

**USING INFORMATION TECHNOLOGY TO SECURE
AMERICA'S BORDERS: INS PROBLEMS WITH
PLANNING AND IMPLEMENTATION**

HEARING
BEFORE THE
SUBCOMMITTEE ON
IMMIGRATION AND CLAIMS
OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED SEVENTH CONGRESS
FIRST SESSION

—————
OCTOBER 11, 2001
—————

Serial No. 43
—————

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

—————
U.S. GOVERNMENT PRINTING OFFICE

75-673 PDF

WASHINGTON : 2001

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

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
ED BRYANT, Tennessee	MELVIN L. WATT, North Carolina
STEVE CHABOT, Ohio	ZOE LOFGREN, California
BOB BARR, Georgia	SHEILA JACKSON LEE, Texas
WILLIAM L. JENKINS, Tennessee	MAXINE WATERS, California
ASA HUTCHINSON, Arkansas	MARTIN T. MEEHAN, Massachusetts
CHRIS CANNON, Utah	WILLIAM D. DELAHUNT, Massachusetts
LINDSEY O. GRAHAM, South Carolina	ROBERT WEXLER, Florida
SPENCER BACHUS, Alabama	TAMMY BALDWIN, Wisconsin
JOE SCARBOROUGH, Florida	ANTHONY D. WEINER, New York
JOHN N. HOSTETTLER, Indiana	ADAM B. SCHIFF, California
MARK GREEN, Wisconsin	
RIC KELLER, Florida	
DARRELL E. ISSA, California	
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	
MIKE PENCE, Indiana	

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON IMMIGRATION AND CLAIMS

GEORGE W. GEKAS, Pennsylvania, *Chairman*

DARRELL E. ISSA, California	SHEILA JACKSON LEE, Texas
MELISSA A. HART, Pennsylvania	BARNEY FRANK, Massachusetts
LAMAR SMITH, Texas	HOWARD L. BERMAN, California
ELTON GALLEGLY, California	ZOE LOFGREN, California
CHRIS CANNON, Utah, <i>Vice Chair</i>	MARTIN T. MEEHAN, Massachusetts
JEFF FLAKE, Arizona	

GEORGE FISHMAN, *Chief Counsel*
LORA RIES, *Counsel*
CINDY BLACKSTON, *Professional Staff*
LEON BUCK, *Minority Counsel*

CONTENTS

OCTOBER 11, 2001

OPENING STATEMENT

The Honorable George W. Gekas, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Immigration and Claims	1
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Immigration and Claims	2

WITNESSES

Mr. Randolph C. Hite, Director, Information Technology Systems Issues, United States General Accounting Office	
Oral Testimony	5
Prepared Statement	6
Mr. Glenn A. Fine, Inspector General, United States Department of Justice	
Oral Testimony	11
Prepared Statement	13
The Honorable James W. Ziglar, Commissioner, Immigration and Naturalization Service (accompanied by Mr. Scott Hastings, Associate Commissioner for Information Resource Management)	
Oral Testimony	20
Prepared Statement	23
Mr. Demetrios G. Papademetriou, Co-Director, Migration Policy Institute	
Oral Testimony	27
Prepared Statement	29

APPENDIX

STATEMENTS SUBMITTED FOR THE RECORD

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas	49
--	----

MATERIAL SUBMITTED FOR THE RECORD

Mr. Demetrios G. Papademetriou, Co-Director, Migration Policy Institute	51
Letter From the U.S. Department of Justice, the Honorable James W. Ziglar, Commissioner, Immigration and Naturalization Service	66
Letter From the U.S. Department of Justice, the Honorable James W. Ziglar, Commissioner, Immigration and Naturalization Service	68

USING INFORMATION TECHNOLOGY TO SECURE AMERICA'S BORDERS: INS PROBLEMS WITH PLANNING AND IMPLEMENTATION

THURSDAY, OCTOBER 11, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON IMMIGRATION AND CLAIMS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, Hon. George W. Gekas [Chairman of the Subcommittee] presiding.

Mr. GEKAS [presiding]. The hour of 10 o'clock having arrived, the scheduled hearing for the Immigration and Claims Subcommittee of the Judiciary will come to order. We have thus kept faith in dropping the gavel with our theme of beginning every hearing and every meeting exactly on time, and now we have to recess until the appearance of a second Member because the rules of the House, and therefore the rules of the Committee, mandate that at least two Members have to be present for an official hearing.

So you have a choice between now and the time that the second Member comes. I could recite Shakespeare or break into song until that Member appears. [Laughter.]

Mr. GEKAS. Until you make up your minds, this Committee stands in recess until the second Member appears.

[Recess.]

Mr. GEKAS. The time of the recess has expired. We note, and we want the record to indicate that the lady from Texas, Ms. Jackson Lee, Ranking Minority Member, is present, thus, constituting with the chair a hearing quorum.

We will begin the proceedings by asking the witnesses, those seated at the table and those prospective witnesses who might testify to something to please stand and be sworn.

Is Mr. Papademetriou here?

Mr. PAPADEMETRIOU. Yes, Mr. Chairman.

Mr. GEKAS. Will you please raise your right hands and be sworn. [Witnesses sworn.]

Mr. GEKAS. You may be seated. We will call upon you as the order of witnesses indicates.

The first order of business is to get rid of the bells. [Laughter.]

Mr. GEKAS. The order of witnesses is exactly as the witnesses have been seated from our right to the left, and Mr. Hite will be the first witness. He is the Director of Information Technology Systems Issues at the U.S. General Accounting Office. He has been

there for 25 years, has directed reviews of many and multifarious types of information-gathering techniques and particularly on the technology, which will possibly be the focus of today's hearing in quantity. He has a degree in business administration, and has received many awards, including the GAO's Meritorious Service Award.

Before he feels free to proceed, the chair will indulge in a brief opening statement to set the stage for the hearing, which I have already, in some ways, indicated through the introduction of Mr. Hite.

Way before the events of September 11, and especially since, the status of aliens in our country is a weighty problem, heightened of course by what we have seen, the fury of activity in tracing aliens, and hijackers, and potential hijackers, et cetera, ever since the calamities of September 11.

We want to indulge in finding out what has happened to some of the mandates that we have presented to the INS in the past as a Congress, particularly with the border crossing cards and that technology. It seems to us that, thus far—and perhaps I am preparing Commissioner Ziglar for possible answers to our pointed questions—we see no reason for what has happened at the border with these cards, and we want fullest explanations and remedies.

Then there is the student visa problem, SEVIS or SEVIS [long e], as we want to call it, where it has been uncovered that the intent of Congress has not been fulfilled with an accountability on a range of people who are involved in the prosecution of that program. So the technology involved there and in the border crossing cards will be two of the focus issues of this hearing. We may wander into others, as is the want of the Members of Congress from time to time, like always, and we will ask the witnesses to consider what the chair has said as to the focus during the question and answer period that will follow the initial presentations.

We note the presence of Congressman Flake, a Member of the Committee. Let the record indicate that he is present.

We now yield to the lady from Texas for an opening statement.

Ms. JACKSON LEE. Good morning to the witness, and, Mr. Chairman—witnesses—and Mr. Chairman thank you very much for holding this very important hearing. I look forward to working with you as this Committee works its will and works with our colleagues to emphasize the importance of the work of the INS, but as well to ensure that we have the skills and the tools to do the job that the American people desire.

Let me welcome Commissioner Ziglar. I believe this may be the first time he has testified before this Committee. I may be incorrect. He may have been busy, and we may have seen him before, but I think this is the first time, and I welcome the other witnesses.

These issues have been before these—this Committee, dealing with the securing of America's borders for many, many years, through many chairpersons and Ranking Members. This Oversight Hearing on Using Information Technology to Secure America's Borders: INS Problems with Planning and Implementation is important for two reasons.

First, this hearing will help us understand what we can do to prevent events such as September 11; second, this hearing is so vital because the mission of the INS to provide immigration services to alien citizens and businesses and to enforce the Nation's immigration laws is absolutely dependent on information technology. With poor information technology, we are making Immigration inspectors, Border Patrol officers and investigators work too hard. INS border security enforcement systems do not work effectively. We need systems that are versatile. This does not mean that INS employees and management are not working hard. It does mean that we have a lot to fix.

Instead of hastily appropriating more money to INS, whose budget has increased from \$1.4 billion in fiscal year 1992 to over \$5 billion in fiscal year 2001, we need to pursue additional options. It is clear to me from my many dealings with the INS that the main fix that is needed is a radical shift in the mentality of the Immigration and Naturalization Service, and I would also add a restructuring of the INS.

For years I have struggled with the Agency that is unable to meet congressional deadlines. After pouring in massive amounts of revenue, Congress has not seen the improvements it desires. However, with better planning, structure, organization, most importantly management, there is no question that the Agency should be able to meet its goals. It is unclear how many different types of border security enforcement systems exist. INS has been auditing what systems it has in place since January of 2000. In addition, it is unclear what the purpose of each system is and how they operate.

I hope, Commissioner Ziglar, that you will be able to inform us about the different systems that exist and how they operate, all with the goal of making all of us better.

Furthermore, I would like to highlight some of the concerns I have with the current structure of information technology. A current snapshot of INS management and investment of information technology, as well as its information security, shows that INS cannot ensure that the money it spends each year on information technology will be able to support the function of the Agency or, B, that its information technology resources are adequately protected from unauthorized access or service disruption.

There are simply too many different border security enforcement systems to be used or managed. Serious consideration needs to be given to consolidating as many of these systems as possible or creating one system that is all relevant data, so that all relevant data becomes available.

One major system, the IDENT system, which is used to track recidivous aliens along the border between ports of entry, has been badly implemented, despite an investment exceeding \$80 million. Department of Justice Management Division is moving forward with an additional \$27 million integration effort. Serious consideration should be given to declaring a moratorium on spending money on this system, and instead replacing it with a new system that is truly integrated with all INS and FBI criminal database.

We worked very closely with the Resendez-Ramirez case and held hearings on this matter in this Committee. This was a failure

of INS to adequately track a known criminal, a serial killer, unfortunately. Such a situation cannot happen again, and hopefully this hearing will lead the way in correcting that.

Currently, some of INS systems require biometric cards, some do not. Some cards have bar codes, others have laser media. Some systems do not even use biometric data. There should be some discussion as to creating some conforming system so that all of the information can be used for a single type of card reading.

The recent terrorist attacks have seriously impeded legitimate international travel and commerce. That means that we really have to do something. Coming from Texas, I know that you have changed to the bar-coded cards, I believe. I hope you will comment on that and tell us how that is working. Certainly, coming from Texas, there have been many calls of concern on both sides of the border, as it relates to the delays, whether you have enough staff, whether the carding is working, and I think that is extremely important.

In the Antiterrorist Bill, I offered suggestions for the spending of the \$50 million for the Canadian border, more cooperation between our law enforcement, of course, and Canadian law enforcement, more intimate relationships, if you will, or coordination/collaboration, in addition, using the highest type of technology, infrared technology, as well.

As I close, I simply want to say that we can spend a lot of time and are spending a lot of time on September 11. We wish and call upon all that we believe in that it did not happen. I would like the INS to be part of the solution, not part of the problem. And, if anything, we need to be at the top of our game, if you will, in sharing information, in technology utilization.

And, clearly, let me say that the tracking of the visas, specialty visas, as the Chairman has so noted—he mentioned student visas—is an imperative, and I would like to have a response as to how the INS intends to coordinate with the State Department, who gives the visas, in terms of tracking overstays. Without knowing any detailed information about the intimacies of the final results of the investigation of September 11, I would hate to find out that many of those individuals were the result of overstays. We must give to the American people our word that their security is our most important responsibility, balanced, of course, with those individuals who have accessed legalization legally and are here to contribute to this Nation, respecting their rights as well.

I hope this hearing will lend itself to giving, minimally, some of the answers to the American people.

I yield back. I thank the Chairman.

Mr. GEKAS. The record will indicate that the lady from California, Ms. Lofgren is present, the gentleman from Texas, Mr. Smith.

Any opening statements that the Members might have can, by unanimous consent, become a part of the record, and they will appear immediately following the opening statements by the Chair and the Ranking Minority Member.

Mr. GEKAS. We now will proceed with the testimony with the already-introduced Mr. Hite, to whom we say we will allot 5 minutes

for an oral presentation of your written statement, which is already becoming a part of the record, and we ask you to proceed.

TESTIMONY OF RANDOLPH C. HITE, DIRECTOR, INFORMATION TECHNOLOGY SYSTEMS ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

Mr. HITE. Thank you, Mr. Chairman, and Members of the Subcommittee for the opportunity to participate in today's hearing.

The events of September 11, 2001, have made INS's very important border security mission more prominent. When one considers that America's borders extend thousands of miles, involve hundreds of ports of entry, through which millions of visitors pass, an appreciation of how challenging this mission is begins to emerge. Couple this with the fact that INS must work in lockstep with a number of other Federal agencies that also play key roles in this border security mission area, then the challenge becomes more daunting.

How can INS meet its challenge? As with any organization, the key is leveraging resources, in the form of people, processes, and technology as the means to the desired end. For INS and its border security mission, however, people resources can only do so much given the vast number of border entry and crossing points. To augment its people, INS must transform both the way it does business and the technology it uses to support its business processes, thereby expanding its reach and visibility over our borders.

How can this be accomplished? Our research of private- and public-sector organizations that are successful in using IT shows that doing so requires the establishment of certain institutional IT management enablers. Two of these are enterprise architecture management and IT investment management, neither of which INS has currently implemented.

Let me start with enterprise architecture management. Simply stated, an architecture consists of a set of explicitly defined models that show, in both business terms and technology terms, how an organization operates today, how it needs to operate tomorrow, and it provides a road map for transitioning between those two points in time. The goal is to ensure that new and modified Agency assets and the business processes that they support are designed and implemented in a way that promotes interoperability and avoids duplication.

Last year, we reported that INS did not have an enterprise architecture and that its efforts to develop one were unlikely to produce success. The good news is that INS has agreed with the recommendations and has made progress in implementing them. The bad news is that INS still does not have the enterprise completed and much remains to be done. Without an architecture, the best that INS can hope for is to patch together stovepipe operations and supporting systems. This would produce marginal improvements in performance.

