% of the fingers in the INS database, the friction ridges are too damaged to be matched with existing technology. The proposed system requirements therefore include both fingerprint and face biometrics. NIST measurements indicate that a dual biometric system including two fingerprint images and a face image is needed to meet projected system requirements.

The FBI's IAFIS (Integrated Automated Fingerprint Identification System) is intended to be used for criminal background checks for obtaining Visas and other travel documents. Previous work on fingerprint identity searches by Mitretek Corp. has shown that adequate identification can be obtained using the IAFIS. In this study, at least four fingers are required to perform identification on a database of 40 million individuals.

For identification checks using the IAFIS, fingerprints will be submitted to the FBI using the ANSI/NIST standard, *Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information* (ANSI/NIST-ITL 1-2000). This standard formats fingerprint data to perform background searches against the FBI or another Automated Fingerprint Identification System's (AFIS) criminal file. This standard is perfectly consistent with the fingerprint portion of the biometric standard recommended by NIST.

**Responses to Senator Jon Kyl's Questions:**

1. *Congratulations on near completion of the technology standard for biometric identifiers. Experts in this field, and admittedly neither I nor my staff is such an expert, have asked why biometric standards were not considered for hand geometry identification (despite its reported success in the INS INSPASS system) or for voice recognition technology. Please provide me with an update on the development of biometric standards.*

Due to the time constraints imposed by the Patriot and Enhanced Border Security acts, biometrics to be initially tested and certified by NIST as being highly accurate must conform to certain conditions. First, any biometric to be considered must be an available and established technology. Second, the captured biometric image outputs from the biometric devices must be available to NIST. Finally, large-scale databases of realistic samples must be available for testing.

Biometric accuracy determination requires the use of large-scale databases for testing in order to capture the variation in subject population. Large realistic test samples of face and fingerprint images were obtained by NIST from the State and Justice Departments. These samples were obtained from operational, rather than laboratory, settings. The scale of these tests is significantly larger than any tests previously published. At this time, only fingerprints and face recognition biometrics are included in the NIST accuracy certification studies; iris-based technology was not included due to the lack of an iris database of sufficiently large sample size.

Fingerprints and faces are also the first two biometrics tested by NIST because there exist large legacy databases with which to compare new subjects for identification during enrollment. Both the INS and the FBI have large fingerprint databases to check for criminal records. . The Department of State has large databases of visa face images and fingerprints. In addition, within the intelligence community, facial data is often the only biometric data that has been and is currently being captured. Face data is one key source for "watch lists," and in many situations fingerprint data cannot even be captured to use in constructing a "watch list."

The Border Security Act states that countries that participate in the visa waiver program must incorporate biometric standards consistent with the International Civil Aviation Organization (ICAO). It is therefore desirable that any biometrics used by the INS or State Department also be consistent with ICAO standards. ICAO biometrics standards include only face, fingerprint, and iris.

NIST has not considered hand geometry for several reasons. First, NIST was informed by the INS that they do not plan to continue working with hand geometry because of the identification requirements required for travel documents. Second, hand geometry is not included in the ICAO international standards. Third, no attempt to use hand geometry for large scale identification has ever been tested operationally. INSPASS is a verification system without identification capability.

Voice recognition technology is not currently being considered by NIST for several reasons. First, there are no large-scale sample databases available to NIST. Second, voice biometrics does not fit within the existing legacy databases available to the State and Justice Departments. Finally, voice biometrics are not included in the ICAO international standards.

# SUBMISSIONS FOR THE RECORD

**STATEMENT OF**

**MICHAEL CRONIN**
**ASSISTANT COMMISSIONER FOR INSPECTIONS**

**AND**

**SCOTT HASTINGS**
**ASSOCIATE COMMISSIONER FOR INFORMATION RESOURCES MANAGEMENT**
**AND DEPUTY CHIEF INFORMATION OFFICER**

**U.S. IMMIGRATION & NATURALIZATION SERVICE**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**
**SUBCOMMITTEE ON TECHNOLOGY, TERRORISM**
**AND GOVERNMENT INFORMATION**
**UNITED STATES SENATE**

**REGARDING**
**IMPLEMENTATION OF THE ENHANCED BORDER**
**SECURITY ACT AND**
**THE PATRIOT ACT**

**226 DIRKSEN SENATE OFFICE BUILDING**

**WEDNESDAY, OCTOBER 9, 2002**
**10:00 AM**

GOOD MORNING MADAM CHAIRWOMAN, AND MEMBERS OF THE SUBCOMMITTEE. I appreciate the opportunity to participate in this hearing concerning coordinated information sharing among Federal agencies in the war against terrorism. Since September 11, we at the Immigration and Naturalization Service (INS) have seen an unprecedented sharing of data and knowledge among federal agencies.

Congress signaled its support for these efforts by enacting the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act (P.L. 107-56) which became law on October 26, 2001, and the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173) which became law on May 14, 2002. As you know, this legislation requires the INS to fully integrate all of its databases and data systems that process or contain information on aliens. This integration will become part of the interoperable electronic system, called Chimera. When completed, Chimera will provide current and immediate access to information in law enforcement and intelligence databases relevant to determine whether to issue a visa and to determine the admissibility of an alien.

The INS is one of the core agencies that require enhanced information sharing capabilities. We need to tap into additional external sources of data to support our enforcement and intelligence functions, and we recognize that the data we collect can be crucial to the law enforcement and intelligence communities to combat the threat of terrorism. Efforts to improve the quality and timeliness of information access will strengthen our ability to prevail against the threat of terrorism while limiting the disruption to legitimate commerce that might otherwise arise.

Madam Chairwoman let me begin by describing some important things we are already accomplishing to meet these challenges. As you know, the Office of Homeland Security, in conjunction with the Office of Management and Budget, is overseeing initiatives that promote information sharing between Federal agencies horizontally, and then from those agencies to State and local governments. We also are working internationally to develop better ways of sharing information that will support international enforcement and intelligence operations.

I cannot over-emphasize the commitment of the INS and other participants to work together in order to achieve a more supportive and comprehensive information environment. Prior to September 11, the INS shared data in many ways with other agencies in support of law enforcement efforts. Since then we have redoubled our efforts to contribute data and information that have supported counter-terrorism intelligence, investigative, and enforcement operations.

For many years, the INS has taken steps to enhance the exchange of information through greater cooperation among the law enforcement community. As early as 1985, the INS was sharing vital information with the U.S. Customs Service through the Interagency Border Inspection System (IBIS), the primary automated screening tool currently used by Customs and the INS to which many Federal agencies contribute lookout information. Since that time, we have put in place a number of other initiatives to exchange information with other entities, which are in various stages of implementation.

For example, in October 2001, INS Commissioner James Ziglar and Assistant Secretary of State for Consular Affairs Mary Ryan jointly agreed to begin transmitting data from the Department of State's Consolidated Consular Database to IBIS that includes nonimmigrant visa issuance information and a photograph of the alien. Because of that cooperation, the alien's photograph is now available at our ports-of-entry to determine if the alien engaged in any document fraudulent conduct. That deployment was completed in January 2002. In Miami, where access to the data was first instituted, INS Inspectors credit the initiative with detecting 108 fraudulent visa holders in the first six months. INS Inspectors using this data in New York caught an alien trying to enter the US on a falsified Russian diplomatic passport. In another instance, a 41-year old man was discovered using the altered visa of a three-year old Brazilian boy.

Another example involves the sharing of fingerprint data. Prior to September 11, the INS had worked with the U.S. Marshals Service to incorporate fingerprint data of their wanted persons into the INS fingerprint identification system known as IDENT. After September 11, the

INS worked with the Federal Bureau of Investigation (FBI) to incorporate fingerprint data from their Integrated Automated Fingerprint Information System (IAFIS) "wants and warrants" file into IDENT as well. IAFIS contains fingerprints for persons wanted by Federal, State, and local law enforcement agencies. This effort has been extremely successful and has already resulted in the identification and apprehension of over 3,100 individuals wanted for felony crimes.

The Federal Government maintains a number of databases that provide real-time information to foreign diplomatic outposts, border ports-of-entry, and interior domestic law enforcement. We work closely with other federal agencies to maintain these databases to prevent terrorists from entering the United States, to detect and apprehend those already in the country, and to gather intelligence on terrorist plans and activities or conspiracies.

Examples of systems that share data include:

- The Department of State TIPOFF System--designed to alert Consular Officers and Immigration Inspectors of suspected terrorists who are not U.S. citizens as they apply for visas overseas, or attempt to pass through border ports-of-entry.
- The FBI's National Crime Information Center--the nation's principal law enforcement automated information-sharing tool. It provides on-the-street access to criminal history information to over 650,000 Federal, State, and local law enforcement officers.
- The Interagency Border Inspection System (IBIS)--the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry. The inclusion of data on terrorists in this integrated database helps preclude the entry of known and suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time.

Let me now discuss other key programs that INS is undertaking related to the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act of 2002. Under

the conceptual framework of creating a U.S. entry-exit system, INS and the Department of Justice have implemented the National Security Entry Exit Registration System (NSEERS). Also related to this effort are the expanded use of electronic passenger manifests, the Student and Exchange Visitor Information System (SEVIS), and the continuing development of the use of biometrics in travel documents.

**Development of an Entry Exit System**

An integrated entry-exit control program that records and matches the arrival and departure of non-U.S. citizens enhances the security of the United States by providing government officials with specific information about who is entering the country and who is staying past their period of authorized admission. Managing the entry, stay and departure of alien visitors is a major component of controlling our borders and requires collecting information regarding the movement of aliens in, through, and out of the United States. Armed with this information, the United States Government can make better-informed policy and management decisions, identify and take action against those who violate the law, more easily locate individual aliens of interest to law enforcement entities, and validate the immigration status of aliens so that only eligible persons receive immigration benefits. At the same time, we remain mindful that any process required to support an Entry Exit program must facilitate legitimate travel and commerce so we do not adversely affect the economies of the United States and its neighbors.

In order to effect the creation of an integrated entry exit system in a timely manner, the INS established an interagency project team. Consisting of members from the Departments of Justice, State, Treasury, and Transportation - those agencies with principal responsibility for managing the U.S. borders – the project team defines their mission in terms of "managing the people, cargo, and means of conveyance crossing U.S borders." The U.S. Entry Exit Program is a joint effort by these Departments whose intent is to significantly improve the processes,

policies, workforce, and systems utilized to manage the pre-entry, entry, stay, and exit of international travelers through over 300 ports-of-entry.

The Entry Exit Program will also facilitate collaboration across the Border Management Community through tighter integration of processes and data relevant to travelers, cargo, and means of conveyance. And lastly, the Program will foster greater cooperation with Federal, State, and local intelligence and law enforcement organizations through improved access to more complete and timely data generated by the Border Management Community, as well as information generated by State and local law enforcement where the assistance of the Federal law enforcement community is requested.

**Electronic Passenger Manifests**

INS has already taken the first steps in developing the entry exit system. Since January 2002, air carriers have been required to submit passenger and crew arrival information electronically to the US Customs Service. INS is able to acess this information via IBIS. The electronic transmission of manifests is a critical piece of the Entry Exit System. The Advance Passenger Information System (APIS) [Creates consistency with Page 9 reference to APIS] allows the INS to conduct analysis and identify and apprehend national security threats as well as criminals. With the addition of electronic departure data, the INS will be able to improve not only our ability to identify and apprehend National Security Threats and criminals but also improve our ability to provide valid overstay data.

On October 1, 2002, the INS began accepting passenger data electronically for both arriving and departing passengers who arrived in the United States by air or sea carrier under the visa waiver program. This new initiative implements the requirements that had been set forth in the Visa Waiver Permanent Program Act of 2000. The next step involving electronic manifest will occur on January 1, 2003, when air and sea carriers will be required to transmit electronic

arrival and departure data for all arriving and departing passengers including new data elements which will aid in the identification of mala fide travelers.

The information captured from the electronic manifests feeds into the Arrival Departure Information System (ADIS). The ADIS will be the repository for arrival and departure records for non-citizens. The ADIS will match arrival and departure records to accurately identify those individuals who are out of status. In order to do this, the system will need to interface with several systems inside and out of INS. The system will also need to interface with Department of State systems to update visa records to show when individuals overstay their authorized stay. The Immigrant Services Division (ISD) case management systems will need to interface with ADIS to pass any adjustment of status or extension of stay information.

**National Security Entry Exit Registration System (NSEERS)**

We have also taken the initiative to expand our knowledge through the National Security Entry-Exit Registration System (NSEERS). The INS began to implement at NSEERS at U.S. ports-of-entry on September 11, 2002. Under NSEERS, INS is fingerprinting in IDENT and photographing certain nonimmigrant aliens who may potentially pose a national security risk upon their arrival in the United States. In addition, these non-immigrant aliens are required to register periodically with the INS, allowing us to better verify that they are complying with the terms of their nonimmigrant status.

Nonimmigrant aliens subject to special registration provide specific information and have their fingerprints and photograph taken upon their arrival into the United States (US). They must update their registration information approximately 30 days after arrival, every twelve months after arrival, and upon certain events (such as changes of address, employment, or school). Finally they must record their departure from the United States from designated locations. Approximately 100,000 people per year will be registered through this program.