Let me now turn to IT investment management, which, in general terms, is the mechanism for implementing the architecture. In short, investment management consists of the steps to assure that senior executives are adequately involved and informed about the crucial capital investment decisions that are central to moving an agency from where it is today to where it needs to be tomorrow.

The goal is to assure that IT projects are implemented at acceptable costs, within reasonable and expected time frames, and are contributing to tangible, observable improvements in mission performance.

In this regard, we also reported last year that INS lacked the full set of investment management processes and practices—to ensure that IT projects would be delivered on time, on budget, would perform as intended, and more importantly would represent the right mix of systems to best support mission needs and priorities.

While the good news is that INS has agreed with these recommendations and has made progress in implementing them, the bad news is that these processes and practices have yet to be implemented. Until it does, INS mission effectiveness and efficiency, in my view, are not achievable goals.

In summary, what this “technology speak” means is this: When it comes to investing in IT, and by association the processes that IT implements, INS is not positioned to know that it is doing the right thing and it is doing it the right way. To be right, INS must know, at a minimum, whether its investments in IT are aligned with an agency blueprint for change and whether they are the best mix of investments to maximize benefits, and minimize costs and risks. If this is not done, INS process and system environments will not evolve appreciably from where they are today, and it is unlikely that INS will be able to effectively and efficiently leverage process and technology resources to best meet border security mission needs.

That concludes my statement. I will be happy to answer any questions.

[The prepared statement of Mr. Hite follows:]

PREPARED STATEMENT OF RANDOLPH C. HITE

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today’s hearing on the Immigration and Naturalization Service’s (INS) use of information technology (IT) to secure America’s borders. My statement is based on reports we have issued during the last year that address INS’ institutional IT management process controls, and our recent follow-up work to determine progress in implementing the recommendations that we made in these reports.¹

IT management process controls, such as investment management and enterprise architecture management, are recognized indicators of whether an organization, like INS, can successfully develop, acquire, implement, operate, and maintain IT systems and related infrastructure. Together, enterprise architecture management and investment management, respectively, serve to explicitly blueprint the future operational environment, in both business and technology terms, needed for an organization to effectively and efficiently achieve its strategic mission, and to assure adequate senior executive involvement in the crucial capital investment decisions required to effective and efficiently put in place this target environment.²

In summary, INS has yet to implement the set of practices (e.g., policies, activities, abilities, measures) associated with effective IT investment and enterprise architecture management. As a result, INS is not positioned to know that its ongoing and planned IT investments are the “right things to do,” meaning it does not know

¹*Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture* (GAO/AIMD-00-212, August 1, 2000) and *Information Technology: INS Needs to Better Strengthen its Investment Management Capability* (GAO-01-146, December 29, 2000).

²The importance of both agency architectures and IT investment management is recognized by the Clinger-Cohen Act and guidance from the Office of Management and Budget (OMB), as well as leading private and public sector organizations. (In the fiscal year 1997 Omnibus Consolidated Appropriations Act, P.L. 104-208, the name “Clinger-Cohen Act of 1996” was given to Divisions D (the Federal Acquisition Reform Act) and E (the Information Technology Management Reform Act) of the 1996 DOD Authorization Act, P.L. 104-106.)

whether these investments will produce mission value commensurate with costs and risks or whether these investments are superior to competing investment alternatives. Further, INS does not know that these investments are “being done the right way,” meaning it does not know whether investments are aligned with an agencywide blueprint (architecture) that defines how the agency plans to operationally and technologically function in the future, and it does not know whether each of its ongoing investments are meeting their cost, schedule, and performance commitments.

In light of the recent terrorist attacks, INS’ border security mission has gained prominence. How effectively INS can perform this vital mission will depend in part on how well it can leverage both existing and new IT resources. Given the difficulty of this mission, effectively and efficiently leveraging technology would be a challenge even if INS had the requisite management process controls. Since it does not, INS’ challenge becomes even more challenging. In the recommendations that we made in our recent reports, we recognized that INS would have to make near-term investments to meet pressing mission needs before it had established IT management process controls. A key to INS’ doing so effectively is for its leadership to proactively compensate for missing management controls by ensuring that the requisite human capital skills and expertise are brought to bear on IT projects supporting its border security mission. While this is clearly not a long-term solution to the agency’s IT management challenges, this strategy can serve as a temporary “crutch” until INS can follow through on its ongoing efforts to establish and implement effective management process controls and devote the resources to ensuring that these controls are practiced agencywide.

BACKGROUND

The mission of INS, an agency of the Department of Justice, is to administer and enforce the immigration laws of the United States. To accomplish its mission, INS has three interrelated business areas—enforcement, immigration services, and corporate (i.e., mission-support) services. Enforcement includes border inspections of persons entering the United States, detecting and preventing smuggling and illegal entry, and identifying and removing illegal entrants. Immigration services include granting legal permanent residence status, nonimmigrant status (e.g. students and tourists), and naturalization. INS efforts to protect our nation’s borders are performed under both of these core mission areas. Corporate services include functions such as financial and human capital management. INS’ field structure consists of 3 regional offices, 4 regional service centers, 3 administrative centers, 36 district offices, 21 Border Patrol sectors, and more than 300 land, sea, and air ports of entry.

To carry out its responsibilities, INS relies on IT. For example, the Integrated Surveillance Intelligence System (ISIS) is to provide “24 by 7” border coverage through ground-based sensors, fixed cameras, and computer-aided detection capabilities. Also the Student Exchange Visitor Information System (SEVIS) is to manage information about nonimmigrant foreign students and exchange visitors from schools and exchange programs.

Each year INS invests, on average, about \$300 million in IT systems, infrastructure, and services.

INS’ Longstanding Problems in Managing IT Projects Have Been Well Chronicled

Recent studies have identified significant weaknesses in INS’ management of IT projects. In August 1998, the Logistics Management Institute (LMI) reported that INS did not track and manage projects to a set of cost, schedule, technical, and benefit baselines.³ LMI noted that while INS had defined good procedures for developing systems, it did not consistently follow them. Similarly, in July 1999, the Justice Inspector General (IG) reported that INS was not adequately managing its IT systems.⁴ In particular, the IG reported that (1) estimated completion dates for some IT projects had been delayed without explanation, (2) project costs continued to spiral upward with no justification for how funds are spent, and (3) projects were nearing completion with no assurance that they would meet performance and functional requirements.

³*Reengineering Information Technology Management at the Immigration and Naturalization Service*, Logistics Management Institute, August 1998. LMI is a private, nonprofit corporation that provides management consulting, research, and analysis to governments and other nonprofit organizations.

⁴*Follow-up Review: Immigration and Naturalization Service Management of Automation Programs*, Office of the Inspector General, Audit Division, U.S. Department of Justice, July 1999.

DESPITE RECENT PROGRESS, INS LACKS IMPORTANT INSTITUTIONAL IT MANAGEMENT CONTROLS

In light of the reported problems on individual projects, we reviewed INS' institutional approach to managing IT to determine the root cause of project problems and to provide the basis for recommending fundamental management reform. In doing so, we focused on two key and closely related IT management process controls: investment management and enterprise architecture management. In August 2000 and December 2000, we reported that INS lacked both of these management process controls because the former agency leadership had not viewed either as an institutional priority. We also provided INS, through our recommendations, a roadmap for establishing and implementing both controls.⁵ INS agreed with our findings and recommendations, and it committed to implementing the recommendations. Although INS has made progress to date in doing so, much remains to be accomplished before it will have implemented these management controls and have the capability to effectively and efficiently manage IT.

Effective Planning and Implementation of IT Requires Architecture-Centric Investment Management

As defined by the Clinger-Cohen Act of 1996 and associated Office and Management and Budget instructions, and as practiced by leading public and private sector organizations, effective IT investment management requires implementing process controls for maximizing the value and assessing and managing the risks of investments. The goal is to have the means in place and functioning to help ensure that IT projects are being implemented at acceptable costs, within reasonable and expected time frames, and are contributing to tangible, observable improvements in mission performance.

To help agencies understand their respective IT investment management capabilities, we developed the Information Technology Investment Management (ITIM) maturity framework. The ITIM framework is a tool that identifies critical processes and practices for successful IT investment and organizes them into a framework of increasingly mature stages.⁶ A fundamental premise of the framework is that each incremental stage lays a foundation on which subsequent stages build. The initial stage focuses on controlling investments already underway, while also starting to establish a way to select new investments. Later stages emphasize managing investments from a portfolio perspective in which individual investments are evaluated as a set of competing options based on their contribution to mission goals and objectives. The goal is to arrive at the optimal mix of projects in which to invest resources. Agencies can use the framework for assessing the strengths and weaknesses of their existing investment management processes and for developing a roadmap for improvement. The Chief Information Officers Council has endorsed the ITIM framework.

In order for an agency to achieve a minimum level of IT management effectiveness, it needs to first gain control of its current investments. To do this, it must establish and implement processes and practices for ensuring that projects have defined cost, schedule, and performance expectations; that projects are continuously controlled to determine whether commitments are being met and to address deviations; and that decisionmakers have this basic investment information to use in selecting new projects for funding and deciding whether to continue existing projects. Once it has established these project-specific control and selection processes, the agency then should move to considering each new investment not as a separate and distinct project, but rather as part of an integrated portfolio of investments that collectively contribute to mission goals and objectives. To do this, the agency should establish and implement processes and practices for analyzing the relative pros and cons of competing investment options and selecting a set of investments that agency leadership believes best meets mission-based and explicitly defined investment criteria.

Integral to an effective IT investment management process is having a well-defined enterprise architecture or blueprint for guiding the content and characteristics of investments in new and existing IT systems, infrastructure, and services. The goal is to help ensure that the new and modified IT assets will, among other things, be designed and implemented to promote interoperability and avoid duplication, thereby optimizing agencywide performance and accountability.

⁵ GAO/AIMD-00-212, August 1, 2000 and GAO-01-146, December 29, 2000.

⁶ *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft) (GAO/AIMD-10.1.23, May 2000).

In more specific terms, an enterprise architecture is a comprehensive and systematically derived description of organization's operations, both in logical terms (including business functions and applications, business rules, work locations, information needs and users, and the interrelationships among these variables) and in technical terms (including IT hardware, software, data, communications, security, and performance characteristics and standards). If defined properly, enterprise architectures can clarify and help optimize the connections among an organization's interrelated and interdependent business operations and the underlying IT supporting these operations.⁷ A complete enterprise architecture includes both the current architecture (as it is now) and the target architecture (the goal), as well as a plan for moving between the two. To assist agencies in developing, maintaining, and implementing enterprise architectures, we collaborated with the Chief Information Officers Council to develop a practical guide for enterprise architecture management.⁸

INS Has Taken Steps to Improve IT Investment Management But Effective Processes and Practices Have Yet To Be Implemented

In December 2000 we reported that while INS had some investment control elements, it nevertheless lacked the full set of foundational investment management processes and practices needed to effectively control its ongoing IT projects and ensure that they were meeting cost, schedule, and performance commitments and contributing to measurable mission performance and accountability goals. For example, INS had not consistently (1) developed and maintained project management plans that specified cost and schedule baselines, (2) linked projects to INS mission needs, and (3) tracked and monitored projects to determine whether they were meeting project baselines and mission needs. Without this information, the investment review board (that, to its credit, INS had established to make investment selection decisions) could not act to effectively address deviations. The result was increased risk that the technology needed to support mission goals, such as securing America's borders, would not be delivered on time and on budget and would not perform as intended.

We also reported in December 2000 that INS was not effectively managing its IT investments, both new proposals and ongoing projects, as a portfolio, meaning that INS' investment review board was not making portfolio selection and control decisions in terms of what mix of proposed and ongoing projects collectively best supported achievement of mission needs and priorities. In particular, INS had not defined, and thus was not using, investment selection criteria that were linked to mission needs and addressed cost, schedule, benefits, and risk. Without such criteria, the board lacked the basic information needed to assess the relative merits of and make trade-offs among its options for increasing IT capabilities, including acquiring new, enhancing existing, and operating and maintaining existing systems and infrastructure. By not employing portfolio investment management, we concluded that INS was at risk of not having the right mix of technology in place to support critical mission priorities, such as protecting America's borders against the threat of terrorism. Accordingly, we made a series of recommendations to INS aimed at, among other things, treating the development and implementation of IT investment management process controls as an agency priority and managing them as such.

Since our December 2000 report, INS has taken steps to implement our recommendations for establishing and following rigorous and disciplined investment management controls. In particular, it has developed a guide for IT investment management that, according to INS, defines many of the missing processes and practices. The key for INS will be to ensure that these processes and practices are effectively implemented. Given that the Justice IG, in reporting on IT project problems, found that INS was not following established project management procedures, successful implementation of INS' newly developed investment guide cannot be taken for granted, and needs to be given the attention it deserves.

⁷In our experience with federal agencies, attempts to define and build major systems without first completing an enterprise systems architecture often result in systems that do not effectively optimize mission performance, being duplicative, not well integrated, and unnecessarily costly to maintain and interface. See, for example, *Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization* (GAO/AIMD-97-30, February 3, 1997) and *Customs Service Modernization: Architecture Must Be Complete and Enforced to Effectively Build and Maintain Systems* (GAO/AIMD-98-70, May 5, 1998).

⁸A Practical Guide to Federal Enterprise Architecture, version 1.0 (Chief Information Officer Council, February 2001).

INS Is Taking Steps to Develop an Enterprise Architecture, But It Still Lacks this Important IT Management Tool

In July 2000, we reported that INS did not have an enterprise architecture, including a description of both its “as is” and “to be” operational and technology environments and a roadmap for transitioning between the two environments. Moreover, we also reported that the efforts underway to develop the architecture were flawed and unlikely to produce useful architectural products.⁹ In particular, the development efforts were limited to a producing a bottom-up description of INS’ current IT environment (e.g., hardware and system software computing platforms, data structures and schemas, software applications) and mapping the software applications to mission areas. While this was a reasonable start to describing the current architectural environment, important steps still needed to be accomplished, such as linking the systems environment description to a decomposed view of agency mission areas, including each area’s component business functions, information needs, and information flows among functions. Moreover, doing this reliably required the participation of agency business owners; however, these owners were not involved.

Also, INS had not begun developing either a target architecture or a capital investment plan for sequencing the projects that will it allow to migrate from its current architecture to its target architecture. These two components would be integral to INS’ previously mentioned need to implement effective investment management processes and practices because both controlling and selecting IT projects requires ensuring that these projects are provided for in the sequencing plan and are aligned with the target architecture. By doing so, investment decisionmakers can know (1) how proposed projects contribute to the strategic mission goals, needs, and priorities and (2) whether these projects will be engineered according to the technical models and standards, that are both embedded in the target architecture descriptions.

Equally important, we reported that INS’ architecture development efforts were not being managed as a formal program, including having meaningful plans that provided a detailed breakdown of the work and associated schedules and resource needs. Further, these efforts did not include performance measures and progress reporting requirements to ensure that the effort was progressing satisfactorily. As a result, we concluded that it was unlikely that INS could produce a meaningful architecture that could be used to effectively and efficiently guide and constrain IT investment and project decisionmaking. Accordingly, we made a series of recommendations to INS aimed at making development of an enterprise architecture an agency priority and managing it as such.

INS agreed with our recommendations and has since taken steps to improve its ability to manage development of its enterprise architecture. For example, INS reports that it has (1) established an enterprise architecture program office, (2) developed a business model of its current operational environment, (3) developed plans for defining a target architecture and capital investment sequencing plan, and (4) established teams representing all business units to define current and target business environments. While these are positive steps, they are only a beginning, and much remains to be accomplished before INS will have the kind of agency blueprint needed to support effective project investment and engineering decision-making.

In conclusion, INS is a challenged agency when it comes to effectively and efficiently managing IT. Nevertheless, immediate border security demands have emerged that require the agency to effectively leverage technology as part of its response to these demands. To address this situation in the near term, INS will have to ensure that it compensates for management process control weaknesses by engaging the requisite human capital expertise on its border security efforts. In the long term, INS will need to continue to implement our open recommendations aimed at reforming the agency’s IT management process controls.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be happy to address any question that you have.

Mr. GEKAS. We thank the gentleman, and we will return to him during the Q and A.

We now turn to an introduction of Glenn A. Fine, the Inspector General of the United States Department of Justice. He has worked for the Department of Justice Office of the Inspector General since January 1995. Initially, he was special counsel to the Inspector General.

⁹*Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture* (GAO/AIMD-00-212, August 1, 2000).

Mr. Fine graduated magna cum laude from Harvard in 1979, with an A.B. degree in economics. He was a Rhodes Scholar and earned B.A. and M.A. degrees from Oxford. He received his law degree magna cum laude from Harvard Law School in 1985.

We ask the gentleman to proceed for a period of 5 minutes to summarize the written statement which, as previously indicated for all witnesses, is already a part of the record.

**TESTIMONY OF GLENN A. FINE, INSPECTOR GENERAL,
UNITED STATES DEPARTMENT OF JUSTICE**

Mr. FINE. Mr. Chairman and Members of the Subcommittee on Immigration and Claims, I appreciate the opportunity to appear before the Subcommittee to testify on the INS's use of information technology to secure America's borders.

My testimony this morning will focus on the work of the Office of the Inspector General in examining INS programs and their related information technology systems. At the outset, I want to stress that while the OIG has noted serious deficiencies in INS IT systems over the years, this should in no way diminish the important contributions thousands of INS employees make on a daily basis. They perform diligently, under very difficult circumstances, and their mission is critical to this country.

Yet our reviews of INS programs and associated IT systems have revealed significant problems in the INS's efforts to fulfill that mission. A 1998 OIG audit of the INS's management of IT systems found that the INS did not adequately manage or monitor its numerous initiatives.

We issued a follow-up audit report in 1999, which again concluded that the INS still could not sufficiently track the status of its IT projects to determine whether progress was acceptable, given the amount of time and funds already spent. Estimated completion dates for projects were delayed without explanation; costs continued to spiral upward with no justification for how funds were spent; and projects neared completion with no assurance of meeting performance and functional requirements.

Since our audits, the GAO has issued two reports reaching related conclusions, which Mr. Hite just summarized. I will briefly summarize some OIG reviews of a few specific systems that are discussed in my written statement.

The INS's automated biometric identification system, known as IDENT, is used, in part, to identify individuals who the INS apprehends. This system scans two fingerprints and pictures of aliens and compares them against records in the IDENT lookout and recidivist databases.

The INS envisioned that most of its operations, including the Border Patrol, Investigations, Detention and Deportation, Intelligence and Inspections, would benefit from IDENT through its quick identification of individuals and its ability to obtain information about them. However, an OIG inspection found that the INS was not enrolling all of the aliens apprehended along the U.S.-Mexico border into IDENT and had virtually no controls to ensure the quality of data entered. We also raised concerns that the INS had not sufficiently trained its employees on the system.

In March 2000, the OIG issued another review that again found problems with IDENT in tragic circumstances. Rafael Resendez-Ramirez was a Mexican national accused of committing several murders in the United States. When local police searching for Resendez contacted INS investigators in Houston, none of the INS investigators placed a lookout for him in IDENT.

Consequently, when Border Patrol agents apprehended Resendez as he attempted to illegally cross the border into New Mexico, nothing in IDENT alerted them to the fact that he was wanted for murder or had an extensive criminal record. The Border Patrol, therefore, followed its standard policy and voluntarily returned him to Mexico. Resendez returned to the United States within days of his release and murdered several more people before surrendering.

Our review of the Resendez case showed problems that were indicative of and partly caused by larger failings in the design and implementation of IDENT. We found that training on IDENT for INS employees, particularly outside the Border Patrol, was ineffective or nonexistent. INS program offices, such as Investigations and Intelligence, viewed IDENT as a Border Patrol initiative and were not educated on how it could be useful to their mission. Also, IDENT was not, and still is not, linked with the FBI's Integrated Automated Fingerprint Identification System and the FBI's National Crime Information Center 2000 system.

The Resendez case vividly illustrated the need for integration of the INS and FBI systems and spurred the FBI and the INS to begin to develop an integration plan. However, that plan is still being developed.

Another OIG review examined the INS's tracking and identification of nonimmigrant visa overstays. These are visitors who enter the United States legally, but fail to depart when required. The INS estimates that 40 to 50 percent of the approximately 6 million or more illegal aliens in the United States fit into this category. Our review found that the principal INS system for tracking visa overstays, the Nonimmigrant Information System, was not producing reliable data, either in the aggregate or on individuals. We also found that the INS had no specific enforcement program to identify, locate, apprehend, and remove overstays, and that using the INS data was of little use for locating them.

Also related to the issue of nonimmigrant overstays, the OIG recently examined the INS's efforts to meet congressional directives to develop an automated entry and exit control system that would collect a record for aliens arriving in the United States from an I-94 card and automatically match these with I-94 departure cards. The OIG found that the INS has not properly managed the project. Despite having spent \$31 million on the system, the INS was operating it at only a few airports and does not have clear evidence that it would meet its intended goals.

We also conducted other reviews discussed in my written testimony that examine the Visa Waiver Program, the Border Patrol's efforts to control illegal activity along the northern border, and how the INS handled the cases of two men who entered and remained in the United States before being arrested on charges of attempting to bomb the Brooklyn subway system in 1999.

In sum, these and other OIG projects have found that the INS failed to manage and implement reliable integrated IT systems in a timely and cost-effective manner. The OIG believes the INS needs to more stringently manage and establish priorities for the development of its systems, rather than spend enormous resources developing so many IT systems for so many different purposes.

Among other recommendations, we urge the INS to ensure that its databases share information both within and outside the INS. We also believe the INS needs to expand the use of biometrics to identify individuals with whom the INS comes in contact. In addition, the INS must improve its tracking of nonimmigrant visa overstays. The current system for identifying them does not produce reliable or accurate information, and the automated I-94 project does not seem to be working.

Solving the problems of INS information technology is a complex issue with no easy solutions. It requires strategic vision, strong leadership, and individual and organizational accountability. This effort needs to be a top priority of the Agency, since effective INS information technology is essential to protecting the integrity of the immigration system and the national security.

I would be pleased to answer any questions.

[The prepared statement of Mr. Fine follows:]

PREPARED STATEMENT OF GLENN A. FINE

Mr. Chairman, Congresswoman Jackson Lee, and Members of the Subcommittee on Immigration and Claims:

I. INTRODUCTION

I appreciate the opportunity to appear before the Subcommittee on Immigration and Claims to discuss the Immigration and Naturalization Service's (INS's) use of information technology to secure America's borders. My testimony this morning will focus on the work of the Department of Justice (Department) Office of the Inspector General (OIG) in examining programs and related automated systems in the INS.

In recent years, the OIG has spent approximately one-half of our total resources on INS-related oversight. We expended this effort in response to concerns expressed within the Department and Congress, as well as our own assessment, about how the INS was handling its important and diverse responsibilities. As the INS's budget and workforce have increased to more than \$5 billion and 33,000 staff, the need for concerted OIG oversight similarly has increased.

At the outset of my statement, I want to stress that while the OIG has noted serious deficiencies in INS operations and systems over the years, this should in no way diminish the important contributions thousands of INS employees make on a daily basis. These employees perform diligently, under very difficult circumstances, and their mission is critical to the proper functioning of our government.

Yet, as this statement will discuss, our reviews of INS programs and their associated information technology systems have revealed significant problems that leave gaps in the INS's attempts to secure the nation's borders. In this statement, I will highlight examples of OIG work in the INS that identifies some of these shortcomings.

Before I turn to these specific OIG reviews, however, let me offer several general observations based upon our body of work in the INS. Over the past decade, the OIG has found serious process and management deficiencies in the INS. Many OIG reviews of INS programs have questioned the reliability of the agency's automated information systems and the accuracy of the data produced by those systems. We see separate automated systems planned for almost every function in the INS, but many of these systems do not "talk" to each other and therefore cannot be used to meet other important agency missions. Furthermore, given the INS's track record in acquiring and managing information technology (IT) systems, the OIG is concerned that the INS will not have the managerial expertise or ability to bring all of its automation initiatives successfully to completion, particularly in a timely and cost effective fashion.

According to Department of Justice estimates, the INS has spent more than \$290 million on automated systems in fiscal year (FY) 2001 and more than \$260 million in FY 2000. All told, through fiscal year 2001, the INS planned to spend approximately \$2.6 billion on its automation programs. However, two OIG reviews of the INS's management of its automation initiatives found lengthy delays in completing many automation programs, unnecessary cost increases, and a significant risk that finished projects would fail to meet the agency's needs.

The OIG first notified the INS in 1995 of our concerns regarding systemic problems in INS automation programs. Based on our extensive audit work during the early 1990s, we identified ten risk areas in the INS's management of its automation programs that required close scrutiny by agency managers.

In March 1998, the OIG completed the first of two comprehensive audits of the INS's management of its automation programs. In our first audit, we found that the INS did not adequately monitor its automation programs. We concluded that the INS lacked comprehensive performance measures and insufficiently tracked the status of its projects. Consequently, the INS could not determine if progress towards the completion of the projects was acceptable. As a result, we stated that the INS faced risks that: (1) completed projects would not meet the overall goals of the automation programs; (2) completion of the automated projects would be significantly delayed; and (3) unnecessary cost increases would occur.

In July 1999, the OIG issued a follow-up report, which again found that the INS was not adequately managing its automation programs. In the 1999 audit, we noted that the INS still could not sufficiently track the status of its automation projects to determine whether progress was acceptable given the amount of time and funds already spent. We reported that: (1) estimated completion dates for projects were delayed without explanation; (2) costs continued to spiral upward with no justification for how funds were spent; and (3) projects neared completion with no assurance for meeting performance and functional requirements.

We identified three causes for these problems. First, INS managers did not have a common base line of automation projects by which to focus their collective efforts. In fact, the INS had substantial difficulty providing us with a complete list of their automation projects. Second, project information needed for effective management and decision-making was not readily available. Third, INS managers did not develop, document, or implement basic management control processes necessary to ensure that projects would be completed on schedule and meet performance and functional requirements. The ultimate cost for the INS's automation programs was uncertain because actual costs incurred were unreliable and projected cost estimates were unsupported.

Furthermore, we found that the INS had not implemented adequate safeguards to ensure the accuracy of existing data that would be used by systems being developed or re-engineered, or the adequacy of future data inputs. As a result, new or existing INS systems could contain inaccurate or unreliable data.

Since these audits, the General Accounting Office (GAO) issued reports in August 2000 and December 2000 that reached related conclusions about the INS's management of its information technology programs. Those reports concluded that the INS does not have an enterprise architecture to ensure that the hundreds of millions of dollars it spends each year on new and existing technology will optimally support the INS's mission. The GAO also concluded that the INS did not have adequate processes in place to effectively manage its planned and ongoing information technology programs.

I will now describe several OIG reviews that examined the management and performance of individual INS information technology systems.

II. OIG REVIEWS

A. Automated Biometric Identification System (*IDENT*)

In 1989, the INS began to develop an automated biometric identification system to identify quickly individuals who are apprehended or have come into contact with the INS. Biometrics are biological measurements unique to each person, such as fingerprints, hand geometry, facial patterns, retinal patterns, or other characteristics, that are used to identify individuals. Fingerprints are the most common biometric used by law enforcement agencies. Historically, without a biometric system, the INS had to rely upon the names provided by aliens who were apprehended when checking against their databases or other records. But aliens often used false names or different names during different apprehensions. Also, many persons have similar names, and spelling errors can result in problems identifying individuals accurately.

After several studies, in 1994 the INS began implementing the Automatic Biometric Identification System, called *IDENT*. *IDENT* was first deployed in the San Diego

Border Patrol Sector and subsequently throughout the southwest border. IDENT workstations consist of a personal computer, camera, and a single-fingerprint scanner. During enrollment of individuals into IDENT, INS agents scan an individual's two fingerprints, take the individual's photograph, and enter basic apprehension information about the individual into the automated system. When this information is saved, IDENT matches the fingerprints of the individual against the corresponding fingerprints of all individuals in two central IDENT databases, the lookout database and the recidivist database.