**Use of Biometrics**

Another important piece of the system involves the use of biometrics. Currently the National Institute of Standards and Technology (NIST) is working expeditiously to identify and define biometric standards. These tests are being conducted so that the NIST can provide guidance to the Attorney General and Secretary of State, who are responsible for setting standards to be used in United States issued travel documents. All United States travel documents issued to aliens must include biometric identifiers if the documents are issued on or after October 26, 2004.

Since 1998, the DOS and INS have produced over five million Border Crossing Cards that include biometrics. The Border Crossing Card has two fingerprints and a digital photograph imbedded in an optical stripe. The INS will shortly begin testing biometric verification systems at six ports-of-entry. The Space and Naval Warfare System Center, San Diego (SPAWAR) has been contracted to conduct this evaluation. The INS has awarded two contracts for Optical Reader/Writer and Biometrics Verification Systems that will be used for this test. The SPAWAR will conduct tests, gather the metrics, and evaluate the concept of BCC Biometric Verification Systems (BVS) at different inspection ports-of-entry and climatic environments. The test will consist of 30 optical stripe (laser card) readers and biometric verification systems at small, medium and large land and air ports-of-entry. The designated ports are Los Angeles, San Ysidro, Nogales, Falcon Dam, San Antonio, and Atlanta. The testing process will help ensure that whatever biometric equipment is ultimately put in place will meet the needs of the entry exit system. If the evaluation is successful the INS will begin the procurement process to deploy these biometric verification systems along the border.

**Student and Exchange Visitor Information System (SEVIS)**

The INS has made considerable progress in implementing a new system that will greatly enhance our ability to track and monitor foreign students and exchange program visitors. This progress leaves us confident that we will meet the January 1, 2003 deadline for full implementation as established in the USA PATRIOT Act. This Internet-based system, known as the Student and Exchange Visitor Information System (SEVIS), will maintain critical, up-to-date information about foreign students and exchange visitors, and their dependents, and will allow for electronic access to this information. As such, it will enable the INS to track students in the United States more accurately and more expeditiously. SEVIS, as a fully implemented system, will be an integrated system that incorporates information directly from schools, exchange programs, several INS systems, and the DOS.

The INS deployed the core operational component of SEVIS and began accepting and reviewing school petitions for eligibility (Form I-17) as of July 1. As of October 7, 2002, there were 2,625 schools currently in various stages in the system, with 1,090 approved schools issuing and updating student records electronically in SEVIS. Also as of October 7, 692 schools had completed and submitted an electronic petition and were awaiting approval to use SEVIS. Another 870 schools created and saved drafts of such petitions but had not yet submitted a completed petition for adjudication. Upon approval, these schools will be able to access SEVIS to create and update student records.

To help facilitate effective implementation of SEVIS, the INS has worked closely with many education associations including the American Council on Education, the Association of International Educators, the National Association of State Universities and Land-Grant Colleges, and the California Community Colleges Chancellor's Office. Further, INS has established a SEVIS-dedicated, national call center with multiple tiers to answer technical and policy-related questions.

The INS is exerting greater control over the institutions authorized to admit foreign students in F and M visa status. The INS believes that for this brand new SEVIS system, review of all schools is the best method to ensure integrity. To facilitate the review of INS-approved schools and to ensure the enrollment of eligible schools in SEVIS in a timely manner, the INS has implemented a two-phased process for school review and SEVIS enrollment. Phase 1 was a preliminary enrollment period in which schools that have been INS-approved for at least the last three years to admit foreign students and are recognized as accredited or Title IV by the Department of Education were reviewed and granted access to SEVIS. Phase 2 will involve the certification of a school after a full review, including an on-site visit in many cases. For some schools, the on-site visit will verify their bona fides, but more importantly, the on-site visit will help ensure record keeping and reporting compliance, as well as confirm that the schools are aware of their responsibilities. An interim rule that will explain the school certification process has been published.

The INS is working toward enhancing our data share arrangement with the DOS Office of Consular Affairs in order to electronically provide SEVIS data for verification during the visa issuance process. INS and DOS currently have a Nonimmigrant Visa (NIV) Datashare arrangement, whereby DOS is sending all nonimmigrant visa issuance data to INS and Customs systems. SEVIS plans to extract data of all the F (academic), M (vocational), and J (exchange visitor) records from that existing arrangement.

The SEVIS program staff have been working closely with the INS Entry/Exit program staff in order to collect data, such as date and port-of-entry as mandated by the USA PATRIOT Act. SEVIS has been included in the functional requirements for phase 1 of a comprehensive entry/exit system. Phase 1 consists of the Visa Waiver Permanent Program Act (VWPPA) Support System, which leverages existing information technology systems, specifically the Advance Passenger Information System (APIS) and the Arrival Departure Information System (ADIS) to capture data electronically. This first phase of the entry/exit system will provide entry data on all F, M and J aliens to SEVIS at all air and sea Ports-of-Entry. For those Ports-of-Entry

not yet included in the entry/exit system, we will have alternative processes to provide data to SEVIS and notice to the schools.

The Enhanced Border Security and Visa Entry Reform Act (Border Security Act) of 2002 requires schools to report the failure of a foreign student to enroll within 30 days after the schools' registration deadline. The INS has established a toll-free, 1-800, number for schools to report a foreign student's failure to enroll, and once all schools are enrolled they will be able to report directly in SEVIS. The INS is also required by this legislation to review all schools every two years to ensure compliance with record-keeping and reporting requirements.

Full implementation of SEVIS will revise and enhance the process by which foreign students and exchange visitors gain admission to the United States. The INS, through SEVIS, will increase its ability to track and monitor foreign students and exchange visitors in order to ensure that they arrive in the United States, show up and register at the school or exchange visitor program, and properly maintain their status during their stay as valued guests in this country.

**Conclusion**

Madam Chairwoman, having addressed what we have been doing to deal with the immediate challenges in response to guidance from Congress and the Administration, let me turn to the activities that address emergent issues on the horizon.

To improve in the information technology area, the management principle to develop information systems is to build on a sound strategic foundation. The INS has established important mechanisms to address these principles internally. One of these mechanisms is our formal Enterprise Architecture. In May 2000, the INS initiated a project to develop a business-driven Enterprise Architecture (EA). The result of the project is a multi-year IT modernization plan whose implementation will require consistent oversight, funding, and systems development. The EA Plan was completed on schedule and on budget in July 2002. The EA Plan provides the blueprint and build-out plan for modernizing information systems and technical infrastructure

that will enable the INS to better meet its business objectives. In addition, an Information Technology Investment Management (ITIM) process has been in place for over three years. ITIM is the standardized process by which investment dollars are approved for information technology (IT) projects. This process ensures that IT investments are spent wisely and coordinated among INS components. In doing so, we are mindful of the relationships that we must support with our technical enhancements while integrating our business objectives and developing technical solutions.

Thank you Madam Chairwoman for this opportunity to share my views with you and the Committee. I will be happy to answer any questions you may have at this time.

###

**STATEMENT OF**

**STEPHEN A. EDSON**
**ACTING DEPUTY ASSISTANT SECRETARY OF STATE**
**FOR VISA SERVICES**
**BUREAU OF CONSULAR AFFAIRS**
**UNITED STATES DEPARTMENT OF STATE**

**BEFORE THE**
**JUDICIARY SUBCOMMITTEE ON TECHNOLOGY, TERRORISM AND GOVERNMENT INFORMATION**

**UNITED STATES SENATE**

**CONCERNING**

THE STATUS OF IMPLEMENTATION OF THE ENHANCED BORDER SECURITY AND VISA ENTRY REFORM ACT
October 9, 2002

Madame Chair and distinguished members of the Committee, thank you for allowing me to speak this morning concerning the progress to date of the Department of State's efforts to implement the provisions of the Enhanced Border Security and Visa Entry Reform Act of 2002.

In implementing the immigration laws of the United States and managing the visa process, the Department of State has no higher priority than our national security. We participate with the border security agencies and the broader law enforcement and intelligence communities in a wide range of activities including but not limited to the visa process to ensure the greatest possible cooperation in our joint efforts to secure our borders and fight terrorism. Although these relationships are long-standing, they have been significantly expanded in the year since the tragic attacks of September 11, 2001. We are dedicated to meeting the opportunities provided by the Enhanced Border Security and Visa Entry Reform Act, both to build on our efforts to date and to break new ground in our common search for a safer United States.

For the sake of comprehensiveness, in my testimony today I will address in order each section of the Enhanced Border Security and Visa Entry Reform Act that involves the Department of State and briefly outline the Department's efforts in each area.

Section 103 concerns the amount of the machine-readable visa fee and authorizes a surcharge for issuing visas in passports which are not machine-readable. The machine-readable visa fee will go up from $65 to $100 on November 1, 2002, reflecting increases in the actual cost of providing visa service. Added security screening procedures, restrictions on the role of Foreign Service

National employees and further increases in management oversight have made visa processing more expensive. Consistent with the principle of full cost recovery, the Department will continue to conduct regular cost of service studies to ensure that this fee remains appropriate for the cost of services provided.

The Department has not yet implemented a surcharge for bearers of passports which are not machine-readable but appreciates the authorization to do so and stands prepared to collect this surcharge should it become necessary.

Section 201(a) of the Act concerns interim measures to maximize information sharing relevant to the admissibility and deportability of aliens. Significant progress has been made in the past year to increase that amount of information available to visa officers overseas and, conversely, to INS and other law enforcement and intelligence agencies in the United States. The State Department's Consular Lookout and Support System (CLASS) is a principal example of this progress. The Department has been able to leverage the provisions of the Enhanced Border Security Act and USA Patriot Act to make CLASS an ever-stronger tool in our efforts to protect our national security. CLASS uses sophisticated search algorithms to match lookout information to individual visa applicants. Every single visa applicant is run through CLASS, and in fact, our automated processing systems will not print a visa until the consular officer has checked and resolved "hits" of the applicant's biodata against the lookout system data. CLASS is only as good, however, as the data that it contains. I am happy to report that post 9/11 this situation has improved dramatically.

CLASS records have doubled since September 11. Per USA PATRIOT Act mandate, more than 7 million names of persons with FBI records were added to the CLASS database by August 2002, augmenting 5.8 million name records from State, INS, DEA, and intelligence sources. These NCIC records include the FBI's Violent Gang and Terrorist Database, a particularly valuable resource. When a visa applicant "hits" against NCIC records in CLASS, consular sections can obtain fingerprints to pass to the FBI for purposes of obtaining a full criminal record if necessary, with the fingerprints to help guard against any identification problems.

20,000 Customs serious violator name records have been added to CLASS since September 11, 2001. CLASS now has over 78,000 name records of suspected terrorists, up 40% in the past year. Most of this information has entered CLASS through TIPOFF, a program run through the Department's Bureau of Intelligence and Research that acts as a clearinghouse for sensitive intelligence information provided by other agencies throughout the US government. The TIPOFF staff is able to review and evaluate information concerning suspected terrorists and pass sanitized index information to CLASS. Since September 11, 2001, approximately 20,000 new terrorist lookouts have been entered in the TIPOFF database.

The Department is working on CLASS enhancements including better data on lost and stolen passports, more deportation records from INS, a backup facility at our Kentucky Consular Center, more hardware capacity, and new search algorithms.

An interoperable law enforcement and intelligence data system with linguistic algorithms and

robust training and support is the subject of Section 202 of the Act. The State Department currently shares electronic data relevant to visa eligibility with other agencies including INS and is rapidly expanding information sharing arrangements throughout the law enforcement and intelligence communities. The Department's systems use open, flexible architecture consistent with industry standards in order to facilitate information sharing. All nonimmigrant and immigrant visa activities at all of our posts worldwide are replicated to the Consular Consolidated Database at five minute intervals, providing the Department, INS and other US government agencies with a near-real-time window into this work.

The State Department's CLASS lookout system has used for sometime now linguistically sensitive algorithms for checking Arabic, and Russian-Slavic names. A Hispanic algorithm is developed and ready for implementation. An algorithm for East Asian languages is under study. The Department of State has been a leader in the development of linguistic logic in search processes and is actively engaged with other US government agencies to share this expertise and ensure optimal implementation of this section of the law by the specified deadline.

The State Department's Bureau of Consular Affairs provides assistance to consular officers in resolving identity and other questions concerning CLASS lookout system hits, in addition to handling substantial numbers of inquiries from INS and various law enforcement entities related to visas and lookout entries.

Although the Department of State has skilled linguists available around the world accessible on an ad hoc basis, we feel that full implementation of this section of the act will require additional formal training, printed materials on various transliteration systems and alternative spellings, and a more formal designation of linguistic expertise in various key languages. In March of 2002 the Consular Training Division began offering a course on Advanced Consular Namechecking techniques. This course teaches students about the language algorithms used in CLASS to ensure officers provide the best information possible regarding applicants and thus increase the reliability of namechecks. We are exploring a number of additional alternatives for providing this expertise, beginning with a support structure in the Department of State, but expect to discuss this further in the context of the formation of the Department of Homeland Security as part of a coordinated support structure.

Section 301 of the Act concerning the electronic provision of visa files is one of several examples of new requirements which complement longstanding partnerships between State and INS. The Department of State currently provides to INS visa issuance information, including nonimmigrant and immigrant visas, electronically. This information is available through the Department's Consular Consolidated Database, which is updated from all posts around the world every five minutes. The information includes biographic data and visa and passport details. For nonimmigrant visa issuances, the electronic record passed to INS includes a digital copy of the photograph of the visa applicant, matching the photograph printed on the visa.
The information on nonimmigrant visa applicants in the CCD will be augmented by an additional 25 data fields, including address and telephone numbers, with the upcoming January release of new visa software, already in Beta test at the Consulate General in Toronto, Canada. We are also developing the capability to capture and share the photos of immigrant visa applicants

electronically as part of our effort to design a machine-readable immigrant visa.