In the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, Congress directed the INS to expand the use of IDENT to "apply to illegal or criminal aliens apprehended Nationwide." INS officials envisioned that most of the agency's programs and operations—including the Border Patrol, Investigations, Detention and Deportation, Intelligence, Inspections, Benefits Adjudication, and the INS Service Centers—would benefit from the IDENT system through its quick identification of individuals and its ability to obtain information about them from previous encounters with the INS, including any criminal history.

In 1998, the OIG evaluated the INS's implementation of IDENT and found that the INS was enrolling less than two-thirds of the aliens apprehended along the U.S.-Mexico border into the IDENT system. In addition, the INS was entering the fingerprints in the IDENT lookout database of only 41 percent of the aliens deported and excluded in FY 1996; of these, only 24 percent had accompanying photographs even though the INS relies on photographs to confirm identification. We found virtually no controls in place to ensure the quality of data entered into the IDENT lookout database. As a result, we found duplicate records and invalid data. We also raised concerns that the INS had not provided sufficient training to its employees on the use of IDENT. These failures hampered the INS's ability to make consistent and effective use of IDENT.

B. The Rafael Resendez-Ramirez Case and the Operation of IDENT

In March 2000, the OIG issued another review that implicated the IDENT system in tragic circumstances. The OIG examined how the INS handled its encounters with Rafael Resendez-Ramirez (Resendez), a Mexican national accused of committing several murders in the United States. Resendez was known as "the railway killer" because he allegedly traveled around the United States by freight train and committed murders near railroad lines. In early 1999, Texas police obtained a warrant for Resendez's arrest in connection with a brutal murder in Houston, Texas. The police mounted an extensive search to find Resendez and contacted several INS investigators in Houston seeking assistance in the search for him. However, none of those INS investigators placed a lookout notice for Resendez in IDENT. Instead, the INS investigators referred the police to other agencies or databases.

Consequently, when Border Patrol agents apprehended Resendez on June 1, 1999, as he attempted to illegally cross the border into New Mexico, nothing in IDENT alerted them to the fact that Resendez was wanted for murder or had an extensive criminal record. As a result, the Border Patrol followed its standard policy and voluntarily returned Resendez to Mexico. He returned to the United States within days of his release and murdered several more people before surrendering on July 13, 1999.

The OIG review concluded that the failings by the INS employees who did not place a lookout for Resendez in IDENT were indicative of and partly caused by larger failings in the INS's design and implementation of IDENT. We found that the training that was given to INS employees on IDENT, particularly outside the Border Patrol, was ineffective or non-existent. In the 1998 OIG report, we had noted problems with IDENT training and recommended that the INS develop and implement a strategy for sufficiently training INS personnel using IDENT. Unfortunately, the INS largely rejected this recommendation, claiming that its IDENT training was adequate. We found in the Resendez review that INS program offices, such as Investigations and Intelligence, viewed IDENT as a Border Patrol initiative and were not educated on how IDENT could be useful to their mission.

When we interviewed INS employees in various offices involved with the Resendez case, we found that their knowledge of IDENT was severely lacking. The INS investigators who were contacted by police searching for Resendez did not think of IDENT, even when they were asked to place a lookout in INS databases for Resendez. Although the INS had distributed a lookout policy, it provided no training on the policy and did little to ensure that the policy was understood or read.

IDENT was not, and still is not, linked with FBI databases. The INS's IDENT system and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the National Crime Information Center (NCIC) 2000 system were developed separately and along different time lines. Although the INS and the FBI

periodically discussed integration of their systems as they were being developed, there was never a sustained effort to achieve that goal and no agreement on integration was reached. We were told that the INS and the FBI made little effort to understand the operational requirements of the other agency. Each agency focused on meeting its own requirements and did not pursue integration. As a result, when the FBI finally deployed IAFIS and NCIC 2000 in July 1999, the FBI fingerprint systems were not linked to IDENT.

The Resendez case vividly illustrated the need for integration of the INS and FBI systems and spurred the FBI and the INS to develop an integration plan. The plan required studies to help determine the feasibility of integration of the systems, which initially would allow the fingerprints of aliens apprehended by the INS to be searched against a subset of the FBI's Criminal Master File and eventually against the entire master file. However, an integration plan is still in the process of being developed and may take years to implement fully.

C. Nonimmigrant Overstays

The INS estimates the number of illegal aliens in the United States at 5 million to 6 million, while others estimate the number to be even higher. A common perception about illegal aliens is that the vast majority enter the United States by surreptitiously crossing our land borders, primarily from Mexico. In fact, the INS estimates that approximately 40 to 50 percent of the illegal alien population entered the United States legally as temporary visitors but simply failed to depart when required. The INS refers to these illegal aliens as nonimmigrant "overstays." More than 90 percent of overstays are tourists or business visitors, but overstays also include students and temporary workers.

In a 1997 inspection, the OIG found that the principal INS record-keeping system for tracking nonimmigrant overstays, the Nonimmigrant Information System (NIIS), does not produce reliable data, either in the aggregate or on individual nonimmigrants. Normally, passengers arriving in the United States fill out an I-94 form and present it to the INS inspector upon arrival. The inspector collects the arrival portion of the form and returns the departure portion to the passenger. The arrival portion is sent to an INS contractor, who inputs the data into NIIS. When the person leaves the United States, the airlines are supposed to collect the departure portion of the I-94 form and provide it to the INS for input into NIIS. The data is then matched by NIIS to identify nonimmigrant overstays.

We found that the NIIS data is incomplete and unreliable due to missing departure records and errors in processing of the records. NIIS does not contain departure records for a large number of aliens, most of whom the INS assumes have left the United States. The INS believes that unrecorded departures result from airlines failing to collect departure forms, from aliens departing through land borders, from data entry errors, from records being lost through electronic transmission or tape-loading problems, or from the failure of the system to match arrival and departure records.

We also found that the INS had no specific enforcement program to identify, locate, apprehend, and remove nonimmigrant overstays, and we concluded that NIIS data would be of little use for locating aliens.

D. The INS's Automated I-94 System

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 directed the Attorney General to develop an automated entry and exit control system that would collect a record for every alien departing the United States and automatically match these departure records with the record of the alien's arrival. This proposal was designed to replace the manual system of collecting I-94 cards and enable the INS, through on-line searching procedures, to identify lawfully admitted nonimmigrants who remain in the United States beyond the period authorized. In 2000, however, Congress extended the deadline for implementing the system for airports and sea border ports of entry until December 31, 2003, and for high-traffic land border ports of entry until December 31, 2004.

In response to this congressional requirement, the INS introduced a pilot system in 1997 to automate the processing of air passenger I-94 forms. This automated I-94 system captures arrival and departure data electronically and uploads non-U.S. citizen data to the INS's NIIS.

This summer, the OIG completed an audit of the design and implementation of the automated I-94 system and found that the INS has not properly managed the project. Despite having spent \$31.2 million on the system from FY 1996 to FY 2000, the INS: (1) does not have clear evidence that the system meets its intended goals; (2) has won the cooperation of only two airlines; (3) is operating the system at only a few airports; and (4) is in the process of modifying the system. INS officials esti-

mated that an additional \$57 million would be needed for FY 2001 through FY 2005 to complete the system. These projections include development, equipment, and operation and maintenance costs.

As a result of our concerns, we made a series of recommendations to help ensure that the INS rigorously analyzes the costs, benefits, risks, and performance measures of the automated I-94 System before proceeding with further expenditures.

E. The Visa Waiver Program

The Immigration Reform and Control Act of 1986 created the Visa Waiver Pilot Program (VWPP), which permitted citizens from certain countries to enter the United States as visitors without first obtaining a visa. The law allowed VWPP visitors to stay in the United States for up to 90 days per visit and required them to possess a round trip ticket and waive their rights to appeal immigration officers' determinations of admissibility or contest any deportation actions.

In October 2000, the program became permanent and is now known as the Visa Waiver Program. Currently visa requirements are waived for citizens of 29 countries who wish to visit the United States.

In 1999, the OIG assessed the INS's efforts to minimize illegal immigration and security threats posed by abuse of the VWPP. Because visitors traveling for business or pleasure under the VWPP were not required to obtain visas, they were not screened in any way prior to their arrival at U.S. ports of entry. Instead, VWPP visitors presented their passports to INS inspectors on arrival. The inspectors observed the applicants, examined their passports, and conducted checks against a computerized lookout system to decide whether to allow applicants entry into the United States. This review by INS inspectors was the principal means of preventing illegal entry. INS inspectors had, on average, less than one minute to check and decide on each applicant.

As a result of our review, we found that INS inspectors did not query all VWPP passport numbers against the INS's computerized system. In addition, our inspection noted that terrorists, criminals, and alien smugglers have attempted to gain entry into the United States through the VWPP.

During our review, the INS informed the OIG that the theft of passports from VWPP countries was a serious problem. Because these stolen passports are genuine documents, their fraudulent use is difficult for INS inspectors to detect. During our review, we tested a sample of 1,067 passports stolen from VWPP countries and found that almost 10 percent may have been used to successfully enter the United States. We also identified problems with the way the INS maintains its lookout system, including its failure to enter information about stolen VWPP passports into the lookout database in a timely or accurate manner. As a result, 567 stolen passports in our sample of 1,067 (53 percent) had no lookout record in the INS system. Of the 500 passport numbers that had lookout records, 112 (22 percent) were not entered accurately. This missing or inaccurate information reduced the effectiveness of the lookout system and increased the possibility that inadmissible VWPP applicants could enter the United States.

F. The OIG's "Bombs in Brooklyn" Report

In a report issued in March 1998, the OIG examined how two individuals, Gazi Ibrahim Abu Mezer and Lafi Khalil, entered and remained in the United States before their July 1997 apprehension in Brooklyn for allegedly planning to bomb the New York City subway system. Mezer was subsequently convicted and sentenced to life imprisonment. Khalil was acquitted of charges stemming from the bombing plot but found guilty of immigration violations.

In our report, we described how both men were able to enter the United States and remain here. Khalil, who had a Jordanian passport, applied to the U.S. Consular Office in Jerusalem for a visa to travel through the United States en route to Ecuador. The consular official gave him a 29-day, C-1 transit visa after a three-minute interview. When Khalil arrived in New York on

December 7, 1996, an immigration inspector mistakenly granted him a 6-month, B-2 tourist visa. He overstayed that visa and was arrested in Brooklyn, along with Mezer, in July 1997.

Mezer, who claimed Jordanian nationality, received a visa from the Canadian Embassy in Israel to study in Canada. Shortly after arriving in Canada in September 1993, he applied for convention status, which is similar to political asylum in the United States, based on his claimed fear of persecution in Israel. Mezer later admitted that he had traveled to Canada with the intent to reach the United States.

In 1996, Mezer was detained by the Border Patrol twice while attempting to cross the border into Washington State. Each time the Border Patrol voluntarily returned him to Canada. In January 1997, the Border Patrol apprehended Mezer in Wash-

ington a third time and initiated formal deportation proceedings. Mezer then filed an application for political asylum in the United States and was later released on a \$5,000 bond. In his asylum application, Mezer claimed that Israeli authorities had persecuted him because they wrongly believed he was a member of Hamas. The immigration court requested comments from the State Department about Mezer's asylum application, and the State Department returned the application with a sticker indicating that it did not have specific information on Mezer. Mezer's attorney later withdrew the asylum application, stating that Mezer had returned to Canada. Mezer was arrested shortly thereafter in Brooklyn for plotting to bomb the subway system.

During our review, we did not find any information that Mezer was a known terrorist. However, we found systemic problems that were revealed by his case. Our review found that Mezer had entered and remained in Canada despite two criminal convictions there, which highlighted the ease of entry into Canada and the difficulty of controlling illegal immigration from Canada into the United States. We also noted the inadequacy of Border Patrol resources to address illegal immigration along the northern border. In addition, Mezer's case reflected confusion between U.S. government agencies as to which agency would conduct a check for information on whether an asylum applicant was a terrorist. We recommended that the INS and the State Department coordinate more closely on accessing and sharing information that would suggest a detained alien or asylum applicant may be a terrorist.

G. Border Patrol Efforts Along the Northern Border

In February 2000, the OIG issued a report that systematically examined the Border Patrol's efforts to control illegal activity along the northern border, examined how the Border Patrol collects and assesses information about illegal activity and responds to it, and evaluated the allocation of Border Patrol resources to the northern border.

The nearly 4,000 miles of border between the United States and Canada are managed by 8 of the Border Patrol's 21 sectors. As of September 30, 1999, 311 of the national total of 8,364 Border Patrol agents (3.7 percent) were assigned to northern border sectors. In keeping with the INS's strategic plan, the Border Patrol deployed 7,706 Border Patrol agents (92.1 percent of the total) to its nine southwest Border Patrol sectors. The remaining 347 agents were assigned to the coastal sectors, headquarters, INS regional offices, and the Border Patrol Academy. Currently, according to the INS, there are 334 Border Patrol agents assigned to the northern border.

Border Patrol sectors on the Canadian border face significant challenges, even though the volume of known illegal alien entries is much less than along the Mexican border. The OIG review reported an increase in illegal activity along the northern border, including an increase in alien and drug smuggling. But the INS was unable to assess the level of illegal activity along the northern border, given the limited personnel and equipment resources allotted to its eight northern Border Patrol sectors. However, it is clear that the level of illegal activity exceeds the Border Patrol's capacity to respond. We also found that other factors, such as the detailing of agents from the northern to the southwest border and lack of detention space to house apprehended aliens, further diluted the Border Patrol's enforcement capabilities along the northern border.

We concluded that the number of agents assigned could not adequately patrol the entire length of the northern border. Shifts with no Border Patrol coverage left the northern border open. INS Intelligence officers also told us that criminals monitor the Border Patrol's radio communications and observe their actions. The criminals know the times when the fewest agents are on duty and plan their illegal operations accordingly. The Border Patrol realized this risk but, because of the low numbers of agents assigned to northern border sectors, it could not cover all shifts 24 hours a day, 7 days a week. Most Border Patrol officials we interviewed believed around-the-clock coverage was the minimum acceptable level of coverage for northern Border Patrol stations.

"Force-multipliers" such as cameras, sensors, and other technology aid the Border Patrol in its surveillance and interdiction activities, but we found that northern border sectors do not have adequate amounts of this equipment. For example, at the time of our inspection, one northern border sector had identified 65 smuggling corridors along the more than 300 miles of border within its area of responsibility, but the sector had only 36 sensors with which to monitor these corridors.

The Border Patrol's Strategic Plan, issued in 1994, does not address the northern border until the plan's fourth and final phase. Phase I of the Strategic Plan was designed to control the San Diego and El Paso Corridors; Phase II to control South Texas and Tucson corridors; Phase III to control the remainder of the southwest border; and Phase IV to control the rest of the borders, including the northern bor-

der. At the time of our inspection in 2000, the Border Patrol was in Phase II of its strategic plan, and no date had been set for implementation of Phase IV. In addition, the strategic plan did not articulate the strategies that the Border Patrol would eventually use to control the northern border once it has achieved control of the southwest border.

The OIG recommended that the INS Commissioner outline the approach the Border Patrol would take to secure the northern border, including determining the minimum number of Border Patrol agents required to address existing gaps in coverage, determining the amount of intelligence resources needed to more accurately assess the level of illegal activity, and identifying and implementing accurate data collection methods to support decisions about personnel and equipment. INS eventually wrote a strategic plan regarding the northern border, but we understand that it has not been implemented. We also recommended that the Commissioner evaluate whether there was a continuing need to detail Border Patrol agents out of northern sectors.

H. Other OIG Reviews

In addition to these reviews, the OIG has examined other INS programs and their related automated systems, including:

- *Voluntary Departures:* A 1999 OIG inspection found that the INS could not verify evidence of departure in 54 percent of the cases that we reviewed in which an illegal alien had been permitted to voluntarily leave the United States rather than face deportation. We found that the INS's record keeping for voluntary departures was seriously flawed. The INS's failure to document voluntary departures resulted in an incomplete immigration history for these illegal aliens and hampered subsequent efforts by INS or other law enforcement officials who need to complete immigration histories for each illegal alien they encounter in order to make appropriate decisions about the alien's disposition.

In addition, we concluded that the INS's Interior Voluntary Return Tracking System (IVRTS), implemented in FY 1997, did not track individual aliens who were granted voluntary departure and thus could offer only an incomplete count of the number of these departures nationwide. At the time of our review, IVRTS did not record the names or alien numbers of the aliens granted voluntary departure. Furthermore, the system provided no information suitable for follow-up enforcement and no useful information to include in the INS's lookout indices.

- *Secondary Inspections at Airports:* The Treasury Enforcement Communications System (TECS) is a system used by the U.S. Customs Service, the INS, and other federal agencies to access information about individuals who are of interest to law enforcement agencies so that their entry into the United States may be monitored or prevented. TECS allows INS inspectors to review an individual's travel history, including the results of prior inspections, when determining the admissibility of persons seeking entry into this country. Other federal agencies and INS programs, including those focusing on intelligence and counterterrorism, often rely on INS inspection data in TECS.

A March 2001 OIG audit tested INS data in TECS related to secondary inspections (inspections of travelers that require a more detailed review than the standard primary inspection) at three airports. The audit examined whether the data accurately reflected referrals of travelers to secondary inspection and whether the data included secondary inspection results. We found that the INS's data in TECS for inspections performed at two airports were reliable, while the data for inspections at the third was not. We found that the third airport's inspectors entered the required referral designation and secondary inspection results in TECS for only 3 percent of the secondary inspections performed.

III. CONCLUSION

As described by these reports, our work has found that the INS has not managed its diverse information technology systems well. We found numerous and long-standing problems of failures by INS managers to implement reliable, integrated systems in a timely and cost-effective manner.

We believe that the INS needs to more stringently establish priorities on the development of its systems, rather than spend enormous resources and effort to develop so many systems for so many different purposes. The INS has in use or in development approximately 100 automated information systems and it appears to

have a separate system for each function in the agency, without sufficient connection or interrelation.

Among other recommendations, based on our work we urge the INS to ensure that its databases share information, both within and outside the INS. For example, the INS and the FBI's automated fingerprint systems—IDENT, IAFIS, and NCIC 2000—need to be connected. The INS also needs to expand the use of biometrics to accurately identify individuals with whom the INS comes into contact.

It is clear that more resources need to be devoted to the northern border. Technology such as cameras and sensors can help in this effort, but there are too few agents and inspectors along the northern border.

The INS also must improve its tracking of nonimmigrant visa overstays. The current system for identifying overstays—manual I-94 cards inputted into the NIIS database—does not produce reliable or accurate information, either as a whole or on individual overstays, and the automated I-94 project has not worked. The INS must design a system that can accurately capture arrival and departure data, and automatically match them in a reliable fashion.

Solving the problems of INS information technology is a complex issue with no easy solutions, but it requires a strategic vision, strong leadership, and individual and organizational accountability. This effort needs to be a top priority of the agency, since effective INS information technology is essential to protecting the integrity of the immigration system and the national security.

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

Mr. GEKAS. We thank the gentleman.

We turn to Commissioner Ziglar. James Ziglar had, prior to becoming Commissioner of INS, served as sergeant at arms in the Senate of the United States. There, he, in effect, came back to the Senate because he, at one time, served as an aid to then-Senator Eastland. He also had served as a law clerk for Supreme Court Justice Blackmun, has served on Wall Street with a lot of different entities and now comes to bring his long legal experience, and practical experience, and political experience, I might add, to the current post of Commissioner of the INS.

We welcome him and ask him to proceed with a 5-minute summary of his written testimony. But before he does that, we will ask him to identify the colleagues who have joined him, the ones who joined him in taking the oath, so that we can identify them for the record. So would you introduce them separately.

TESTIMONY OF THE HONORABLE JAMES W. ZIGLAR, COMMISSIONER, IMMIGRATION AND NATURALIZATION SERVICE; ACCOMPANIED BY SCOTT HASTINGS, ASSOCIATE COMMISSIONER FOR INFORMATION RESOURCE MANAGEMENT; DAVID YENTZER, ASSOCIATE COMMISSIONER FOR ADMINISTRATION; AND MICHAEL PEARSON, EXECUTIVE ASSOCIATE COMMISSIONER FOR FIELD OPERATIONS

Mr. ZIGLAR. Thank you, Mr. Chairman. I have with me today a variety of the folks from the INS who are expert in a number of the issues, areas that you are talking about today.

Mike Pearson is head of field operations; Mike Cronin, who is our program director; Bob Gardner, who is our budget director; Dave Yentzer with the management side of the business; George Bohlinger, who is with the management side of the business; Paul Rosenberg, who is head of our Enterprise Architecture Area; and Scott Hastings, who is our technology guru.

Mr. GEKAS. We may have to pepper them with some questions along with questions for you at a later point. Proceed.

Mr. ZIGLAR. I was pleased that you put them under oath, so that you could.

Mr. GEKAS. Very good. Please proceed.

Mr. ZIGLAR. Thank you, Mr. Chairman. I am pleased to have this opportunity to come today and talk to you about technology, in terms of how it can help us to secure our borders. This is, as Congresswoman Jackson Lee noted, my first appearance before this Committee, and I am pleased to be here. I certainly enjoyed my time over on the Senate side as sergeant at arms, and I had an opportunity in that job to work with a number of Members of the House, as well as some of your officers in the House, and it was a great experience for me.

When I started this job 2 months ago, I knew I had a big challenge in front of me, and Congressman Gekas certainly made that point to me on several occasions when we discussed it. I never had even an inkling, Mr. Chairman, that events would take the dramatic turn that they have, and we sit here today facing what we face.

The goals that the President set for me and that the Congress wholeheartedly endorsed when I took this job were really threefold: First was to restructure the INS in a way that it would focus on its two missions and focus on them effectively, and that is enforcement and service; the second goal that I was given was to modernize the management structure and the processes of the INS so that it could do its job and serve its mission better; and thirdly was to modernize, synchronize and rationalize the IT technology system at the INS again so that we could better serve the missions that we have in front of us, and that is enforcement and service.

Mr. Chairman, these goals are exactly the same today as they were before September the 11, for the simple reason that an effective and efficient INS is the best way that I know of to help protect Americans, along with other Government agencies, against the evils that we saw and that occurred on September 11. Congresswoman Jackson Lee, I can tell you that we want to be part of the solution to the problem, not the problem.

Mr. Chairman, I am neither inclined, nor particularly willing, to waste my time on trying to assign blame for failures in the past or perceived failures in the past. I think we can, and we should, learn from failures, but we need to move ahead, and we need to move ahead aggressively with this organization.

I believe that the INS has the will, I believe that it has the determination, and I believe that with adding some human resources, we have the human resources necessary to accomplish the mission that you want us to accomplish and that the President wants us to accomplish. We are moving ahead rapidly, Mr. Chairman, as I speak, in making those changes. Let me give you some examples.

First, we will very soon be providing to you a reorganization, a restructuring plan that is significant, that is substantial. That plan has been developed, and we have continued the development of it even since September 11. It has been personally approved by the Attorney General. He has spent time with me looking at it, and he has personally approved it. It is now pending before OMB, and it is in the final stages of approval over there, at which point we will bring this draft plan up to you and to your colleagues, and show

it to you, and get your feedback, and work with you on it, and we will need your help on that, Mr. Chairman.

Mr. Chairman, we are aggressively developing an IT enterprise architecture, and we are doing it, as Mr. Hite noted, we are doing it in concert with the GAO, and we are doing it based upon a suggested plan that the GAO has given us. We are proceeding with the GAO. We have people at GAO and our organization on a regular basis. We welcome their help. They have been a great resource for us in the development of this enterprise architecture.

Also, Mr. Chairman, let me address one thing about that enterprise architecture and what the GAO did, and that is that with respect to our investment management, we have created an Investment Review Board that is, on a regular basis—and I have personally gone to these meetings. I have not left them to other people—we are looking at every technology that we are trying to employ now, even ahead of the enterprise architecture design being completed and using something called the interim technology architecture to make sure that the employment of these technologies will fit on the platform that will ultimately come out of the enterprise architecture planning. So we are dealing with the investment management area. And, again, GAO is quite aware of what we are doing, and working with us, and working with us very cooperatively.

Mr. Chairman, with your support, we are prepared to move ahead with the SEVIS system—it used to be called the CIPRIS system—but which is the student tracking system. As you know, that system has been delayed for a variety of reasons. It was the subject of great opposition by the academic establishment and some institutions. It was the subject of a bit of criticism, particularly from Congress, and particularly with respect to the fees that would be collected and how they were collected, and it took legislation to change that process.

We have, all of a sudden, experienced, for some reason, a disappearance of all of that opposition since September the 11. And, in fact, several weeks ago I sent over for approval the regulations to implement the fee collection structure so that we can start getting revenues in for the system, and as you know, the system has to be paid for out of the revenues collected.

Mr. Chairman, with some appropriated funds up front so that we can build the system quickly, as opposed to building it out of the revenues that come out of the exam fees, we can deliver the SEVIS system a year, I believe, in advance of the December 20, 2003, deadline that Congress has set on us to have that system in place, but we need your help. We need your money to do that.

Mr. Chairman, we are integrating our various, and we have got a bunch of them, our various enforcement databases, and they are already designed to do different things out there. It is an interesting exercise to try to figure out these databases, and I have been working hard at it, but we are integrating those databases into something called the ENFORCE system. The ENFORCE system literally will draw from all of the different databases that we have, as well as reaching out beyond our databases into the FBI and other places, to bring information in about individuals who then

that we come in contact, so that we know as much as there is to be known about these individuals.

We also have integrated, and it is fully integrated, our system, our ENFORCE system, which is the data collection system, with our IDENT system, which is an identification system. IDENT is not a database system, it is an identification system based upon biometrics. We have integrated those.

Mr. GEKAS. Without objection, we will extend an extra 2 minutes to the Commissioner to complete his oral statement because he is giving us vital information at this juncture.

Mr. ZIGLAR. Thank you, Mr. Chairman. I didn't realize I had run out of time.

In any event, the point is that we are building this platform and, in fact, we are putting in place, we are actually bringing our databases into the ENFORCE system now, and that platform will be on top of the overall enterprise architecture plan that is being developed.

Mr. Chairman, we are also going to be bringing on line soon the transitional work stations for the integration or the ultimate integration of the IDENT system with the IAFIS system which, of course, is the FBI system. That is being managed by the Justice Management Division. INS and the FBI are working together on them, but it will be soon that we will have in place those first work stations that are transitional work stations to the integration of that system. That is not inconsistent with our integration of IDENT and ENFORCE. It simply adds to the breadth of it.

Mr. Chairman, we are moving aggressively to implement the entry-exit tracking system that has been talked about so much. I have to tell you, on a personal note, I am very much in favor of putting that system into place, and I believe that we have our first deadline is in 2003, and I believe that we are going to meet that deadline, and I think we are going to beat that deadline. I am pushing people just as hard as I can to make things happen, and we can obviously talk about that in a few minutes in greater detail.

Finally, Mr. Chairman, with your support, we can complete the employment of the border crossing card system, and we can expand the IDENT system, and those are two issues I know that you want to talk about, as we go forward, in this hearing. I would love to be able to answer your questions on this.

Mr. Chairman, I appreciate the additional time that you have given me, but I want to make one last statement. I want you and this Committee to know, and I want the American people to know that the INS is moving forward and that we were moving forward before September 11 occurred.

Mr. Chairman, I appreciate the time, and I look forward to answering your questions.

[The prepared statement of Mr. Ziglar follows:]

PREPARED STATEMENT OF JAMES W. ZIGLAR

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE, I am pleased to have this opportunity to testify on "The Use of Information Technology in Immigration Enforcement."

This is my first opportunity to appear before this committee since being confirmed as Commissioner and I look forward to working with you for the benefit of the American people.

I am here today to discuss with you how the INS can enhance our country's security at our borders and in our processes, particularly in the context of the better employment of technology. While I am sure we could spend a great deal of time dwelling on past shortcomings in technology or other areas, I hope that we can focus on the future. Whatever the facts are from the past, Mr. Chairman, they are not a prologue for the future.

I have been on the job approximately two months. I cannot account for the reason one or another system did not come online by a particular date or did not function as advertised. Experience has taught me that there usually is plenty of blame to spread around. I have no interest in playing the blame game. My interest and inclination is to fix problems and always look ahead.