The latest versions of our nonimmigrant visa processing system also support the scanning of nonimmigrant visa applications and other documentation. Soon all visa processing posts will have this software, and we have procured and shipped scanners to each post to allow them to scan serious refusal files into the consolidated database. We will soon expand this procedure to require posts to scan visa applications in cases requiring special security screening. Telecommunication and other resource issues prevent us from immediately scanning all applications worldwide, although this is our longer-term intention.

We should also note that we have begun efforts to allow applicants to submit applications electronically, which will ultimately facilitate more efficient sharing of these files.

The implementation of an integrated entry and exit system with appropriate technology standards is dealt with in Section 302. The Department of State is working closely with the Department of Justice and the National Institute of Standards and Technology on development of the technology standard for travel documents. The Department has issued machine-readable documents since 1981. Beginning in April 1998 the Department has collected two fingerprints and a digitized photo for all applicants for border crossing cards in Mexico, and we have gained valuable experience in that program. Since the inception of the BCC program, the Department has adjudicated over 7 million applications and issued over 5.6 million cards. We are confident that we will be able to deploy a global visa issuance system that will use appropriate biometric standards.

I defer to my colleague from INS on the progress of work to establish a database of arrival and departure data, but I should note that the Department of State is a regular participant in discussions of this issue and stands firmly behind INS efforts. We believe that the Consular Consolidated Database with its repository of visa information will be a key resource in this effort.

The Department of State's Consular Lookout and Support System (CLASS) database is interoperable with the Interagency Border Inspection System (IBIS) that INS uses in regard to determining admissibility under section 212 of the INA. In fact, State and INS began electronic sharing of data through these systems in 1995. The systems architecture used by the Department lends itself readily to interoperability and we look forward to expanding information sharing activities with INS and other agencies.

The Department of State meets regularly with the INS in the interagency Entry Exit Program Team, the Datashare Working Group, the Senior Implementation Group of the Border Agency Partnership, and other ad hoc meetings to discuss and resolve issues related to facilitation of lawful and efficient cross-border movement of persons and border security. We feel that we and INS have important experience with the problems of moving large numbers of people that will help ensure optimal implementation of this section of the law.

Finally, the Department is taking the lead in discussions with the governments of Canada and

Mexico on closer cooperation on matters of border security.

Section 303 concerns standards for and implementation of machine-readable, tamper resistant travel documents. The report called for in Section 303(a) is currently under preparation and the State Department is participating fully in this process.

The Department of State, in coordination with the Department of Justice and other concerned agencies, is working to determine the appropriate type of document and biometric standards to use with travel documents issued to aliens. Although many of the final implementation details will have to wait for formal decisions on these standards, the Department of State already issues nonimmigrant visas which are machine-readable and include digitized photos. Since the attacks of September 11, we have successfully rolled out the new Lincoln nonimmigrant visa, which contains major enhancements to prevent alteration and duplication, in pilot posts overseas, with plans to complete worldwide deployment by early 2003. Prior to 9/11, we had already begun design work on a machine-readable immigrant visa, also to include a digitized photo.

We are currently collecting input from our missions in countries participating in the Visa Waiver Program and have already met with each of these nations to discuss the requirement that they incorporate biometric identifying data in their passports. Although all of these countries recognize the importance of including biometric indicators in their travel documents, and most already use at least digitized photos, specific plans are still under development. This section of the law refers to standards established by the International Civil Aviation Organization (ICAO), rather than to the NIST-developed standard necessary for our own visas. An ICAO working group has identified three acceptable biometric identifiers—face, fingerprint and iris. A full ICAO meeting in early 2003 should finalize the standards. We will continue an active dialogue with ICAO and the governments involved on this issue and are preparing to report to Congress as required by Section 303(a) of the Act.

The Department of State is meeting the provisions of Section 304 for terrorist lookout committees through the Visas Viper program, a program which began in the aftermath of the first World Trade Center bombing in 1993 and has been significantly enhanced pursuant to the requirements of the Enhanced Border Security Act. It is an ongoing interagency collaboration here in Washington and at our posts abroad. Overseas agencies and sections meet monthly or more often to review data on possible terrorists and terrorism supporters for submission to Washington for inclusion in the lookout system. Quarterly reports will be prepared for Congress as required by the Act.

Since the Visas Viper program began, over 60,000 names of persons suspected of involvement in terrorism have been submitted through this channel and entered into the Consular Lookout and Support System through the TIPOFF database.

Section 305 expands the existing training required for consular officers. Much required consular training has always included instruction on the detection of fraudulent documents, imposters, and indicators of criminal intent. The Department's training center, the Foreign Service Institute, has initiated several changes to the basic consular course and other training. As mentioned earlier, in

March of 2002 the Consular Training Division began offering a course on Advanced Consular Namechecking Techniques. We have now trained 70 offices in 2002 and expect to train 120 more in each of FY 03 and FY 04. This course teaches students about the language algorithms used in the CLASS system to ensure officers provide the best information possible regarding applicants and increase the reliability of namecheck matches. A separate but very important benefit of this course has been the direct feedback opportunities between field officers, computer technical staff, and Department management. Officers in this course are also updated on special security requirements, including new screening programs instituted during the past year.

The basic course also contains information on new security screening requirements and now included additional emphasis on ethics and accountability. In addition, FSI plans to provide new officers with briefings on terrorism, additional fraud training, and more time to hone interviewing skills. The latter initiatives are in varying stages of planning and implementation. FSI is collaborating with Counter-Terrorism officials at the FBI to start counter-terrorism sessions for consular officers as soon as the FBI has the training segment ready.

As an initial measure, to ensure that visas are not issued to persons from state sponsors of terrorism who might pose a security risk, the Department has put in place a variety of procedures explicitly designed to cut very broadly. As an interim measure, all adult visa applicants who are national or permanent residents of or who were born in one of these nations are subject to formal special clearance requirements. We anticipate reviewing these procedures in consultation with other agencies before making recommendations to the Secretary of State as to a final process for making the required determination under Section 306 of the Act. Under the Act, the Secretary is required to consult with the Attorney General and the heads of other agencies to establish standards to implement the statutory requirement that an individual determination is made that 'such alien does not pose a threat to the safety or national security of the United States' in order for a visa to be issued.

Section 307 establishes a requirement for timely reporting of lost and stolen passports in order for a country to continue participating in the visa waiver program. Although this section will likely not, practically speaking, apply to existing visa waiver nations until such time as they are certified for continued participation in the program, we are discussing this requirement with all visa waiver countries. INS can provide the details of our joint review of six of these nations, but I can confirm that report of theft of passports has been a major topic of discussion in each case. In addition, all consular sections worldwide were instructed to begin discussing this requirement with host governments in a State Department message dated June 27, 2002.

I defer to my INS colleague for comment on the periodic certification of visa waiver participants but note that the Department of State intends to participate fully in each review.

The State Department's CLASS lookout system includes a database of lost and stolen passports which has been improved to address the requirement of Section 308. Each visa applicant's passport issuance number is electronically checked against this database prior to visa issuance. The Department already has in place a system for collecting data on missing blank foreign documents, and enters these documents into the CLASS system where appropriate. We are

currently creating a database that will allow interagency cooperation on document searches to be quicker and more accurate. Currently the CLASS system has over 80,000 US and 250,000 foreign lost and stolen passport numbers in its database.

Section 401 requires a study of the feasibility of a North American National Security Program, which is a matter of ongoing discussion with the governments of both Mexico and Canada. The Department participates fully in these discussions.

We in the State Department are actively participating with the INS and the exchange community in the design and development of the Student and Exchange Visitor Information System (SEVIS), the permanent system that will contribute to our national security as it adds integrity to the student and exchange visa issuing process as required by Section 501 of the Act. At the same time we are working on SEVIS implementation, in response to a separate legislative mandate the Department has launched the Interim Student and Exchange Authentication System (ISEAS), which will provide for the electronic verification of student and exchange visitor visas until SEVIS is fully implemented. ISEAS is an interim system that will operate in a stand-alone capacity until SEVIS becomes final.

ISEAS is a web based system that allows consular officers to verify the acceptance of foreign students and exchange visitors who apply to enter the United States in student ("F," "M") and exchange visitor ("J") nonimmigrant visa categories based on information the schools or exchange program sponsors enter directly into the system. That portion of the legislative mandate that requires the Department to inform INS of F, M or J visa issuance is being accomplished using the existing datashare link.

ISEAS is the means by which INS-approved educational institutions and Department-designated exchange programs meet this legislative requirement. Consistent with the legislation, ISEAS was established as an interim system, with the limited support and capacity implied by the term. ISEAS will only be operational until SEVIS is implemented on January 30, 2002. Given the short timeframe to establish ISEAS, it unfortunately does not have the capability to share any data with SEVIS. As a result, currently, and until SEVIS is implemented and educational institutions and designated program sponsors become SEVIS compliant, designated officials will have to electronically register visa applicants into two separate databases (ISEAS and SEVIS), and consular officers will have to check both data bases to confirm the provenance of those documents, until ISEAS sunsets with final SEVIS implementation on January 30, 2003. The need to report foreign and exchange student information in two separate databases, however, will end once SEVIS is implemented and a program or institution is enrolled to use SEVIS.

Section 501(c) of the Act requires the approved institution or designated exchange program sponsor to transmit electronic evidence of the applicant's acceptance to the Department. Academic institutions and program sponsors enter information from the required forms into the ISEAS web application (provided at www.iseas.state.gov <http://www.ISEAS.state.gov>) for transmission to the Department.

To ensure data integrity, the ISEAS Internet subsystem validates the identification data entered

by the designated institution or program official against approved lists of institutions or program sponsors. INS approved institutions or program sponsors correspond to F and M visas, and State Department, Bureau of Educational and Cultural Affairs approved institutions or program sponsors correspond to J visas.

Once ISEAS confirms that the institution or program is on one of the approved lists, the designated institution or program official will enter certain student or exchange visitor data, and the system returns to the school or exchange official a confirmation number which is maintained as part of the student's record. The ISEAS confirmation number will serve as evidence that a particular visa applicant's data has been entered into the ISEAS system, and is one of the search criteria available to consular officers in the field.

Due to the very short development period mandated by the legislation, we were unable to deploy ISEAS before September 11. Consequently, participating academic institutions and program sponsors were unable to enter the required data into ISEAS in advance.

That fact, coupled with the Act's clear wording - no student or exchange visitor visa can be issued after September 11, 2002, without electronic evidence of documentation of the alien's acceptance - meant that ISEAS deployment represented a potentially significant interruption of student and exchange visitor visa processing. We were concerned that many participating institutions and program sponsors would be unable to enter the required data into the system quickly enough to maintain smooth processing of student and exchange visitor visas. Therefore, we devised back-up procedures to ensure that consular officers receive timely electronic status verification directly from sponsoring institutions and programs, through email communications, when necessary.

ISEAS was intended to be an interim mechanism to collect information on foreign students and exchange visitors pending SEVIS development and not a comprehensive solution to better track these nonimmigrant individuals. As of the October 7, 2002, over 2,988 educational institutions and exchange program sponsors have entered over 71,344 records into ISEAS. 213 visa-issuing posts have verified over 8,942 cases. ISEAS has provided both the Department and INS a better system to verify incoming foreign and exchange students, until SEVIS becomes operational in January 2003.

The Department has designed and implemented a new form, the DS-158, now required of all student and exchange visitor visa applicants to meet the expanded data-collection required by the act.

We are actively pursuing expanded electronic information sharing as discussed in Section 603 with the governments of Canada and Mexico, as well as with the European Union, to which the bulk of the visa waiver nations belong. We have existing data sharing arrangements with Canada and Australia that we hope can be expanded significantly.

On October 2, 2002, State Department officials met with counterparts from the Mexican government to discuss sharing terrorist watchlist data and implementing a terrorist interdiction

program in Mexico. The proposal built on months of preliminary discussion and was well received, with meetings proposed for early November. Next steps include technical consultations and allocation of resources, as well as preparation of a Memorandum of Understanding.

In the immediate aftermath of the September 11 attacks, the Department instructed consular posts to retain all visa applications indefinitely. Since the passage of the Act, the Department has instructed all posts to retain these applications for at least seven years. Interim measures have been taken to provide for paper storage of these applications. Changes to consular automated systems being implemented this fall will allow consular sections to scan many of these applications for later retrieval and for easier collaboration with other concerned US government agencies on special clearance and other procedures. All visa applications dating from at least October 2000 will be retained for at least seven years in a form admissible in US courts.

Madame Chair and members of the Committee, this concludes my review of the Department of State's efforts to date in implementing the provisions of the Enhanced Border Security and Visa Entry Reform Act of 2002. I would be happy to take any questions that you might have.