I can assure you of one thing, Mr. Chairman, and that is meeting deadlines set by the Congress and the President is my top priority. If a deadline cannot be met either because it is not realistic or for another legitimate reason, then my policy will be to tell Congress or the President in advance.

I have worked in the Congress, having served as the Senate Sergeant at Arms from November 1998 to August 2001, and as a staffer in the Senate from 1964 to 1971. I enjoy and treasure warm friendships with many Members of Congress from both sides of the aisle. I intend for my relationships with Members—and the agency's relationship—to be positive. I want us to work together for the sake of the American people. I have been very pleased that in the days and weeks since September 11, the sentiment I've heard time and again from Members of Congress has been: "How can we help?"

It is in that spirit that I come to you with this testimony about our technology systems, but, more importantly, with a series of ideas to improve our security in the months and years ahead.

STEPS TO IMPROVE SECURITY

Even before September 11, we were examining how we can improve the INS, at all levels, and especially in the area of technology. We recognize that technology is a huge "force multiplier" that we must employ effectively at the INS if we are to accomplish our mission.

Pursuant to the mandates of the Clinger-Cohen legislation, in response to the recommendations of the General Accounting Office (GAO), and because it makes good business sense, the INS is currently in the process of developing its Enterprise Architecture. This project represents our long-term, strategically-oriented approach to accomplishing the information driven aspects of the INS mission. We began the planning for this project in October 2000 and I expect the final delivery of this project, the transition plan to our target architecture, to be ready at the beginning of the 3rd quarter of FY 2002.

In addition, as part of our restructuring initiative, which I have discussed with you and a number of Members, I encouraged our employees at all levels to think "outside the box" as to how we can better accomplish our mission. They responded with a number of creative ideas, some of which we are still evaluating. However, within the context of what is already known to be "do-able" and effective, we are considering a series of measures that would strengthen our enforcement capabilities. We are working within the Administration to determine how to implement these measures. Some of our ideas are as follows:

Border Patrol

- As requested in the President's budget, increase the number of Border Patrol agents and support staff along the northern border, while not neglecting the continuing needs along the southwest border. Such increases should also include necessary facilities, infrastructure and vehicles.
- Provide additional agent support equipment and technology enhancements. Unfortunately, neither the Senate nor the House currently is funding the President's request at \$20 million for "force multiplying technology."
- Expand access to biometric identification systems, such as IDENT.

Inspections

- In the Inspections area, as we proposed in our FY 2002 budget, we believe we should increase the number of Inspectors at our Ports of Entry.
- Require inspection of all International-to-International Transit Passengers (ITI) so that all travelers who arrive in the United States are inspected.

Information and Technology Initiatives

- Require carriers to submit Advance Passenger Information before boarding passengers (whether the passenger is heading to the United States or attempting to depart the United States) to assist in preventing known or suspected terrorists, criminals, and inadmissible passengers from boarding.
- Make Advance Passenger Information data widely available to law enforcement agencies, enhancing the ability to identify potential threats prior to departure from or arrival in the United States, as well as to prevent the departure of individuals who may have committed crimes while in the United States.
- Implement the National Crime Information Center Interstate Identification Index (NCIC III) at all ports of entry so that aliens with criminal histories can be identified prior to or upon arrival in the United States. NCIC III should also be available at all consular posts, INS service centers and adjudication offices to help identify aliens who pose a potential threat.
- Improve lookout system checks for the adjudications of applications at INS service centers.
- Improve INS infrastructure and integration of all data systems so that data from all sources on aliens is accessible to inspectors, special agents, adjudicators, and other appropriate law enforcement agencies. This initiative is ongoing.

Personnel Issues

- Waive the calendar-year overtime cap for INS employees to increase the number of staff-hours available by increasing the overtime hours people can work. This proposal is included in the Administration's Terrorism Bill.

Other Initiatives

- Re-examine and potentially eliminate the Transit Without Visa Program (TWOV) and Progressive Clearance to prevent inadmissible international passengers from entering the United States.
- Reassess the designation of specific countries in the Visa Waiver Program to ensure that proper passport policies are in place. This initiative will require the concurrence of and joint participation by the Department of State.
- Obtain from the Department of State visa data and photographs in electronic form at ports of entry so that visa information will be available at the time of actual inspection.
- Explore alternative inspection systems that allow for facilitation of low risk travelers while focusing on high-risk travelers.
- Review the present listing of designated ports of entry, in concert with the U.S. Customs Service, to eliminate unnecessary ports. This will allow the INS to deploy more inspectors to fewer locations making for a more efficient use of resources.

DATABASE IMPROVEMENTS

In addition to the measures cited above, I have instructed my staff to move forward expeditiously on two database improvement projects mandated by Congress. While neither of these is a panacea, but both would be an improvement over the status quo. First, there has been much attention paid to student visas in recent weeks. Today, the INS maintains limited records on foreign students and is able to access that information on demand. However, the information is on old technology platforms that are insufficient for today's need for rapid access. That is why we are moving forward with the Student Exchange Visitor Information System (SEVIS), formerly known as CIPRIS. These objections, primarily by the academic establishment, have delayed its development and deployment. However, with the events of September 11, these objections have virtually disappeared and the INS, with your help, will meet, and intends to beat, the Congress' date of December 20, 2003 to start implementation of SEVIS with respect to all foreign nationals holding student visas. I hasten to add that there is a critical need to concurrently review and revise the process by which foreign students gain admission to the United States through the I-20 certification process as we build the system.

Second, substantial attention also has been paid to entry and exit data. Currently, the INS collects data on the entry and exit of certain visitors. The data, most of which is provided to the INS in paper form to meet our manifest requirements, first must be transferred by hand from paper to an electronic database. This is an extremely inefficient way of processing data which delays access to the data by weeks and months. Knowing who has entered and who has departed our country in real time is an important element in enforcing our laws. The Data Management Im-

provement Act, passed in 2000, requires the INS to develop a fully-automated integrated entry-exit data collection system and deploy this system at airports and seaports by the end of 2003, the 50 largest land ports of entry by the end of 2004, and completing the deployment to all other ports of entry by the end of 2005. The legislation also requires a private sector role to ensure that any systems developed to collect data do not harm tourism or trade.

The INS already uses limited airline and cruise line data which is now provided voluntarily as an integral part of the inspection process at airports and seaports. We will work closely with Congress, other agencies, and the travel industry in the coming months to expand our access to needed data and to enhance our use of that data to ensure border security and more complete tracking of arrivals and departures.

There has also been a great deal of focus on the databases used to identify persons who are inadmissible to the United States or who pose a threat to our country. The INS, the Customs Service, and the Department of State's Bureau of Consular Affairs have worked diligently over the past decade to provide our ports of entry and consular posts with access to data needed by our officers. The data contained in the National Automated Immigration Lookout System (NAILS), the Treasury Enforcement Communications System (TECS II), and the Consular Lookout and Support System (CLASS) are uniformly available to our ports of entry through a shared database called the Interagency Border Inspection System (IBIS) that is maintained on the U.S. Customs Service mainframe computer.

Through IBIS, the officers at our ports of entry can also access limited data from the National Crime Information Center (NCIC). Immigration and Customs officers have long had the capability to check NCIC wanted persons data on a limited basis. Only recently have immigration inspectors been authorized to routinely use NCIC criminal history data (NCIC III) to identify criminal aliens in advance of their arrival. This capacity now exists at two ports of entry. Before September 11, the INS was working to expand the availability of this valuable data source to additional locations. Legislation is being considered to ensure this expansion is successful. I strongly support this legislation. To expedite this process, we will require the assistance of Congress for additional communications and mainframe capacity so that we may obtain real-time NCIC III data.

Many people who cross our land borders do so with a Border Crossing Card (BCC). The INS and State Department have been working aggressively over the past several years to replace the old Border Crossing Cards with the new biometric "laser visa." Based on the statutory deadline, holders of the old BCC can no longer enter the country. The new BCC has many security features that make it a much more secure entry document.

Both at and between our ports of entry, the INS has used a fingerprint identification system known as IDENT to track immigration violators. This system has provided the INS with a significant capacity to identify recidivists and impostors. Congress has directed the Department of Justice to integrate IDENT with access to the FBI's automated fingerprint system, IAFIS, and we have been proceeding toward that objective with the FBI and under the Department's direction.

THE LIMITS OF TECHNOLOGY

There is no quick fix, technological or otherwise, to the problems we face. We must work with advanced technology and do all we can to improve our systems. But we should not mislead ourselves into thinking that technology alone can solve our problems. Technology must be coupled with a strong intelligence and information-gathering and distribution system if we are to leverage our resources and maximize our capabilities. That will require the seamless cooperation among the many government agencies involved.

It should be noted that more than five hundred million inspections are conducted at our ports of entry every year, and hundreds of millions of people enter the United States without visas, through visa waiver programs or other exemptions from the normal visa process; the INS has only 4,775 inspectors to process these hundreds of millions of visitors and approximately 2,000 investigators and intelligence agents throughout the country who are available to deal with persons who have entered illegally, are criminal aliens, or have overstayed their visas or otherwise have violated the terms of their status as visitors in the United States.

If we are to meet the challenges of the future, we need to make changes at the INS and we are in the process of making those changes. The structure of the organization and the management systems that we have in place are outdated and, in many respects, inadequate for the challenges we face. Our information technology systems and related processes must be improved in order to ensure timely and accu-

rate determinations with respect to those who wish to enter our country and those who wish to apply for benefits under our immigrations laws. The management restructuring of the INS is on its way—a mandate the President and the Congress have given me—and the improvement of our information technology systems is moving ahead and can be accomplished with the help and support of Congress.

Mr. Chairman, I would like to say one word about INS employees and the events of September 11. Within hours of the attacks, the INS was working closely with the FBI to help determine who perpetrated these crimes and to bring those people to justice. Within 24 hours, under “Operation Safe Passage,” the INS deployed several hundred Border Patrol agents to eight major U.S. airports to increase security, prevent further terrorist incidents and restore a sense of trust to the traveling public. At America’s ports of entry, INS inspectors continue to work tirelessly to inspect arriving visitors, while ensuring the flow of legitimate commerce and tourism. Meanwhile, despite the tragedies and the disruptions, our service operations have managed to complete over 35,000 naturalizations nationwide and process thousands of other applications since September 11. America should be proud of the extraordinary effort of these men and women.

LOOKING AHEAD

It has been said that after September 11 “everything has changed.” I hope that is not true. America must remain America, a symbol of freedom and a beacon of hope to those who seek a better life for themselves and their children. We must increase our security and improve our systems but in doing so we must not forget what has made this nation great—our openness to new ideas and new people, and a commitment to individual freedom, shared values, innovation and the free market. If, in response to the events of September 11, we engage in excess and shut out what has made America great, then we will have given the terrorists a far greater victory than they could have hoped to achieve.

Thank you for this opportunity to appear, Mr. Chairman. I look forward to your questions.

Mr. GEKAS. I thank the gentleman.

Let the record indicate that the gentleman from California, Mr. Gallegly, has joined the Committee.

And now I may be the only one in the room qualified to pronounce the name of the next witness, Mr. Papademetriou. You notice how fluently I was able to say it? [Laughter.]

Mr. GEKAS. He is our final witness from this panel. He has taught at American University, the University of Maryland, Duke, et cetera, and he has been published extensively on the immigration and refugee policies of the United States and other industrialized nations, and specifically on the impact of legal and illegal immigration on the U.S. labor market.

He, very interestingly, is one of the credits on a recent publication, “Economic Migrants: Trends in Global Migration,” which of course is apropos to all of the subject matters upon which we are touching in this hearing and in subsequent times.

So, with that, we ask Mr. Papademetriou to proceed.

TESTIMONY OF DEMETRIOS G. PAPADEMETRIOU, CO-DIRECTOR, MIGRATION POLICY INSTITUTE

Mr. PAPADEMETRIOU. Thank you, Mr. Chairman. Thank you, Ms. Jackson Lee, and Members of the Subcommittee. It is my pleasure to be here, and it is indeed a pleasure to have the Chairman be able to pronounce my name better than I can. [Laughter.]

Mr. PAPADEMETRIOU. I have also submitted a more detailed statement for the record, and there are several recommendations that you may find at the end of that statement that you may find of some value.

Ensuring our safety requires a comprehensive, systemwide response that goes well beyond the jurisdiction of this Subcommittee and includes not only the INS, but each and every public agency with which foreign entrants interact. Our Nation's security from foreign nationals who may wish us ill in the months and years ahead rests on the simultaneous and sustained pursuit of several initiatives. This is an extraordinary task under any circumstances. It becomes even more so, however, given our record as a people of a generally low attention span on matters large and small.

This tendency makes it all the more important that we resist the twin compulsions of, one, throwing money at the problem. This problem is too large, and it can break the bank rather quickly; and, two, rushing to create new and cumbersome data systems that may offer only marginal benefits to the common objective of making our country more secure, while having enormous long-term costs on who we are as a Nation.

The following is a list of actions focusing on the act of seeking access to the United States that, if pursued in concert and with determination, can truly enhance our collective security. When appropriate, certain caveats are also included.

First, engage in patient human and electronic intelligence gathering;

Second, share intelligence with all necessary safeguards and civil liberties with other agencies authorized to have direct or indirect access to that information in a timely fashion. The issue of how direct such access shall be will be crucial to how deep interagency cooperation will be and to the protection of our basic freedoms;

Third, insist on making cooperation among law enforcement agencies organic. That means breaking down in fundamental ways unhealthy bureaucratic competition over turf and resources and reducing jurisdictional overlap to the minimum required to maintain necessary redundancies;

Fourth, over time, achieve similar levels of cooperation with the intelligence gathering and law enforcement agencies of our allies in this war on terrorism, and particularly with those of our North American partners—Canada and Mexico. Seamless cooperation in protecting our common North American space, what some people now call “perimeter defense” is a goal worth pursuing at a pace and with as much vigor as prudence and the capabilities of each of our partners allow;

Fifth, use public resources smartly, efficiently, and responsibly, which, and apropos to the information technology focus of today's hearing, means keeping up with technological innovations in the pursuit of our national objectives. It may not necessarily mean, however, much greater reliance on increasingly more complex systems. Such reliance may make us less, rather than more capable to deliver what is needed over the medium term. This suggests that, in terms of technology, we should at least consider whether less may actually be more.

A single fundamental premise and overarching caveat, if you will, undergirds each one of these recommendations, and it is this: That we should not act in haste either in establishing new data systems or in adapting the latest technology. Proper use of existing data systems and incremental improvements in technology, to-

gether with stronger management by and career-long training of those who tend to and use those systems are likely to give us all of the tools our country needs to meet our security needs.

There are lessons, including ones in legislative humility, if you will allow me, to the fact that every time a Government bureaucracy's information systems are put under the microscope, extraordinary failures seem to be the inevitable refrain. This fact seems to hold whether the agency, under the microscope is the IRS, the INS or the Social Security Administration. The lesson seems to be that it takes time to assimilate new technologies and it takes real and sustained effort to use technologies efficiently.

A good rule of thumb about new data systems is to ask ourselves whether we are likely to be as eager to invest in maintaining and upgrading those systems and to use the information in them toward meeting an important public policy objective 3 or 5 years from now, when the national emergency no longer exists and other national priorities take their proper place in our policy and legislative pantheon as we are now. Given the apparent enthusiasm for various ideas about developing new tracking systems for noncitizens, this rule of thumb may be as good a common sense test as any we might apply to these proposals.

A crucial corollary to this rule of thumb stems from the simple fact that complex systems of any type, and particularly of systems that rely on the diligence and commitment of diverse governmental and nongovernmental actors for their successful operation require an extra dose of thoughtfulness before they are put in place. Tracking systems for foreigners should thus be particularly mindful of the following rule: they will be only as good as the data that go into them.

Such data will come from the INS, other enforcement agencies, the private for-profit sectors, such as airlines, contractors, et cetera, the private not-for-profit sector such as universities, employers of all types, and the like. Will all of these actors be as motivated as the INS may become, and apparently is, in always searching for missed records, fixing unintentional misreportings, or purging records as needed?

And what would the incentives be for doing so, especially since those in such a system will be foreigners, rather than U.S. citizens? In my view, the potential for enormous gaps, at least by the standard we seem to demand these days, increases exponentially in relation to the complexity of a system and to the number of the actors whose inputs become part of that system.

I would like to make one last comment. I know I am running over my time. A general proposition, keeping undesirable individuals out of the United States through "front-gate controls," that is, the visa issuance and border inspection regimes, is both easier and more effective than attempting to catch up with such persons after they enter the United States, and I have a number of recommendations of how we might do that, Senator.

[The prepared statement of Mr. Papademetriou follows:]

PREPARED STATEMENT OF DEMETRIOS G. PAPADEMETRIOU

Mr. Chairman, Members of the subcommittee: Ensuring our safety requires a comprehensive, system-wide response that goes well beyond the jurisdiction of this subcommittee and includes not only the INS but each and every public agency with

which foreign entrants interact. Our nation's security from foreign nationals who may wish us ill in the months and years ahead rests on the simultaneous and sustained pursuit of several initiatives.

This is an extraordinary task under any circumstances; it becomes even more so, however, given our record as a people of a generally low attention span on matters large and small. This tendency makes it all the more important that we resist the twin compulsions of (1) throwing money at the problem (this problem is too large and it can "break the bank" rather quickly) and (2) rushing to create new and cumbersome data systems that may offer only marginal benefits to the common objective of making our country more secure while having enormous long term costs on who we are as a nation.

The following is a list of actions focusing on the act of seeking access to the US that, if pursued in concert and with generally uncharacteristic determination, can truly enhance our collective security. When appropriate, certain caveats are also included.

- Engage in patient human and electronic intelligence gathering;
- Share intelligence—*with all necessary civil liberties' safeguards*—with other agencies authorized to have direct or indirect access to that information *in a timely fashion*. (The issue of how "direct" such access should be will be crucial to how deep inter-agency cooperation will be and to the protection of our basic freedoms.)
- Insist on making cooperation among law enforcement agencies *organic*. That means breaking down in fundamental ways unhealthy bureaucratic competition over turf and resources and reducing jurisdictional *overlap to the minimum required to maintain necessary redundancies*.
- Over time, achieve similar levels of cooperation with the intelligence gathering and law-enforcement agencies of our allies in this "war on terrorism," and particularly with those of our North American partners—Canada and Mexico. Seamless cooperation in protecting *our common North American space*, what some people now call "perimeter defense," is a goal worth pursuing at a pace and with as much vigor as prudence *and the capabilities of each of our partners allow*.
- Use public resources smartly, efficiently and responsibly—which, and apropos to the information technology focus of today's hearing, means keeping up with technological innovations in the pursuit of our national objectives. It may not necessarily mean, however, much greater reliance on increasingly more complex systems. Such reliance may make us less, rather than more capable to deliver what is needed over the medium term. This suggests that, in terms of technology, we should at least consider whether *less may actually be more*.

A single fundamental premise—an overarching caveat, if you will—under-girds each of these recommendations to this subcommittee. It is that we should not act in haste either in establishing new data systems or in adopting the latest technology. Proper use of existing data systems and incremental improvements in technology, *together with stronger management by and career-long training of those who tend to and use those systems*, are likely to give us all of the tools our country needs to meet its security needs. (There are lessons—including ones in legislative humility—in my view, to the fact that every time a government bureaucracy's information systems are put under the microscope, extraordinary failures seems to be the inevitable refrain. This fact seems to hold whether the agency under the microscope is the IRS, the INS, or the Social Security Administration. The lesson seems to be that it takes time to assimilate new technologies and it takes real and sustained effort to use technologies efficiently.)

A good rule of thumb about new data systems is to ask ourselves whether we are likely to be as eager to invest in maintaining and upgrading those systems—*and use the information in them toward meeting an important public policy objective*—three or five years from now, when the national emergency no longer exists and other national priorities take their proper place in our policy and legislative pantheon. Given the apparent enthusiasm for various ideas about developing new tracking systems for non-citizens this rule of thumb may be as good a common sense test as any we might apply to these proposals.

A crucial corollary to this rule of thumb stems from the simple fact that complex systems of any type, as well as systems that rely on the diligence and commitment of diverse governmental and non-governmental actors for their successful operation, require an extra dose of thoughtfulness before they are put in place. Tracking systems for foreigners should thus be particularly mindful of the following rule: *they will be only as good as the data that goes into them are*. Such data will come from

the INS, other enforcement agencies, the private for-profit sectors (airlines, contractors, etc.), the private not-for-profit sector (universities), employers of all types, etc. Will all these actors be as motivated as the INS may become in always searching for missed records, fixing unintentional misreporting, or purging records as needed? And what would be the incentives for doing so—especially since those in such a system will be foreigners, rather than US citizens? In my view, the potential for enormous gaps (at least by the standard we seem to demand these days, that is, some sort of a near-guarantee that attacks on us will not be repeated) increases exponentially in relation to the complexity of a system and to the number of the actors whose inputs become part of any data system.

By way of a conclusion, I will dwell briefly on how we may protect ourselves better from those seeking to take advantage of our immigration system for nefarious purposes. The particular focus of these remarks is the juxtaposition between “external” controls, that is, actions that we might take *before* an undesirable alien gains entry into our country and “internal” controls, that is, measures taken once one has been admitted.

I will start with a general proposition. *Keeping undesirable individuals out of the US through “front gate controls” (that is, the visa issuance and border inspection regimes), is both easier and more effective than attempting to catch up with such persons after they enter the US.* Focusing most of our additional resources on prevention measures has numerous advantages over any other single set of initiatives. Among them as the following:

- They afford law enforcement agencies more time to consider thoroughly and, as needed, investigate a foreigner’s application for a visa, while offering them “more bites at the enforcement apple.” Specifically, authorities have a chance to prevent one’s entry at the visa issuance step, at the point where such a person attempts to “breach” the North American perimeter defense (if they try to gain entry into the US by first entering either of our two contiguous neighbors), or when that person tries to enter the US. Conversely, the probability of stopping such a person diminishes the closer one gets to that last step.
- The visa applicant has few rights—our sovereign prerogatives are strongest at that point in the process and visa decisions are not reviewable.
- Arguably, adverse visa decisions do less damage to our international image, at least during national emergencies.
- At the visa issuance point, the amount of resources devoted to a post and the extra time we may wish to invest in looking over an applicant will affect the rate of entry of persons from certain countries and individuals fitting certain “profiles.” In the post-September 11 circumstances, most will judge such precautions as reasonable precautions.
- Finally, over time, investing resources in much more robust visa decisions will be less expensive both in capital costs and in costs to our civil liberties.

Thank you, Mr. Chairman, for the opportunity to appear before the Subcommittee.

Mr. GEKAS. We thank the gentleman. That concludes the formal testimony of the empaneled witnesses. We will begin with a period of questioning allocated to each Member of the Committee, beginning with the chair.

Just as we are stressing some of the inadequacies of technology in our national problems, we find a flaw in our own technology. Now you are going to have to rely on the chair to determine when 5 minutes have passed. So now the chair reluctantly yields to himself 5 minutes for the first round of questioning.

Mr. Ziglar, I want to get right to the nub of one of the problems and maybe we can solve it right here and now, you and I, right here in front of this Committee.

Answer this question for me or refer to one of your colleagues. Are the scanners for the border crossing card, have they been selected? Are they ready to be employed? Where are the scanners?

Mr. ZIGLAR. Mr. Chairman, as you know, and it has been reported, we do not have scanners in place. There is a fairly simple—

Mr. GEKAS. No, I am not asking—I know they are not in place. What I want to know is have we selected, under the bid process or any other process in the INS, which scanner you intend to use?

Mr. ZIGLAR. Mr. Chairman, we have two options. There is a scanner that is indigenous to this particular card or there is a scanner that is a more general scanner that will read a substantial amount of information in the laser card. Now let me explain what is going on here. At the time this was designed and implemented—

Mr. GEKAS. What was designed?

Mr. ZIGLAR. The laser card system, border crossing card system, was designed, it was designed to read these cards or for these cards to do a specific thing, and it had biometrics in it. Since that time, and the fact that we have not actually deployed the readers, and the reason for that has been no money to do it. No money has been appropriated. INS has requested the money. In '99, 2000, 2001, OMB cut the money out, it was never in the President's—

Mr. GEKAS. Wasn't the money allocated or appropriated in '96 to accompany the mandate for the program?

Mr. ZIGLAR. The money was only appropriated to get the program up and to start the creation of the cards itself, but money for the readers themselves has not been appropriated.

Let me back up and explain to you what is going on here. It is actually, in some ways, almost good news—I know it is sometimes hard to find good news here—good news that we have not deployed those scanners because now there are scanners that are available that are more generic that we can use other kinds of biometric technology and other kinds of technology and read those cards, but the IDENT system which we have deployed in 800 locations, and we are prepared to employ it at 1,100 more locations if Congress will lift its moratorium on the further deployment of IDENT. As you know, there has been a moratorium since 2000 on that.

The IDENT system is an effective biometric system. The laser card that has been created for the people at the border has their fingerprint in it. Those fingerprints have now been put into the IDENT system so that we have the same information with respect to the biometrics in our IDENT system that we have on that card. We can use the IDENT system now in secondary more effectively because it is more secure, and still use the laser card, because it has got the photograph on it, use the laser card in primary and be able to read that card.

So the answer is we have two choices in technology. Our preference, if we can get the money to deploy these readers, is to use the more generic reader and use the IDENT system for the biometric part of it.

Mr. GEKAS. Well, I am asking you right now, make a decision right here. Do you want to proceed with the one choice of the two? Let's proceed with one.

Mr. ZIGLAR. Yes, sir, we would like to.

Mr. GEKAS. Which one?

Mr. ZIGLAR. We would like to use the generic card.

Mr. GEKAS. Well, let's give directions to everybody—let's start formulating the program with that system in that mind.

Mr. ZIGLAR. Now that you mention it, Mr. Chairman, we have asked for money in the supplemental that is coming up here to do just that.

Mr. GEKAS. All right. So now the scanners—assuming that you get the full funding, when can we implement it?

Mr. ZIGLAR. Let me ask that question.

Mr. HASTINGS. The scanners that he is referring to will read multiple documents.

Mr. GEKAS. You better put that to the—Mr. Ziglar has to switch over—there—Mr. Papademetriou has accommodated us.

Mr. HASTINGS. Thank you. The scanners requested in the supplemental were designed to give us more flexibility in terms of secondary, where we see multiple documents that aren't necessarily standardized against our BCCs. We would have to go through a procurement and come up with a deployment schedule for that, but we could do that in a fairly dramatic time frame, I believe.

Mr. GEKAS. I want to pinpoint the schedule. What kind of a schedule can we halfway promise here today or move toward so we have something concrete? Every time we start saying we are going to have a time table, we are going to do it, and so forth, we have to bring you back here, we have to find out why you haven't done it, et cetera. I want to establish a time table, tentative, right now. And then if that doesn't suit, we will come back and reconjure it. But right now I need, for my purposes, an estimated time table.

Mr. ZIGLAR. Mr. Chairman, can I put an addendum on this because what I was talking about is what we think is now a more effective system because of the technology advances since we first started that, and that is using the IDENT system for the biometrics. And all of the cards that have been issued have the biometrics in the IDENT system. That is something, if the Congress will take its moratorium off and appropriate the money, we are ready to deploy 1,100 IDENT machines around the system. That is a very early effective way, in a fairly short time frame, to get up and running at the border using biometrics.

The other machine, if you will, that we are talking about is this generic card reader—I call it generic. It is not generic—this card reader that reads, can read a lot of different kinds of cards that we would like to deploy for that. That is—that would be subject to procurement and deployment, and that means it would be manufactured. My guess is I have no idea how long it would take to do the procurement and the manufacture, but my guess is—just give me a guess.

Mr. HASTINGS. With a competitive process, it could be 8 to 10 months. What we are saying here is in a fairly short order, if we would use the IDENT retrieval method, rather than the BCC, we would be retrieving the same data that we would get with a reader only with the IDENT fingerprint. We would be pulling back the same type of data, and that's technology we have in place now that with some minimal tinkering with it could be our solution in a very short time frame.