**Statement of Glenn A. Fine**
**Inspector General, U.S. Department of Justice**
**before the**
**Senate Judiciary Committee**
**Subcommittee on Technology, Terrorism, and Government Information**
**October 9, 2002**

Madame Chairwoman, Senator Kyl, and Members of the Subcommittee on Technology, Terrorism, and Government Information:

## I. INTRODUCTION

I appreciate the opportunity to appear before the Subcommittee on Technology, Terrorism, and Government Information to discuss the Office of the Inspector General's (OIG) recent audit of the Federal Bureau of Investigation's (FBI) counterterrorism program. Our full 131-page audit, which is classified at the "secret" level, was provided last week to the Department of Justice, the FBI, and congressional oversight committees, including this committee. Last week, the OIG also released an unclassified executive summary that highlighted our major findings and recommendations.

Since the September 11, 2001, terrorist attacks, the Attorney General and the Director of the FBI have elevated counterterrorism and the prevention of future attacks against U.S. interests as the top priority of the Department of Justice and the FBI. Consequently, the OIG has undertaken a series of reviews of Department programs and operations that effect counterterrorism issues and national security. The counterterrorism audit that we issued last week, and that I will talk about today, was part of that effort.

Our audit examined certain aspects of the FBI's management of its counterterrorism resources. Specifically, our audit focused on: (1) the FBI's progress toward developing a national-level risk assessment of the terrorist threat to the United States; (2) whether the FBI's strategic planning process provides a sound basis to identify counterterrorism requirements; and (3) the amount of resources dedicated to the FBI's counterterrorism program from 1995 to April 2002. In addition, our review assessed the FBI's management of its training and after-action reporting as they relate to counterterrorism operations.

It is important to note at the outset of my remarks that our audit does not purport to assess all aspects of the FBI's counterterrorism program or how the FBI or other law enforcement and intelligence agencies handled information that may have been related to terrorist activities that resulted in the September 11 attacks. At the request of the FBI Director, the OIG has initiated

a separate review that is examining aspects of the FBI's handling of certain intelligence information prior to the September 11 attacks, including allegations regarding the FBI's investigation of suspected terrorist Zacarias Moussaoui, the FBI's handling of information provided by the Phoenix Division about flight schools, and the FBI's handling of other intelligence information.

In sum, the counterterrorism audit that we released last week found that the FBI has not developed a comprehensive written assessment of the risk of a terrorist threat facing the United States despite its statement to Congress in 1999 that it would. We concluded that such an assessment would be useful not only to define the nature, likelihood, and severity of the threat but also to identify intelligence gaps that needed to be addressed. Moreover, we concluded that a comprehensive, written threat and risk assessment would be useful in determining where to allocate attention and resources – both within the FBI and government-wide – on programs and initiatives to combat terrorism.

In addition, the FBI has not yet incorporated into its strategic plan (a document not updated since 1998) a comprehensive assessment of the threat and risk of terrorist attacks.

Our findings should not be interpreted to mean that the FBI has not taken important steps during the past year to improve its counterterrorism program. After the September 11 attacks, the FBI identified as a critical weakness its ability to analyze intelligence and is working to improve its capabilities in this area. In addition, the FBI has reorganized its Counterterrorism Division and has taken other steps to improve its counterterrorism capabilities.

However, we believe that the FBI can and must do more. We are encouraged by the FBI's reaction to our audit findings and recommendations – the FBI called them "constructive guidance" and agreed to implement the recommendations we made. We are hopeful that these corrective actions will assist the Bureau in improving its ability to meet its critical counterterrorism priorities.

I now will summarize the major findings of our audit.

## II. THREAT ASSESSMENTS

The FBI has never performed a comprehensive written assessment of the risk of the terrorist threat facing the United States. Such an assessment would be useful not only to define the nature, likelihood, and severity of the threat but also to identify intelligence gaps that need to be addressed. Moreover, we believe that comprehensive threat and risk assessments would be useful in determining where to allocate attention and resources to programs and initiatives to combat terrorism. In response to a September 1999 General

Accounting Office (GAO) report, the Department and the FBI agreed that the FBI would conduct a national-level risk assessment of the terrorist threat to the United States.

In March 2001 the FBI said that this assessment, eventually titled "FBI Report on the Terrorist Threat to the United States and a Strategy for Prevention and Response" (Terrorist Threat Report), would address emerging trends, the current threat, the projected threat, FBI initiatives, and future focus. The FBI said the findings in the Terrorist Threat Report would be based on FBI investigations, interagency reporting, public source information, and United States intelligence community publications.

By September 2001, the FBI had developed a draft of a Terrorist Threat Report that described terrorist organizations and State sponsors of terrorism. But this report did not assess the threat and risk of an attack on the United States. In addition, based on our review of the draft report, we concluded that it did not conform to the FBI's assessment guidance, other available guidance on preparing threat and risk assessments, or the FBI's representations as to how it would respond to the GAO's recommendations. Among the report's many omissions were assessments of the training, skill level, resources, sophistication, specific capabilities, intent, likelihood of attack, and potential targets of terrorist groups. Further, the draft report did not discuss the methods that terrorists might use. For example, there was no analysis of terrorists' progress toward developing or acquiring chemical, biological, radiological, and nuclear weapons or any discussion of what the FBI has learned from its past terrorist investigations.

Moreover, contrary to available guidance on conducting threat and risk assessments and the FBI's representations to the GAO and the Congress, the FBI's Terrorist Threat Report did not: (1) provide information to assist FBI management and other government managers in developing counterterrorism strategies and programs and allocating resources on a priority basis; (2) identify critical intelligence requirements; or (3) make recommendations to any level of FBI management. The lack of recommendations in the Terrorist Threat Report underscores the fact that the report was, as one FBI Assistant Director described, "a primer, and not a risk assessment."

We identified a number of causes for the Terrorist Threat Report not adequately addressing these issues. First, the report was the responsibility of at least two different FBI managers and an unknown number of staff, but no single individual was accountable for managing the assessment throughout the process or for maintaining the original reporting objectives. Second, some FBI officials said the FBI lacked the analytical capability or resources to complete such a broad threat assessment. Third, the FBI did not have a system of management controls that ensured compliance with GAO (or OIG) recommendations. Finally, in our judgment, FBI counterterrorism managers

had a tendency to rely on their experience and professional judgment regarding the overall terrorist threat and did not value a formal written assessment that uses a structured methodology. In fact, the Terrorist Threat project had such a low profile within the FBI that it took the FBI nearly a month to identify to us anyone who was familiar with the project and the draft report.

Because the FBI has not completed a systematic written assessment of the most likely terrorism scenarios – taking into account terrorist methods, capabilities, and intent – it may not have identified fully the specific nature of the threat so that it could focus its attention and resources to prepare adequately and respond effectively given the assessed risk. A comprehensive national-level written assessment of the threats and risk of terrorism also would aid the FBI Director's objective of moving the FBI from a reactive, crime investigation culture to a more proactive institution that seeks to prevent, deter, and disrupt terrorist acts. Determining what scenarios are most likely to occur in a comprehensive and more formal manner would better position the FBI to meet its new counterterrorism priority.

In addition, any national-level assessment of the terrorist threat would be incomplete without incorporating an assessment of the potential for, and likelihood of, an attack using chemical, biological, radiological, and nuclear materials or weapons. However, the FBI has not performed a full assessment of the threat and risk of a terrorist attack with chemical and biological materials (or with other weapons of mass destruction), despite its representations that it would.

In response to the GAO report, the FBI's Assistant Director, Office of Public and Congressional Affairs, had reported to the Chairman of the House Appropriations Committee in a March 2000 letter that the FBI:

- supported the GAO's September 1999 recommendation for a formal, authoritative intelligence threat assessment;

- concurred that the assessment process must involve a multidisciplinary team of subject-matter experts;

- viewed the assessment as the first step in providing a guide for future program investment for WMD [weapons of mass destruction] countermeasures;

- would determine the specific WMD hazards chosen for evaluation by analyzing intelligence sources, case histories, related assessment data from the scientific and health communities, and current trends in domestic and foreign WMD terrorist activities;

- would develop and rank a list of chemical and biological agents based on the likelihood that a particular agent would be used over another;

- would develop scenarios for the highest threat hazards so that this information may be utilized to determine deficiencies in response capabilities at the national level; and

- agreed that such an assessment would require updating at least every three years.

However, the approach the FBI actually used was, in our view, unresponsive to the GAO recommendation. Further, the FBI failed to follow through on its promise that it would render a formal, authoritative intelligence threat assessment using a multidisciplinary team of experts that specifically assesses the chemical and biological agents that more likely would be used by terrorists domestically.

Instead of performing its own intelligence threat assessment, the FBI joined in an ongoing contractor assessment funded by the National Institute of Justice (NIJ). The NIJ-funded study had different objectives than the FBI's promised assessment and was never designed to meet the FBI's assessment objectives in response to the GAO recommendation; the FBI's more general need to determine which WMD agents to focus its attention and resources; the FBI's responsibility to provide guidance to others as the federal domestic intelligence agency and the lead federal agency for crisis management and response in the event of a terrorist WMD attack; and the need for input to a broader national-level threat and risk assessment that could be used by the FBI and other federal, state, and local agencies to determine and prioritize programs to combat terrorism and focus WMD preparedness efforts.

Rather, the NIJ-funded study was intended to "assist the NIJ and State and local law enforcement in addressing needs for (a) improved means for detecting nuclear, biological and chemical (NBC) hazards and (b) better NBC protective gear." Further, the NIJ-funded study noted that "...classified materials of any sort were not examined nor considered." The draft report of the NIJ-funded study, which explicitly excluded any consideration of intelligence information, did not assess the threat and risk that either foreign-based or domestic terrorists will use a given chemical or biological agent (or even improvised radiological or nuclear devices) in the United States to create mass casualties.

Consequently, we concluded that the NIJ-funded study is of limited use in meeting the fundamental strategic planning needs – including program and intelligence requirements determination, priorities, and resource allocation – of the FBI or other federal, state, and local agencies involved in developing

countermeasure strategies and domestic preparedness efforts. In our judgment, only a team consisting of subject matter experts could provide an adequately comprehensive assessment of all relevant factors in potential terrorist use of chemical or biological agents or other WMD. Because the NIJ-funded study did not contain intelligence input, the study is not useful to the FBI for assessing risk (although this is not intended as a criticism of the study for use in meeting its intended purpose). The need remains for an authoritative assessment of what chemical and biological agents, as well as radiological and nuclear devices, are more likely to be used by terrorists against targets in the United States.

Our audit also analyzed the FBI's efforts to identify the nation's critical infrastructure. Protecting critical physical infrastructure assets is an important part of the FBI's counterterrorism program. In an effort to identify and better protect critical infrastructure, the FBI began a Key Asset Program in the 1980s. The program developed slowly, and in 1998 the FBI sought to re-emphasize the effort, now renamed the Key Asset Initiative. However, the FBI's attempt to create a nationwide database of key assets has encountered difficulties. For example, the FBI inconsistently classified the priority of assets and it lacks an adequate database management system to compile and categorize voluminous data on key assets nationwide.

**III. STRATEGIC PLANNING**

Our audit reviewed the FBI's strategic planning as it relates to its counterterrorism mission. The FBI has developed an elaborate, multi-layered strategic planning system over the past decade. Yet, while the planning system acknowledged a general terrorist threat to the nation, the FBI did not perform and incorporate into its strategic plan a comprehensive assessment of the threat and risk of terrorist attacks on U.S. soil. Similarly, the planning system identified numerous vulnerabilities and weaknesses in the FBI's capabilities to deal with the general terrorist threat, but before September 11 this identification did not result in fundamental changes in the FBI necessary to correct the deficiencies.

The FBI planning system consists of Annual Field Office Reports, which serve as the 56 FBI field offices' strategic plans and identify their counterterrorism program vulnerabilities; FBI division-level Program Plans, which incorporate the results of the field office plans and accompany the annual budget submissions; the Counterterrorism Division's Director's Report to articulate the division's goals; and the FBI Strategic Plan. Since at least 1993, these layers of planning have not been guided by an overall strategic-level assessment of the threat and risk of terrorist attacks on the United States but, rather, by judgments at each level about the general nature of the terrorist threat. Further, the FBI's Strategic Plan has not been updated since 1998 and does not conform to the counterterrorism priorities in the Department's

November 2001 Strategic Plan, the FBI Director's new priorities, or the Counterterrorism Division's approach to develop the maximum capacity to deal with the terrorist threat.

After September 11, the FBI Director refocused the FBI's traditional crime-fighting orientation of investigating criminal acts after-the-fact for prosecution to place the highest priority on preventing terrorism. The Director also shifted resources to meet this new priority. However, we concluded that the FBI's strategic planning process lacks management controls to ensure that resources will be requested and allocated consistent with the Director's and the Attorney General's counterterrorism priority, particularly at the field office level. For example, during our audit period foreign language translation requests did not always receive priority over drug-related translation requests. Also, the FBI lacks an effective system of performance measures and standards that holds managers at all levels accountable for achieving the goals and objectives stated in FBI strategic plans. If the new strategic focus on counterterrorism is to be achieved, the existing gap between the formal planning process and actual operations must be narrowed.

Further, we found the FBI had made slow progress in completing its assigned tasks under the 1998 Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan. In addition, the FBI has not issued a policy on or developed a system for capturing, disseminating, and using lessons learned from past terrorism incidents, operations, and exercises to improve the FBI's counterterrorism capabilities.

## IV. RESOURCES

Our report also details the level of resources that the FBI has dedicated to counterterrorism and related counterintelligence between 1995 and 2002. While the exact figures are classified and redacted from our public report's Executive Summary, I can say that those resources have increased dramatically – about threefold – between 1995 and 2002. With the exception of 1996, appropriations for FBI counterterrorism and counterintelligence have increased each year.

Our classified report examines the number of FBI staff dedicated to counterterrorism in the 7-year period from 1995 to 2002. The staffing numbers include headquarters staff of the Counterterrorism Division, counterterrorism squads in the 56 FBI field offices, and support staff both at headquarters and in the field. Our report also includes FBI projections of the size of growth of its counterterrorism staffing in 2003, both in agents and support staff.

Finally, we found that the FBI has not established a core training curriculum and proficiency standards for these new agents working in counterterrorism. Moreover, we found that the type and extent of counterterrorism-related training varies throughout the FBI.

## V. RECOMMENDATIONS

Our audit report offers 14 recommendations to help improve management of the FBI's counterterrorism program, including recommendations that the FBI:

- prepare an authoritative written national-level threat and risk assessment of terrorism with a predictive and strategic view, including the potential use of weapons of mass destruction;
- identify the chemical and biological agents most likely to be used in a terrorist attack and assess fully the threat and risk of terrorists' use of all types of weapons of mass destruction;
- develop criteria for evaluating and prioritizing incoming threat information for analysis, and establish a protocol to guide the distribution of threat information;
- establish a time goal and a process for building a corps of professional, trained, and experienced intelligence analysts for assessing and reporting on threats at both the strategic and tactical levels;
- update the FBI strategic planning process to effectively conform to the current Department of Justice strategic plan and the FBI Director's counterterrorism priority;
- close the gap between planning and operations by establishing an effective system of performance measures and standards and holding managers at all levels accountable for achieving the goals and objectives stated in FBI strategic plans;
- issue a policy on and develop a system for capturing and disseminating lessons learned from counterterrorism incidents, operations, and exercises; and
- establish a core training curriculum and minimum competencies for agents assigned to counterterrorism.

The FBI responded that it concurred with our recommendations and stated that the recommendations provide constructive guidance. The FBI also described the steps it is taking to address the recommendations, including agreeing to draft a comprehensive written national threat assessment; updating the FBI's strategic plan; revising the FBI's performance measures to conform with a prevention-driven counterterrorism program; initiating a system of review for the purpose of gaining "lessons learned" from past major investigations; and designing a core training curriculum and minimum competencies for FBI special agents assigned to counterterrorism investigations.

## VI. CONCLUSION

We believe that completing the national-level threat assessment is critical to the FBI's counterterrorism efforts. The assessment must include an evaluation of the likelihood that specific chemical, biological, radiological, and nuclear weapons of mass destruction will be acquired or developed and used against American targets and citizens. Fully assessing the threat, probabilities, and likely consequences of a terrorist attack by different methods will be of significant benefit, not only to the FBI in allocating resources, but also for targeting domestic preparedness efforts and counterterrorism programs at all levels of government.

Furthermore, we believe that implementing our other recommendations will help improve the effectiveness and efficiency of the FBI's counterterrorism program. These improvements will aid the FBI in making the management changes set in motion by the FBI Director to move the Bureau from a reactive, post-crime investigatory culture to a more proactive organization that seeks to identify and deter terrorists before they can strike.

Our findings are not intended to criticize the expertise of FBI employees and managers who work on counterterrorism matters or the extensive knowledge they have developed through their casework and regular discussions within the FBI and the intelligence community. Yet, we believe that the professional judgment of FBI officials is not a substitute for a formal and comprehensive written strategic assessment of the threat and risk of terrorist attacks in the United States. We believe, as did the GAO when it made the recommendation, that a comprehensive written assessment will provide a better mechanism to analyze and assess the threats facing the United States.

# Department of Justice

STATEMENT

OF

ALICE FISHER
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM
AND GOVERNMENT INFORMATION
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

IMPLEMENTATION OF THE USA PATRIOT ACT

PRESENTED ON

OCTOBER 9, 2002

**Testimony of Alice Fisher**
**Deputy Assistant Attorney General, Criminal Division**
**United States Department of Justice**
**on October 9, 2002**

**Before the Senate Judiciary Subcommittee on**
**Technology, Terrorism and Government Information**
**United States Senate**

Chairman Feinstein, Ranking Member Kyl and distinguished members of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, I am honored to appear before you to testify about the Department of Justice's implementation and use of the important anti-terrorism provisions in the USA PATRIOT Act. I want to thank this Subcommittee's members, who helped to develop and enact the USA PATRIOT so swiftly in the wake of last September's attacks. As Deputy Assistant Attorney General of the Criminal Division, with responsibility over the Terrorism and Violent Crimes Section, I have been personally involved in seeing that the tools Congress provided in the Act have been used as intended: to enhance the ability of law enforcement to bring terrorists and other criminals to justice.

The unprecedented and heinous attacks on our nation, in which over three thousand innocent civilians were killed in New York City, in Pennsylvania, and at the Pentagon, occurred just over one year ago. At that time, the President pledged to the American people that we would not relent until justice was done and our nation was secure. Members of this Committee, and the Congress in general, joined the President as key partners in this important undertaking. Congress's swift and comprehensive response, through passage of the USA PATRIOT Act, provided us with vital new tools, and updated those tools already at our disposal, that have been

instrumental to our efforts to combat terrorism in the most extensive criminal investigation in history. As the President stated when he signed the USA PATRIOT Act on October 26, 2001, we took "an essential step in defeating terrorism, while protecting the constitutional rights of Americans." One year later, I am pleased to report that we have used these tools effectively, aggressively and responsibly.

As the Attorney General told the Senate Judiciary Committee in July, the Department's single and overarching goal since September 11 has been to prevent future terrorist attacks on the United States and its citizens. We have been aggressively implementing the USA PATRIOT Act from the outset. Following its passage, we immediately sent field guidance to United States Attorney's offices, advising them of the Act's new authorities and urging their use, where appropriate, in investigating and prosecuting terrorism and other criminal acts. We have followed up with additional guidance and training over the past year, and we consult informally with federal prosecutors and investigators at work in the field investigating suspected terrorists. Our manual proved invaluable in ensuring that prosecutors around the country could immediately benefit from and utilize the new law enforcement tools provided by the Act.

Law enforcement has been engaged in an ongoing cooperative effort to identify, disrupt and dismantle terrorist networks. We are expending every effort and devoting all available resources to intercept terrorists and defend our nation. Never was this so apparent as last Friday, a defining day in the war on terrorism, when we neutralized a suspected terrorist cell in Portland, Oregon, convicted attempted suicide bomber Richard Reid, and saw John Walker Lindh, an American captured fighting for the Taliban in Afghanistan, sentenced to twenty years' imprisonment. In the last six weeks, we have charged 17 individuals involved in terrorism-

related activities. In addition to Portland, we have broken up terrorist cells in Detroit and Buffalo, and we have charged an individual with attempting to set up an Al Qaeda terrorist training camp in Oregon. Enhanced penalties authorized by the USA PATRIOT Act have proven an important tool in all of these cases.

Today, I will provide a brief summary of the Department's work to date implementing the new powers authorized by the USA PATRIOT Act. I cannot, of course, disclose information that might compromise or undermine ongoing criminal investigations and prosecutions. However, I can discuss a number of areas in which the Department of Justice, in conjunction with other departments and agencies, is making meaningful headway in the war on terrorism. In particular, over the past year, the Department has used the following important new authorities and tools provided by the Act:

- we have charged a number of individuals with crimes under 18 U.S.C. §§2339A and 2339B, which prohibit providing material support to terrorists or terrorist organizations, and carry enhanced penalties;
- we have used newly streamlined authority to use trap and trace orders to track communications of a number of criminals, including the terrorist kidnappers and murderers of journalist Daniel Pearl, as well as identity thieves and a four-time murderer;
- we have used new authority to subpoena information about Internet users' network addresses to track down terrorists and computer hackers;
- we have used newly authorized nationwide search warrants for terrorist investigations at least three times, including during the ongoing anthrax investigation;
- we have utilized provisions in the Act to foster an unprecedented level of cooperation and information sharing between government agencies; and
- we have saved precious time and resources through a provision that permits officials to obtain court orders for electronic surveillance pertaining to a particular

suspect, rather than a particular device.

I will focus my testimony on four key areas in which the USA PATRIOT Act has aided law enforcement efforts: (1) it updated the law to reflect new technology; (2) it removed obstacles to investigating terrorism; (3) it strengthened criminal laws and enhanced penalties; and (4) it facilitated increased intelligence sharing, gathering and analyzing. The fifth key area, protecting our borders, falls within the bailiwick of the INS, which is also presenting testimony today.

**1. Updating the Law to Reflect New Technology**

First, the USA PATRIOT Act allowed us to modernize our badly outmoded surveillance tools. Terrorists engaged in covert multinational operations use advanced technology, particularly in their communications and planning. While terrorists who were plotting against our nation traveled across the globe, carrying laptop computers and using disposable cell phones, federal investigators operated under laws seemingly frozen in an era of telegrams and switchboard operators. Prior to September 11, we operated both at a technological disadvantage and under legal barriers that severely restricted our surveillance capabilities. In particular, we did not have sufficiently sophisticated abilities to monitor communications in either the digital or analog world, and law enforcement officials operated under onerous rules that hindered their ability to conduct investigations in a timely manner. The USA PATRIOT Act modernized existing law, and gave investigators crucial new tools to deal with these problems. We have put this new authority to good use.

Prior to the USA PATRIOT Act, for example, federal law required officers to spend critical time going through the burdensome process of obtaining wiretap orders to access

unopened voice-mail. Now, just as had already been the case with email messages, pursuant to section 209 of the PATRIOT Act, officers can use search warrants to expedite the seizure of voice mail. Federal investigators have used these warrants in a variety of criminal cases, including both foreign and domestic terrorism cases.

Similarly, section 220 of the Act, which permits a law enforcement officer to execute a search warrant for electronic evidence outside of the district that issued the warrant, has proved crucial to dealing with the post-September 11 deluge of search warrant applications seeking evidence stored in computers, or transmitted through the Internet. Before the PATRIOT Act, because a court sitting in one district could not issue a warrant that was valid in another district, officers' access to critical information in the Internet era was unnecessarily delayed and obstructed, as the physical infrastructure, such as servers used by internet service providers, were often located thousands of miles from the scene of the crime under investigation. Even though the internet is a far-flung communications network, with access available to anyone with a properly equipped personal computer, the federal courts in those districts in which ISPs happened to locate their servers (such as in northern California) were required to handle requests for warrants in investigations all across the country. The efficiency resulting from the Act's simple modifications to existing law was invaluable in several time-sensitive investigations, including one involving a dangerous fugitive and another involving a hacker who used stolen trade secrets to extort a company.

The USA PATRIOT Act also modernized the legal requirements for pen register and trap and trace orders, streamlining this authority by clarifying that it can be used in a variety of new communications forms, not just on telephone lines, and by permitting a single order nationwide.

These devices – which reveal, for example, the numbers dialed by a particular telephone or the email address to which an account sends messages – allow investigators to identify patterns of suspicious behavior or connections with known terrorists or terrorist organizations. The Department has used this improved tool to trace communications of a number of criminals, including kidnappers who communicated their demands via email, terrorist conspirators, at least one major drug distributor, identity thieves, a four-time murderer, and a fugitive who fled on the eve of trial using a fake passport. This new provision also allowed prosecutors in the Daniel Pearl case to get information critical in the identification of some of those individuals responsible for his kidnaping and murder.

The USA PATRIOT Act has updated federal law for the digital era by expediting the government's ability to execute orders requiring the help of third parties, such as telecommunications companies, in terrorism investigations. Under previous law, if an officer wanted to enlist the help of third parties to monitor a suspect, the officer had to seek specific court orders for every information source the suspect could potentially utilize. Section 206 of the Act abolished this requirement by permitting officers to simply obtain a court order pertaining to the suspect, not the particular device or devices used. This new authority allows us to avoid unnecessary cat-and-mouse games with terrorists who are trained to thwart surveillance by rapidly changing hotels or residences, cell phones, and Internet accounts before important meetings or communications.

Other provisions, such as section 211, which clarifies that the Electronic Communications Privacy Act, not the Cable Act, governs the disclosure of information regarding communication services provided by cable companies, and section 212, which allows internet providers to

disclose records to law enforcement in emergencies presenting a risk to life or limb, have made it much easier for third party communication providers to assist law enforcement without fear of civil liability. The latter authority, for example, allowed us to track down a student who posted electronic bulletin board threats to bomb his high school and shoot a faculty member and several students. Afraid of being sued, the owner and operator of the Internet message board initially resisted disclosing to federal law enforcement officials the evidence that could lead to the identification of the threat-maker. However, after he was told about the new USA PATRIOT Act emergency authority, he voluntarily disclosed to law enforcement Internet addressing information that was instrumental in the student's timely arrest and confession and in preventing the student from potentially carrying out his violent threats.

Finally, the USA PATRIOT Act has brought the federal wiretap statute into the 21st century by adding terrorism crimes to the list of offenses for which wiretap orders are available. These provisions have proven extremely useful to law enforcement officials. At least one recent wiretap order has been issued based on this expanded list of terrorism offenses. We believe that these enhancements will bring more terrorists to justice and prevent them from inflicting major damage on the infrastructure of telecommunications providers.

**2. Removing Obstacles to Investigating Terrorism**

Second, the USA PATRIOT Act has removed various obstacles to investigating terrorism and has greatly enhanced the Department's ability to thwart, disrupt, weaken, and eliminate the infrastructure of terrorist organizations. Section 219, for example, which allows federal judges to issue nationwide search warrants for physical searches in terrorism investigations, has enabled investigators to avoid expending precious time petitioning multiple judges in multiple districts

for warrants. We have used this provision at least three times, including during the ongoing anthrax investigation. In that case, agents were able to obtain a search warrant from a federal judge in Washington, D.C. in order to investigate the premises of America Media, Inc. in Boca Raton, Florida. Timely action is often of the essence in law enforcement investigations and this new authority will prove invaluable.

Prior to the USA PATRIOT Act, we faced significant barriers in our ability to exclude or remove terrorists because of various statutory loopholes in the definitions concerning terrorism. Section 411 of the USA PATRIOT Act addressed these problems by expanding the grounds of inadmissibility of aliens to include those who provide assistance to terrorist organizations. At the Attorney General's request, the Department of State has listed 46 entities as terrorist organizations pursuant to authority under this provision. Members of these organizations are now denied admission to the United States for any purpose.

We believe that a number of other areas, such as greater authority to collect DNA samples from federal prisoners convicted of certain terrorism offenses under section 503, greater ability to pay rewards to help punish terrorists under sections 501 and 502, enhanced capabilities to investigate computer fraud pursuant to section 506, which permits joint Secret Service-FBI cooperation in investigations, and greater access to education information and statistics under sections 507 and 508, likewise will prove very useful in our efforts. While we have not yet had to use all of the Act's provisions, we know that they will serve as vital tools should the need arise.

3. **Strengthening the Criminal Laws against Terrorism**.

Third, the USA PATRIOT Act substantially strengthened criminal law, helping us pursue

criminals in the most extensive criminal investigation in history. Critical to our efforts is the enhanced ability to prosecute and punish terrorists captured abroad as well as those arrested within our borders. These provisions have proven to be powerful new weapons in our fight against international terrorism as well as other kinds of international criminal activity.

Enhanced criminal laws relating to terrorist financing, for example, have provided an effective tool in getting law enforcement inserted into the early stages of terrorist planning. Title III of the USA PATRIOT Act provides law enforcement with important new authority to investigate and prosecute the financing of terrorism. We can now seize terrorist assets, both foreign and domestic, if the property or its owner is involved in, related to, or in support of acts of domestic or international terrorism. It is now a crime for anyone subject to U.S. jurisdiction to provide anything of value – including their own efforts or expertise – to organizations designated as "foreign terrorist organization." This is true regardless of whether the persons providing such support intend their donations to be used for violent purposes, or whether actual terrorism results. If someone subject to U.S. jurisdiction provides, or even attempts to provide, any material support or resources to Hamas, Hizballah, Al Qaeda, the Abu Sayyaf Group or any of the other designated groups, that person can be prosecuted. And our prosecutors do not have to prove that the support actually went to specific terrorist acts. The Department has used this provision in prosecuting a number of Al Qaeda associated individuals and in breaking up terrorist cells in this country. For example, John Walker Lindh, the American citizen who joined the Taliban and was captured by military forces in Afghanistan, was charged with 10 counts, including a total of six relating to providing material support to individuals and to organizations that commit crimes of terrorism. Lindh, who pled guilty to providing services to the Taliban and

to carrying an explosive while engaged in the commission of a felony, was sentenced last Friday to 20 years imprisonment. On August 28, 2002, we charged Ernest James Ujaama with providing material support to Al Qaeda by, among other things, attempting to set up an Al Qaeda terrorist training camp at a farm in Oregon. On that same day, five Detroit men affiliated with Al Qaeda were charged with providing material support or resources to terrorists. On September 13, 2002, six United States citizens in the Buffalo area, who are believed to be part of another Al Qaeda- affiliated cell, were arrested on charges of providing support or resources to terrorists. And just last Friday, we indicted six individuals in Portland, Oregon, also affiliated with Al Qaeda, with providing material support or resources to terrorists.

Our ability to fight transnational crime was further enhanced by making the smuggling of bulk cash across our border unlawful, adding terrorism and other offenses to the list of racketeering offenses, and providing prosecutors with the authority to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of such a foreign bank's funds held in a U.S. correspondent account. Another important provision expanded our ability to prosecute unlicenced money transmitters by enhancing section 1960 of Title 18. We used this revised statute successfully in the District of Massachusetts. On November 18, 2001, a federal grand jury returned an indictment charging Liban Hussein, the local president of an Al Barakaat money remitting house, and his brother, Mohamed Hussein, with a violation of § 1960. This prosecution was part of a national, and indeed international, enforcement action against the Al Barakaat network, which has financed the operations of Al Qaeda and other terrorist organizations. Mohamed Hussein was convicted and sentenced to 18 months' incarceration for operating an unlicenced money remitting business. His brother is a fugitive.

Title III of the Act also permits the forfeiture of funds held in United States interbank accounts. We used this provision to prosecute James Gibson, who had defrauded clients of millions of dollars by fraudulently structuring settlement for numerous personal injury victims. After he and his wife fled to Belize and deposited some of the monies from the scheme in two Belizean banks, we were able to have a seizure warrant served on the bank's interbank account in the United States and recover remaining funds.

We have attempted to use section 801, which makes it a federal offense to engage in terrorist attacks and other acts of violence against mass transportation systems, in at least one high profile case. One of the counts brought against "shoe bomber" Richard Reid, who was charged for concealing a bomb in his shoe during a transatlantic flight, alleged a violation of terrorist attacks and other acts of violence against mass transportation systems. This charge was dismissed after the judge determined that the definition of mass transportation does not include airplanes. In the meantime, Richard Reid pleaded guilty to the remaining counts brought against him last Friday. He will be sentenced in January and faces a sentence of 60 years to life.

We will continue to use these enhanced capabilities to bring those associated with terrorism to justice.

**4. Enhancing the Capacity of Law Enforcement to Gather, Analyze and Share Intelligence**

Finally, and perhaps most significantly, the USA PATRIOT Act allowed us to significantly enhance our capability to share information and coordinate our efforts. Immediately following the September 11 attacks, the Attorney General ordered a top-to-bottom review and reorganization of the Department of Justice in order to effectively mobilize our law enforcement

resources and justice system. The Attorney General's review found that restrictions imposed decades ago were severely impeding our intelligence gathering and sharing capabilities. As FBI Director Mueller stated several weeks ago before the House Financial Services Committee, "creating an alliance between law enforcement and intelligence agencies is the key to dismantling terrorist organizations and eliminating the threat they pose."

The USA PATRIOT Act fosters this communication across agency lines, breaking down once formidable barriers previously in place. Prior to last October, there was no mechanism for sharing certain types of criminal investigative material with the intelligence community, and the intelligence community could not easily open their files to law enforcement. Sharing was possible, but only in limited situations and through onerous procedures that diverted resources from investigative activity. The loosening of these procedures under section 203 of the USA PATRIOT Act has been invaluable. We are now enjoying an unprecedented level of cooperation and information-sharing between and among U.S. government agencies involved in counter-terrorism. The Department, for example, has made disclosures of information obtained through grand juries and involving foreign intelligence on over forty occasions, and in compliance with section 203, we have filed disclosure notices or obtained prior approval from the courts in at least 38 districts.

On September 23, 2002, the Attorney General announced three new guidelines designed to institutionalize the ongoing sharing of information between federal law enforcement and the U.S. intelligence community. These guidelines formalize the existing framework for information sharing to ensure that vital intelligence information ends up in the hands of those officials who need it most, while respecting the interests generally protected by grand jury

secrecy and wiretap rules.

The Act also allocated funds to the FBI to help facilitate information sharing with the INS and State Department via the National Crime Information Center (NCIC). Access to these files has enabled agencies to better determine whether a visa applicant has a criminal history record. The importance of this system cannot be underestimated. It is the nation's principal law enforcement automated information sharing tool. On April 11, 2002, the Attorney General issued a major directive on the coordination of information relating to terrorism that requires all investigative components within the Department of Justice to provide the names, photographs, and other identifying data of all known or suspected terrorists for inclusion in the database. Since enactment, the FBI has provided the State Department with over 8.4 million records from these databases, and has provided 83,000 comprehensive records of key wanted persons in the databases, as well as information regarding military detainees in Afghanistan, Pakistan, and Guantanamo Bay to the INS.

The USA PATRIOT Act has also improved the effectiveness of the Foreign Intelligence Surveillance Act by permitting the authorization of physical searches and electronic surveillance of foreign powers' employees for up to 120 days, as opposed to the previous 45 days. This additional leeway gives government investigators targeting potential terrorist activity additional time and helps clear court dockets for more far-reaching terrorism related cases and other complex federal prosecution. While the details of FISA operations are classified, I can tell you that this improvement has saved critical time that law enforcement previously spent continuously renewing court orders. Additionally, section 218, which broadened the applicable standard under which law enforcement could conduct FISA surveillance or searches, has reduced officers' need

to weigh constantly the purposes of their investigation, and has allowed for increased collaboration between law enforcement and intelligence personnel.

**Conclusion**

I would like to conclude by thanking the members of this Committee for your efforts in so swiftly developing and passing the USA PATRIOT Act in the wake of last year's attacks on our nation. Your response enabled those of us whose mission it is to combat terrorists at home and abroad to do so with a wide array of new measures that have greatly enhanced our ability to carry out this work. We look forward to continuing to work with the Committee in this collaborative effort. I thank you for your invitation and welcome any questions that you may have.

Statement
*United States Senate Committee on the Judiciary*
**Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland.**
**October 9, 2002**

**The Honorable Orrin Hatch**
United States Senator , Utah

---

Thank you Mrs. Chairman. I want to commend you for holding a hearing on this important topic. I, for one, am proud of the way that Congress has come together on issues of national security since the horrific attacks of September 11. In the wake of those tragic events we worked tirelessly to pass, by a near-unanimous vote of 99-1, the PATRIOT Act which included a critical set of reforms needed to unleash our government's ability to detect and prevent terrorist attacks.

Earlier this year, we continued our bipartisan efforts by unanimously passing the Enhanced Border Security and Visa Entry Reform Act. Like the PATRIOT Act, this legislation concluded long overdue common sense reforms needed to enhance our nation's security.

And It is my hope that enough of that robust bipartisan spirit remains today to overcome our differences and enact landmark legislation to create a Department of Homeland Security by the end of this year.

As the anniversary of the September 11 terrorist attacks that killed thousands of innocent Americans has just passed, it is critical that we examine whether the legislative reforms contained in the PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act have been successful. And it is equally important that we assess whether there is more we in Congress can do to ensure that our law enforcement and intelligence officials have all the tools they need to detect and prevent future terrorist attacks. While I am proud of our efforts to date, I believe that there are a number of additional legislative reforms that we should consider to assist our law enforcement and intelligence communities in their efforts to combat terrorism.

For example, with respect to the Foreign Intelligence Surveillance Act (FISA), I believe Senators Kyl and Schumer have identified a significant problem with the Act - the so-called "lone wolf" problem. Although the Joint Intelligence Committee held a hearing in July to consider the legislation, I am disappointed that the bill - which enjoys bipartisan support, as well as the support of the Administration - has not yet become law. There is little time left to do so, but I remain hopeful that Congress will enact this legislation this year.

I am also concerned that existing statutory constraints on the authority of federal officials to share such information with their state, local and international counterparts may be hindering our national efforts to combat terrorism. The events of September 11 have made it abundantly clear that we must improve our ability to gather, share, and analyze information within and among our federal, state and local agencies, as well as with our international allies. While the PATRIOT Act enhanced the ability of federal law enforcement and intelligence authorities to share grand jury and other sensitive information with one another, it did not address the sharing of information with state, local and international officials. This is another area I believe Congress needs to address.

Similarly, we may well need to revisit provisions of the PATRIOT Act that were intended to alleviate the problems created by the so-called wall that limits the sharing of foreign intelligence information between intelligence agents and criminal agents and prosecutors. Prior to September 11, we in Congress were well aware of these problems which were highlighted in reports prepared by Randy Bellows and

the General Accounting Office. And there is little question that we included provisions in the PATRIOT Act to alleviate these problems. However, the precise scope of the level of coordination that was envisioned by the Act is currently under review by the Foreign Intelligence Surveillance Court of Review. Depending on the FISA court's ruling, we may need to consider additional legislation to address this issue.

These are just a few of the potential areas of legislative reform I believe Congress should consider. I am certain that our distinguished witnesses have much to contribute on this topic. I look forward to your testimony, and I thank all of you for appearing here today.

###

**Statement for the Record**
**Before the Subcommittee on Technology, Terrorism, and Government Information**
**Committee on the Judiciary**
**United States Senate**

# HHS's Progress in Implementing Recently Enacted Legislation to Combat Terrorism

*Statement of*

## Jerome M. Hauer, M.H.S.

***Acting Assistant Secretary for Public Health Emergency Preparedness***
***U.S. Department of Health and Human Services***

**For**
**Release on Delivery**
**Expected at 10:00 am**
**on Wednesday, October 9, 2002**

The Department of Health and Human Services (HHS) welcomes the interest of the Subcommittee in the implementation status of recently enacted statutes to combat terrorism and appreciates the opportunity to report on relevant activities. HHS looks forward to working with the Subcommittee toward ensuring that the full impact of these statutes is realized as soon as possible.

## A. Time lines for promulgation of regulations ensuing from the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

### 1. Select Agents:

Select Agents are dangerous pathogens or toxins that warrant special precautions lest they prove harmful to laboratory workers or other individuals who come into contact with them. Terrorists could use Select Agents to initiate outbreaks of infectious disease or otherwise threaten the health and safety of Americans. Recognizing that the scientific and medical communities must continue to have access to Select Agents for research and other peaceful purposes, the Act calls for updating the list of Select Agents and for broadening the scope of their regulation to include possession and use as well as transfer between registered laboratory facilities.

Following intensive review by experts, the Centers for Disease Control and Prevention (CDC) published a proposed updated Select Agent list on August 23, 2002. Upon completion of its analysis of the public comments, HHS plans to finalize the list

and include it in an Interim Final Rule, which also will include updated requirements for laboratory safety and security. This Rule is to be published on December 9, 2002.

**2. Food Safety:**

The Act provides several new authorities to enhance the ability of the Food and Drug Administration (FDA) to protect the U. S. food supply.

**a. Prior Notice of Imported Shipments**

FDA has drafted a concept paper regarding the envisioned rule. The next steps involve drafting a codified rule and associated preamble and preparing the supporting analyses for the rule. These several documents will be reviewed thoroughly within the HHS and the Executive Office of the President. The target date for publication of the proposed rule for public comment is December 30, 2002.

**b. Registration of Food Facilities**

FDA has drafted a concept paper regarding the envisioned rule. The next steps involve drafting a codified rule and associated preamble and preparing the supporting analyses for the rule. These several documents will be reviewed thoroughly within the HHS and the Executive Office of the President. The target date for publication of the proposed rule for public comment is December 30, 2002.

**c. Administrative Detention of Suspect Foods**

FDA has drafted a concept paper regarding the envisioned rule. The next steps involve drafting a codified rule and associated preamble and preparing the supporting analyses for the rule. These several documents will be reviewed thoroughly within the HHS and the Executive Office of the President. The target date for publication of the proposed rule for public comment is February 11, 2003.

**d. Establishment and Maintenance of Records to Identify Immediate Previous Source and Immediate Subsequent Recipient of Foods**

FDA has drafted a concept paper regarding the envisioned rule. The next steps involve drafting a codified rule and associated preamble and preparing the supporting analyses for the rule. These several documents will be reviewed thoroughly within the HHS and the Executive Office of the President. The target date for publication of the proposed rule for public comment is February 11, 2003.

**B. Interim Notification of Possession of Select Agents.**

The Act calls for implementation of the requirement that, within 90 days of enactment, all non-exempt persons notify HHS of their possession of Select Agents. In collaboration with the U. S. Department of Agriculture, CDC sent notice of this

requirement to over 200,000 persons who were judged to be potential possessors of Select Agents. CDC also provided Notice of Possession forms (OMB Control Number 0920-0561) to facilitate their reporting whether they do or do not possess any of the listed agents. Thus far, over 100,000 persons have responded. On or about October 18, CDC plans to send reminder notices to all those who did not respond to the initial notice. Additional information can be found at the following web address: http://www.cdc.gov/od/ohs/lrsat/possess.htm.

**C. Data Base regarding Possession and Use of Select Agents.**

The Act calls for development of a comprehensive database that includes the names and locations of registered persons, the listed agents and toxins such persons are possessing, using, or transferring, and information regarding the characterization of such agents and toxins. CDC is preparing the statement of requirements necessary to initiate a contract to develop the database. CDC expects to issue a solicitation for contract proposals in early 2003.

**Statement for the Record**

**Dennis Lormel**
**Chief, Terrorist Financing Operations Section,**
**Counterterrorism Division,**
**Federal Bureau of Investigation**
**Before The Senate Judiciary Committee**
**Subcommittee on Technology, Terrorism, and Government Information**

**October 9, 2002**

**Introduction**

Good morning, Madam Chairman, and members of the Subcommittee on Technology, Terrorism, and Government Information. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittee for affording us the opportunity to participate in this forum and to update the Subcommittee on our use of the tools established within the framework of the USA PATRIOT Act and the work being conducted by our Terrorism Financing Operations Section.

As this Subcommittee is well aware, the FBI, in conjunction with law enforcement and intelligence agencies throughout the United States and the world, is engaged in the largest, most complex and perhaps the most critical criminal and terrorism investigation in our history. The FBI continues to dedicate considerable resources to this investigation and remains committed to determining the full scope of these terrorist acts, identifying all those involved in planning, executing and/or assisting in any manner the commission of these acts and others, and bringing those responsible to justice. The FBI will continue to exercise its leadership role in the global war on terrorism by taking all possible steps to prevent any further acts of terrorism.

The war on terrorism will be a long-term battle. It will not be won overnight nor will it be won without the highest levels of cooperation and coordination among law enforcement and intelligence agencies around the globe. Terrorism knows no borders or boundaries. The threat is not limited to any one region of the world. Law enforcement and intelligence agencies throughout the world possess tremendous resources and expertise. Allying these resources against the common enemy of terrorism is the key to dismantling these organizations and eliminating the threat they pose. Make no mistake about it, even with the combined resources and expertise possessed by law enforcement, the threat posed by terrorism is grave. Terrorists do not play by the rules of a civilized society, nor do they respect human decency. They will stop at nothing to commit acts of terror.

From a law enforcement perspective, success in the war on terrorism must be measured in our ability to prevent future acts of terrorism. Whether it be through prosecution, disruption, blocking/freezing of funds, or allowing a funding mechanism to remain in place in order to further an investigation, prevention remains the overarching focus. In this regard, fighting the war on terrorism requires powerful tools. The FBI appreciates the tools provided by the Congress in enacting the USA Patriot Act, including those contained within Title III of this Act, which is also know as the International Money Laundering Anti-Terrorist Financing Act of 2001.

**The Terrorist Financing Operations Section (TFOS)**

I would like to start my discussion regarding the FBI's use of the USA Patriot by focusing on the tools provided within Title III. To illustrate how these anti-money laundering provisions aid our investigative efforts, it is necessary to understand how the FBI has been re-structured to address terrorist financing matters. Identifying and tracking the financial structure supporting terrorist groups is critical to dismantling the organization and preventing future attacks. As in ordinary criminal investigations, "following the money" identifies, links, and develops evidence against those involved in criminal activity. In the early stages of the investigation into the events of September 11, 2001, it was financial evidence that quickly established links between the hijackers and identified co-conspirators.

It was also in the early stages of this investigation that the FBI and Department of Justice (DOJ) identified a critical need for a more comprehensive, centralized approach to terrorist financial matters. In response, the FBI established an interagency Terrorism Financial Review Group (TFRG), operating out of FBI Headquarters. By bringing together vast databases and the expertise of numerous federal agencies, the TFRG, which was subsequently expanded, renamed the Terrorist Financing Operations Section (TFOS), and assigned to the FBI's Counterterrorism Division, focuses a powerful array of resources on the financial tentacles of terrorist organizations.

The TFRG was created with a two-fold mission. First, it was designed to conduct a comprehensive financial analysis of the 19 hijackers to link them together and to

identify their financial support structure within the United States and abroad. Through the execution of this mission, the TFRG was able to establish how the hijackers responsible for the attacks received their money, details of their flight training, where they lived, and details concerning individuals associated with the hijackers. The 19 hijackers opened 24 domestic bank accounts at four different banks. The TFOS analyzed the data associated with these accounts to develop a financial profile that has been used in connection with the FBI's investigation regarding the events of September 11, 2001.

The second aspect of the TFRG's mission was to serve as a template for preventive and predictive terrorist financial investigations. This mission, consistent with the TFRG's restructuring into the TFOS, has since evolved into a broader effort to identify, investigate, prosecute, disrupt, and dismantle all terrorist-related financial and fund-raising activities.

To accomplish this mission, the TFOS has implemented initiatives to address all aspects of terrorist financing. For example, the TFOS is engaged in an aggressive international outreach program to share information regarding terrorist financing methods with the financial community and law enforcement, and has built upon long-established relationships with the financial services community in the United States and abroad. The international outreach initiative is coordinated through the network of FBI Legal Attache Offices located in 44 key cities worldwide, providing coverage for more than 200 countries and territories.

As touched upon earlier, a significant focus of the TFOS' efforts is prediction and

prevention. In this regard, it has developed numerous data mining projects to provide further predictive abilities and maximize the use of both public and private database information. These efforts are complemented by the centralized terrorist financial database which the TFOS developed in connection with its coordination of financial investigation of individuals and groups who are suspects of FBI terrorism investigations. The TFOS has cataloged and reviewed financial documents obtained as a result of numerous financial subpoenas pertaining to individuals and accounts. These documents have been verified as being of investigatory interest and have been entered into the terrorist financial database for linkage analysis. The TFOS has obtained financial information from FBI Field Divisions and Legal Attache Offices, and has reviewed and documented financial transactions. These records include foreign bank accounts and foreign wire transfers. The information contained within the aforementioned database is being used to identify terrorist cells operating in the United States and abroad to prevent further terrorist acts. The TFOS meets regularly with representatives from the banking community and the financial services industry to share information and to refine methods to detect and identify potential terrorists around the world.

The TFOS created and continues to update a financial control list which contains names and identifying data for individuals under investigation for potential links to terrorist organizations. These lists are regularly shared with domestic and international law enforcement and intelligence agencies, and with the Federal Reserve Board, which disseminates the lists to financial institutions so they can flag suspicious financial activity.

The TFOS regularly shares information with Customs' Operation Green Quest and provides daily downloads from its database to Green Quest and the Financial Crimes Enforcement Network (FinCEN). Further, the TFOS is working with FinCEN to explore new ways to data mine the Suspicious Activity Report (SAR), Currency Transaction Report (CTR), and Currency and Monetary Instrument Report databases.

Based on its international investigative abilities, and its close association with the Intelligence Community, the TFOS is in a unique position to coordinate anti-terrorism financial investigations and to ensure those investigations are coordinated with the goals and objectives of the FBI's Counterterrorism Program.

**Use of the USA PATRIOT Act**

I would now like to discuss how the TFOS has been making use of the tools established by the USA PATRIOT Act. Terrorist financing methods range from the highly sophisticated to the most basic. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, bulk cash smuggling, identity theft, credit card fraud, and other criminal operations. Informal Value Transfer Systems, such as "Hawalas," also present problems for law enforcement. They permit terrorists a means of transferring funds that is difficult to detect and trace. These informal systems are commonplace and appear to serve as an efficient means of transacting in mostly "cash" societies such as Pakistan, Afghanistan, and the Phillippines. In applying provisions of the USA PATRIOT Act we

seek to erode the effectiveness of such methods without unduly undermining the legitimate economic activity that may rely on them. The Act establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file SARs, and certain cash businesses to register with FinCEN and file SARs for a wider range of financial transactions.

The Act contains many other provisions that the FBI believes will considerably aid our efforts to address terrorist financing. These include the authority to seize terrorist assets, and the addition of terrorism and other offenses to the list of racketeering offenses. The utilization of this aspect of the USA PATRIOT Act is perhaps best exemplified through actions that have been taken against Non-Governmental Organizations (NGOs) believed to provide financial support to know Foreign Terrorist Organizations and other affiliated Terrorist Cells. As in the case of Halawas, the funding of terrorist organizations such as Al Qaeda and Hamas through NGOs and charitable organizations represents a significant challenge to law enforcement. Funding of terrorism through NGOs is a prime focus of terrorist financial investigations. NGOs may be large international organizations which can be exploited by individual employees sympathetic to terrorist causes through local branch offices; they may be private NGOs which exist solely to support a militant cause; or they may be closely affiliated with a state sponsor of terrorism. One of the challenges in investigations involving terrorist fund-raising through NGOs is distinguishing terrorist fund-raising activities from legitimate or what may appear to be legitimate charitable fund-raising. Fund-raising on the part of terrorist

groups which on the surface appear to be efforts to "help the poor" or fund-raising for charitable, humanitarian or other legitimate purposes actually falls squarely in the realm of logistical support for terrorist activity.

As a participant on the National Security Council's Policy Coordinating Committee (PCC) on terrorist finance, the TFOS participates in the effort to target NGOs believed to provide financial support to known Foreign Terrorist Organizations and affiliated terrorist cells. The PCC coordinates the development and implementation of policies to combat terrorist financing and provides analysis on these issues. Numerous FBI Field Offices have open investigations into organizations that may be funneling money to Foreign Terrorist Organizations and the TFOS has acted as a clearinghouse for these cases and has summarized the collected data.

In order to disrupt terrorist financing channels, the TFOS has coordinated FBI terrorist investigations with the terrorist designation and asset freezing efforts of the OFAC and Operation Green Quest. These efforts have resulted in the freezing of millions of dollars in foreign and US bank accounts. Specifically, the joint efforts targeting Al-Barakaat, the Holy Land Foundation for Relief and Development, the Global Relief Foundation, and the Benevolence International Foundation have resulted in the execution of numerous search warrants and the disruption of the fund-raising and money remittance operations of these and other organizations. Financial investigations of these entities have revealed that approximately $200 million in contributions passed through these organizations each year.

The USA PATRIOT Act also enables prosecutors to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of a foreign bank's funds held in a U.S. correspondent account. Other important provisions expand the ability to prosecute unlicenced money transmitters, allow law enforcement faster access to reports of currency transactions in excess of $10,000, and provide authority for the service of administrative subpoenas on foreign banks concerning records of foreign transactions. This latter provision allows law enforcement to obtain critical information in an investigation on a more timely basis than was possible before. In counterterrorism investigations, of course, speed is of the essence because prevention is the goal.

Section 362 of the USA PATRIOT Act mandates that FinCEN establish a highly secure network to 1) allow financial institutions to file SARs and CTRs on-line, and 2) "provide financial institutions with alerts and other information regarding suspicious activities that warrant immediate and enhanced scrutiny." FinCEN has developed the USA Patriot Act Communication System to meet this mandate and is implementing the system. This will be a valuable tool for law enforcement, but it will require the full cooperation of private financial institutions. The TFOS has worked with financial institutions, and has provided to them information to help detect patterns of activity possibly associated with terrorist activity and the PACS will help considerably in these efforts.

**Use of Other Provisions of the USA PATRIOT Act**

In addition to the provisions effecting changes to money laundering statutes, the USA

PATRIOT Act effected changes in national security authorities, the substantive criminal law, immigration law, and victim assistance statutes, and other areas. In particular, the Act seeks to improve the efficiency of the process associated with the FBI's conduct of electronic surveillance and physical searches authorized through the Foreign Intelligence Surveillance Act (FISA) of 1978 and to remove barriers to the timely sharing of information between counterintelligence and counterterrorism intelligence operations and criminal investigations. These enhancements in efficiency improve our ability to detect and prosecute offenders, and with less disruption to legitimate commerce. I would now like to highlight those provisions that the FBI has been utilizing most often in connection with the execution of its counterterrorism responsibilities.

**Changes in Predicate Standards for National Security Letters (NSLs)**

NSLs are administrative subpoenas that are issued in counterintelligence and counterterrorism investigations to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, or ECPA); records from financial institutions (pursuant to the Right to Financial Privacy Act); and information from credit bureaus (pursuant to the Fair Credit Reporting Act). Delay in obtaining NSLs has long been identified as a significant problem relative to the conduct of counterintelligence and counterterrorism investigations. Two factors contributed most prominently to this delay. These were the complexity of the standard predication for NSLs and the requirement that signature authority be restricted to officials no lower than a Deputy Assistant Director at FBI Headquarters.

Section 505 of the USA Patriot changed the standard predication for all three types of NSLs to one requiring that the information being sought through the NSL is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Prior to the Act, the statutes required both relevance and "specific and articulable facts" giving reason to believe that the subject is an agent of a foreign power, or, in the case of subscriber requests, had been in contact with such an agent. This "agent of a foreign power" prong of the standard made it necessary to collect and document specific facts demonstrating that the standard had been met. This requirement and the complexity of the standard itself often led to extensive delays in generating NSLs.

Section 505 also allowed the Director to delegate signature authority for NSLs to Special Agents in Charge serving in designated field divisions. The provisions delineated within Section 505 have resulted in investigators receiving the data needed in the furtherance of ongoing investigations in a more timely fashion, which in turn has had a positive impact on numerous investigations.

**"Roving" FISA Electronic Surveillance Authority**

Section 206 of the USA PATRIOT Act amends FISA to allow the FISC to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This

means that, when a FISA target engages in conduct that has the effect of defeating electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," to effect the authorized electronic surveillance.

**Changes in the Duration of FISA Authority**

Section 207 of the Act extends the standard duration for several categories of FISC Orders. First, the section allow for electronic surveillances and search orders on non-US person agents of a foreign power pled under Section 101(b)(1)(A) of the FISA, to run for an initial period of 120 days, instead of 90, and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases, which applies to US persons and non-officer/employee targets, from 45 to 90 days. These extension provisions have resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under the FISA.

**Expansion of the FISC**

Section 207 also expanded the FISC from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area. This has increased the availability of FISC judges and has resulted in the convening of the FISC on a weekly basis, which has enabled the FBI to implement FISA-authorized collection operations in a more timely fashion.

**Changes in FISA Pen Register/Trap and Trace Authority**

Section 214 of the Act makes a substantial revision to the standard for a FISA-authorized pen register/trap and trace. Prior to the USA PATRIOT Act, FISA-authorized pen

registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA-authorized pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized in full investigations properly opened under the AG Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. Finally, the new standard does not mean that FISA pen register/trap and trace authority is only available on the subjects of investigations. The authority is available when the information sought is "relevant" to the investigation, as described above. For example, information concerning apparent associates or, or individuals in contact with, the subject of an investigation, may be relevant.

**Conclusion**

The USA PATRIOT Act has provided the FBI with improved tools for conducting

counterterrorism and counterintelligence investigations. These new tools require DOJ and the FBI to gain a complete understanding of the provisions, develop guidelines and protocols for their appropriate use, and educate investigators and prosecutors. In addition, many of the provisions require the Department of Treasury to issue new regulations and rules. While all of this is being done as expeditiously as possible, the full impact of the tools provided by the USA PATRIOT Act are yet to be seen. The FBI is continuing to digest its provisions, develop guidelines and protocols for its appropriate use, and educate investigators and prosecutors. Nevertheless, the Act enhances the ability of law enforcement and intelligence agencies to achieve our common goal of preventing acts of terrorism, without compromising the civil liberties and Constitutional protections enjoyed by our citizens. Thank you for this opportunity to appear today. I welcome any questions you have.

TESTIMONY OF DEPTY UNDERSECRETARY FOR TECHNOLOGY BEN WU

BEFORE SENATE JUDICIARY SUBCOMMITTEE ON

TECHNOLOGY, TERRORISM AND GOVERNMENT INFORMATION

OCTOBER 9, 2002

ON THE U.S PATRIOT ACT AND

THE ENHANCED BORDER SECURITY AND VISA REFORM ACT

Good morning. I am Ben Wu, Deputy Under Secretary for Technology of the Department of Commerce. Thank you for inviting me to discuss the work of the National Institute of Standards and Technology under the U.S.A. Patriot Act and the Enhanced Border Security and Visa Reform Act. The Technology Administration (TA) is the only Federal agency working to maximize technology's contribution to America's economic growth. The National Institute of Standards and Technology (NIST), a part of the Technology Administration, works with industry to develop measurements, standards and a variety of technologies. Our efforts are designed to enhance American productivity, facilitate trade and improve the quality of life.

NIST has four related programs: The laboratories, including the Information Technology Laboratory that works with the biometrics industry. The Baldrige National Quality Program, which promotes excellence in business, health care and education. The Advanced Technology Program, which funds high-risk private sector research on promising technologies that have the potential for making a broad impact on economic growth. And the Manufacturing Extension Partnership, in which NIST works with 2,000 manufacturing specialists and staff at affiliated centers around the country. NIST has a staff of some 3,000 scientists, engineers and other personnel, and about 1,600 visiting researchers.

Last year's terrorist attacks on the Pentagon and the World Trade Center taught us a great deal about our strengths and weaknesses as a nation. We witnessed great courage on the part of men and women in the military, fire fighters, police officers and ordinary citizens. And many of us experienced an unfamiliar sense of vulnerability. Yet, in some ways, the attacks have backfired on the perpetrators. They sparked a sense of solidarity among Americans, and strengthened our determination to enhance the security of our citizens.

President Bush, the entire administration, and the Commerce Department are committed to strengthening homeland security while maintaining American leadership in science and technology and accelerating the pace of scientific discovery and technological innovation.

Systems using biometrics—automated methods of recognizing a person based on physiological or behavioral characteristics—are increasingly being used to verify identities and restrict access to buildings, computer networks, and other secure sites. In our view, biometric technologies are a part of a needed foundation for secure identification. Biometric technologies can support homeland security, prevent ID fraud and play a role in supporting confidential financial transactions. In the biometrics arena, NIST has worked with industry and other government agencies for years.

**Improved Biometrics Critical to Border Security**

The successful use of the classic biometric, fingerprints, owes much to NIST research and development. For more than 30 years, NIST computer scientists have helped the FBI improve the automation process for matching "rolled" fingerprints taken by law enforcement agencies or "latent" prints found at crime scenes against the FBI's master file of fingerprints. NIST test data have been used to develop automated systems that can correctly match fingerprints by the minutiae, or tiny details, that investigators previously had to read by hand. In cooperation with the American National Standards Institute (ANSI), NIST also developed a uniform way for fingerprint, facial, scar, mark, and tattoo data to be exchanged between different jurisdictions and between dissimilar systems made by different manufacturers.

In conjunction with the FBI, NIST has developed several databases, including one consisting of 258 latent fingerprints and their matching "rolled" file prints. This database can be used by researchers and commercial developers to create and test new fingerprint identification algorithms, test commercial and research systems that conform to the NIST/ANSI standard, and assist in training latent fingerprint examiners. The increasing use of specialized "live" fingerprint scanners will help ensure that a high-quality fingerprint can be captured quickly and added to the FBI's current files. Use of these scanners also should speed up the matching of fingerprints against the FBI database of more than 40 million prints.

Computer scientists at NIST also have extensive experience working with systems that match facial images. While facial recognition systems employ different algorithms than fingerprint systems, many of the underlying methods for testing the accuracy of these systems are the same.

This work has been extended to include the specific biometric systems and scenarios required for visa systems under the Patriot Act, as amended by the Enhanced Border Security and Visa Reform Act. NIST has statutory responsibilities to develop and certify a technology standard that can be used to verify the identity of persons applying for a U.S. visa or using a visa to enter the country. The Department of Justice and Department of State also expect NIST to certify the accuracy of specific government and commercial systems being considered for use in this visa system.

These acts call for developing and certifying a technology standard for verifying the identity of individuals, and determining the accuracy of biometrics. NIST is spearheading the Face Recognition Vendor Test 2002, which is evaluating automated facial recognition systems that eventually could be used in the identification and verification process for people who apply for visas to visit the United States. The significance of the Face Recognition Vendor Test 2002 is evident by its large number of sponsors and supporters; this includes sixteen government departments and agencies. The current evaluation builds on the success NIST personnel have had in evaluating face recognition systems over the last decade. The evaluation methodology developed for FRVT 2002 will become a standard for evaluating other biometric technology. We will learn precisely how accurate and reliable these new systems are.

Fourteen companies participated in FRVT 2002. We deliberately designed a tough test that involved matching extremely challenging real world images. It required participants to process a set of about 121,000 images, and match all possible pairs of images from the 121,000 image set. In other words, this required some 15 billion matches. As you can imagine, this generated a mountain of data, and we are crunching all the numbers to see how well the systems worked.

This program will produce standard measurements of accuracy for biometric systems, standard XML-based scoring software, and accuracy measurements for specific biometrics required for the system scenarios mandated under the Border Security Act. We hope this work will have wide

impact beyond the mandated systems; standard test methods are likely to be accepted as international standards, and discussions are under way concerning the use of these same standards for airport security.

Later this year, NIST expects to submit its report on this work to the State and Justice Departments for transmittal to the U.S. Congress. The report will make a recommendation on which biometric, or combination of biometrics, would best secure the nation's borders.

**NIST Plays Key Role in Biometric Standards**

Open consensus standards, and associated testing, are critical to providing higher levels of security through biometric identification systems. Throughout the years, NIST has worked in partnership with U.S. industry and other federal agencies to establish formal groups for accelerating national and international biometric standardization. Two recent additions to the list are the Technical Committee M1 on Biometrics, started in November 2001 by the executive board of the International Committee for Information Technology Standards (INCITS), and a new subcommittee on biometrics (the Joint Technical Committee 1 SC 37-Biometrics) created in June 2002 by the International Organization on Standardization (ISO). A NIST biometric expert is serving as chair of the former and acting chair of the latter.

The Biometric Consortium serves as the federal government's focal point for research, development, testing, evaluation and application of biometric-based personal identification and verification technology. The consortium now has more than 900 members, including 60 government agencies. NIST and the National Security Agency co-chair the consortium. NIST has collaborated with the consortium, the biometric industry, and other biometric organizations to create a Common Biometric Exchange File Format (CBEFF). The format already is part of government requirements for data interchange and is being adopted by the biometric industry. The specification is a candidate for fast track approval as an ANSI standard and as an international standard for exchange of many types of biometric data files, including data on fingerprints, faces, palm prints, retinas, and iris and voice patterns.

Just a few years ago NIST computer scientists did some innovative work that significantly extends the range of fingerprint matching capabilities available to law enforcement officers. Working with the FBI, we developed software that enhances low-quality fingerprints for electronic matching. Low-quality fingerprints are precisely the kind you are most likely to find at a crime scene. They are the opposite of the carefully done prints you get when a suspect is booked at a police station. Those are relatively easy to match electronically. Trying to make a match based on the latent fingerprints found at crime scenes is much more difficult. Typically, investigators have to work with smudged, partial prints that are naturally of poor quality.

Until recently, matching these crime scene fingerprints electronically with those in the FBI's database was almost impossible. The new software we developed in cooperation with the FBI makes it possible to search the entire FBI database, instead of only part of it. It also allows law enforcement agencies in different locations to exchange fingerprint information directly, instead of always working through a national database. The software speeds up and automates what had been a very laborious process.

Both the national and international communities need this work to be done, and time is a compelling factor for new homeland security applications. As you can see, there is much important work still to be done. When the private sector and universities team up with federal and state government, we succeed in leveraging the available resources. Thank you, Madame Chairwoman, I will be pleased to answer any questions you have.

○