Mr. GEKAS. This new system or the one that you want to blend into was not in existence in '96—1996 or 1997 or 1998?

Mr. ZIGLAR. IDENT was in existence, Mr. Chairman.

Mr. GEKAS. Yes.

Mr. ZIGLAR. What we have now though is as a result of issuing these now over 4 million border crossing cards—they are called the laser cards—what we now have are the fingerprints, the biometrics—

Mr. GEKAS. I understand.

Mr. ZIGLAR [continuing]. Through those cards that we have transferred into our IDENT system. That means we can now identify who it is that is coming in by having them put their finger into a little machine.

Mr. GEKAS. But you said before that, back after the act was put into place, that you requested funding to proceed with it, but then at that time you didn't have the fingerprint portion of this biometric system.

Mr. ZIGLAR. Well, we were accumulating those fingerprints all during this entire period, but what wasn't deployed was the card readers—were the card readers. And the reason they weren't deployed was because there were no appropriations for that.

And the INS—I went back and checked this—the INS put the money in their budget request to OMB every year since 1999, and they got—they got nothing. And consequently it's pretty hard to deploy something if you don't have the funds.

Mr. GEKAS. I guess it was in your statement, Mr. Ziglar, that you stated that, based on the statutory deadline, holders of the old BCC can no longer enter the country. Yet we have—maybe you can square these two—a news release from the Department of Justice, which says that those persons seeking admission to the United States on or after October 1, 2001, must possess one of the following documents, and then proceeds to say the new biometric machine-readable, et cetera. Can you square these?

Mr. ZIGLAR. Yes, sir. The card itself that has been issued, there have been 4 million-plus biometric laser cards that have been issued. They are machine readable. They have on them a picture of the person right on the front of the card. They have embedded in the card some general information about the person, plus a biometric, and that is their thumbprint. Those cards will allow you to come across the border. Even though we don't have the machines to read them there, they are still identification. In fact, if anything, they are better—

Mr. GEKAS. Then they can enter the country. The BCC holders can enter the country. That's what you're saying.

Mr. ZIGLAR. Of the new BCC cards. The old BCC cards, that authority expired on October 1 or September 30, and those people who have not come forward and gotten the new card are now being turned back at the border.

As you may recall, Mr. Chairman, that has been extended now over a couple of years to give people an opportunity to come in and get it, the card. The State Department actually issues—

Mr. GEKAS. So they have to reapply.

Mr. ZIGLAR. They have to reapply.

Mr. GEKAS. But the statement on the news release also says, "Must possess one of the following documents: either the old INS-issued, nonbiometric BCC," which you say—

Mr. ZIGLAR. Oh, I'm sorry, Mr. Chairman. There is an iteration here. Those people who have shown up—a lot of people showed up at the last minute before the—before the deadline got their interviews and got approved for the new card, but the production of the new card had not happened. So what we did was we took the old card, we put a sticker that can't be taken off on it, and we clipped it in a certain way. And for those people who have been approved for the new card, they can come through with the old card clipped and stickered. Those people who have not gone through the approval process are being turned back.

Now, Mr. Chairman, I have talked to a number of your colleagues recently about this. If this is having a substantial impact on the border, and all I can judge is what are the number—what is the number of people that are being turned back. Right now we are running about 1,600 people a day that are being turned back.

If the Congress wishes to extend the statute to allow people with old border cards that aren't clipped and stickered, that's an option that the Congress has. I don't have the authority to extend the statute. What I did do was I did make the decision that if you had been approved for the card, but have not received the card yet because it hasn't been produced, that we would notate on the old card in a way that it couldn't be altered—or it would be very difficult to alter—notate that you had been approved for the card so that you could continue to come across, and that's the status of where things are now.

Mr. GEKAS. Well, I'm going to ask the Commissioner if he could establish a tentative deadline for March the 1st, coming, for at least a progress report to this Committee on these very same issues about the border crossing guards, in exchange for which, I will do what we can to see if we can statutorily deal with the matter. But your colleague said 8 months, et cetera. I'm going to try to keep that in mind, but by March the 1st I'd like to know where we are.

Mr. ZIGLAR. Mr. Chairman, I will let you know about that on a regular basis. You don't have to wait till March 1.

Mr. GEKAS. I understand, but I want to put something on the record to—

Mr. ZIGLAR. Sure. Absolutely.

Mr. GEKAS [continuing]. To put the bite on this.

The chair has overextended his 5 minutes, without question, and we now yield to the lady from Texas for 5 minutes.

Ms. JACKSON LEE. This is an important issue, Mr. Chairman, and I thank you for allowing me to overextend in the bipartisan spirit, but I do want to echo the Chairman's line of questioning and extend my hand of bipartisanship to work with him and to emphasize the timing. And knowing the proficiency of the new Commissioner, I would imagine that he could report to us earlier than March and would encourage him to work with us on that.

Following the line of questioning, let me say this, as I have said I think for a period of time, as I note my former chair in the chair, he knows that I always open hearings or make the point that we are a country of immigrants as well as laws or we are a country of laws and we are a country of immigrants, and we are probably both.

I have started saying, as well, that immigration does not equate to terrorism, and I believe this hearing today should reemphasize that, reemphasize that this is not an intent to target any particular group, this is not a hearing of blaming any particular group or isolating any particular group, and I would call out to my fellow Americans today that any actions of hatefulness or taking the law into your own hands should certainly not be promoted or tolerated in this Nation.

But I do have to pursue where we are, Mr. Hite and Mr. Fine, and I am prepared, maybe to the slight smile of Lamar Smith, to throw up my hands in ultimate and utmost frustration.

Tell me what you are speaking to, Mr. Hite. I think you used the word “technology speak,” and to be right INS must show its investment is right, something along those lines. I don’t want to misquote you. What is the basic problem that we have here, if you could give me that, and I’m going to get to you, Mr. Fine, and the Commissioner, and I would appreciate it if I could get my questions quickly answered so that I can sort of build a story that I can understand.

Mr. Hite?

Mr. HITE. I will do my best in responding to that. It’s a complex question, and I’ll try to give a simple answer to it.

You invest in technology for the purpose of advancing your capability to perform your mission. So everything that drives what you invest in should be driven by what your mission is. Knowing what the best mix of technology is to support that mission requires you to start at the top with a mission and deliberately go through a decision-making process of defining what we do, and how we do it, where we do it, who does it, and who needs what.

Until you construct a picture of your organization that way, both in logical business terms, as well in technology terms, and you set certain rules and standards that will govern how you are going to operate, until you do that, you lack the definition that those who are responsible for constructing the systems can follow in order to build an integrated, interoperable, efficient, effective set of supporting technology, infrastructure and systems.

Ms. JACKSON LEE. And that is the plight, if I will then move to the next logical thought, that is the plight you find the INS in at this point?

Mr. HITE. Absolutely.

Ms. JACKSON LEE. And are we too late? You know, mission development, as I recall in my days of study of sociology and psychology, is a long process. We’re in a crisis. What is your direct, I guess, response to how we get there quickly?

Mr. HITE. Right. I would say we’re not too late. As my oldest son says, knowing is half the battle, so the key is knowing where we are right now and then where we need to go to, and my suggestion would be that INS needs to proceed down two parallel tracks, one of which is you do what you can in the near term to address immediate needs through improvements at the margin, I would describe what the Commissioner was testifying to as improvements at the margin. At the same time, you proceed down a parallel track of transforming your organization to allow it to execute the mission effectively and efficiently in the future.

This is not a problem that is unique to INS. Other agencies have faced it. IRS, for example, has faced it. IRS is on the road to addressing this—in my view, well on the road to addressing this.

Ms. JACKSON LEE. So we must wrap this funding request that I think this Committee has, by and large, been fairly supportive. We must wrap it in preciseness, a defined mission and understanding what your technology systems can actually do, and how they integrate, which I think was part of the failure of September 11, 2001, which we keep referring to, but it has been a continuing failure.

Mr. Fine, let me ask you this: If there was ever a passion that I have developed over these last couple of days and you wish the passion was at a level previously, but I think we balance it on what we knew, is a whole issue of tracking the nonimmigrant visas, and I believe your comment was it does not produce reliable data. I would hope today we could tell America that we are starting on an immediate new pattern.

What is the fix? What is your, if you will, point about it is not producing reliable data? How do we correct that?

Mr. FINE. The system that currently exists is largely based on a manual system. It collects cards of arriving passengers. It tries to collect cards of departing passengers and tries to marry them up in the system, the nonimmigrant information system that the INS controls.

There has to be an automated process, and there has to be a clear commitment by all—the INS, the airlines, everyone—to insure that that automated process works because if we continue with the manual process, there will continue to be errors. There will be data errors, there will be matching errors, there will be failure to collect all of the data, and we will have no idea who has come into the country and who has left the country. That is the situation we are in right now.

The INS believes, when it matches the data and finds that there are several million nonmatches, that most of those people have left, but they can't tell for sure. The INS needs to look at the automated system that is being developed, see if it is going to accomplish the mission and move forward with that. Currently, we have done an audit of the pilot of the automated system, and we have seen problems with it. Part of the problems are that not everyone is participating. The airlines aren't participating. There may be a role for Congress, for example, to require participation in this process to ensure that there is an automated system that works.

Ms. JACKSON LEE. Let me go then—thank you. We could—I could probe you even more. I just wanted to isolate that. Commissioner Ziglar, please, there are two things. One, it looks like I lost where you were between biometric and generic. It looks as if, you know, the way to track this, and I'm going to get to his point, would be the generic with the handprint and the thumbprint, but how do you—how do you answer this immediately, dealing with automization, if you will, and being able to provide the viable data that is necessary to track overstays? Not saying that is the only solution to all of our problems, but it certainly is an important one. How can you get us to that point with taking into account your mission and understanding what kind of technology systems that you should use?

Mr. ZIGLAR. If you will indulge me, let me put this in some perspective. The notion of having an entry-exit tracking system for everyone who comes across our border who is not a United States citizen is a very ambitious project, and the reason that it's an ambitious project is because you have more than airports and seaports for people to come in. In fact, as you know, living in Texas, that most of the non-U.S. citizens that come into this country come over our land ports of entry.

What the Inspector General is talking about here, the system that we have in terms of tracking people who come in through airports, those ports of entry, we have a system. It's not effective, as the Inspector General pointed out, and we are moving to meet that deadline of 2003 to have an effective system at the airports and seaports. That is only one part of the equation.

Having an effective entry-exit system at all ports of entry, including land ports, creates a much bigger challenge because it will, as you can imagine, create potentially some huge backlogs and deterrent for people to come in the country over those land borders. So we need to define exactly what is it that we're looking at in terms of an entry-exit system.

I might also add—

Ms. JACKSON LEE. The gentleman is telling me that—excuse me, Commissioner, and I want to get your answer, but the Chairman has mentioned the timing, and I want to respect that as well. Can you just give me, I guess the succinctness of, and I will probe this with you later, but just this succinctness of this automation so we can—I hear what you're saying, but is there something that we can pinpoint and get done, and do you know what visas the hijackers came in on? I mean, how can that play into how we determine further what you do?

Mr. ZIGLAR. Congresswoman, it is my understanding that within the next day you will be getting information on these folks.

Ms. JACKSON LEE. All right. That's very important to us, but go ahead. I want to get my good friend at the end very quickly.

Mr. ZIGLAR. At least with respect to the ports of entry that are our airports and seaports, we are in the process of developing that entry-exist system, probably using the IBIS system as a base—not probably—using the IBIS system as a base. We think that we can implement that in pretty short order. Is that the answer you were looking for?

Ms. JACKSON LEE. That is the correct answer, and I will ask you, if you would later, give me a report on General Accounting Gao Zhang, who has been put on the back burner, a person trying to access legalization. I think you know her. She is a Chinese national that has suffered a lot.

I will conclude, Mr. Chairman, by just—I want Mr. Papademetriou to tell us why we can't throw money at the problem. He is our expert, and he had some suggestions that he didn't comment on at the end, and if he would do that, I thank the Chairman for his indulgence, and I thank the witnesses very much.

Mr. SMITH [presiding]. Thank you, Ms. Jackson Lee.

Ms. JACKSON LEE. Excuse me, Mr. Chairman. He was going to finish his sentence.

Mr. SMITH. We are beyond 10 minutes on the questions, and I think we probably ought to move on. I suspect the Chairman will have a second round.

Ms. JACKSON LEE. Thank you.

Mr. GEKAS [presiding]. The chair now recognizes the gentleman from Texas, Mr. Flake. Is he prepared? Congressman Flake?

Mr. FLAKE. I would be interested—thank you for the testimony—Mr. Fine, in your assessment of the testimony of Commissioner Ziglar. It sounds as if the only problem all along has been lack of funding or lack of appropriations to implement some of this. Is that the way you see it?

Mr. FINE. I think it's a complex problem. I don't believe it's solely a lack of funding. I'm encouraged by Mr. Ziglar's attention to this issue and dedication to ensuring that information technology issues in the INS get top priority. I believe it's a question of management and monitoring of information technology systems, designing and prioritizing which are the most important ones, focusing your attention on that, ensuring that there are standards and benchmarks by which the systems are judged so that they don't go on without any careful monitoring, go over cost, and that they are brought to fruition in a way that can fulfill the Agency's mission. I think it's a question of leadership and vision, and Mr. Ziglar has expressed the intent and the desire to focus attention on that, and I think that's an important expression.

Mr. FLAKE. Thank you.

Commissioner Ziglar, the IDENT system was really developed in the early 1990's, was it not?

Mr. ZIGLAR. I'm sorry. Did you say IDENT?

Mr. FLAKE. IDENT, yes.

Mr. ZIGLAR. I think it was started in '89, was started development, right.

Mr. FLAKE. Some are saying that it just doesn't work or isn't what we need for the future. Why should we invest in that? Is that still investing in old technology or not?

Mr. ZIGLAR. Congressman, I don't think so. The system works. What has happened is that it has not been deployed throughout the system. We have about 800 machines, if you will. We need another 1,100 to have it functional in the system. It has been now married up with the ENFORCE system, which is a database system which draws from other or will draw as we add the modules to it from the other databases that we have in outside databases. And when you remember that IDENT is not an information system, it's an identification system, it leads you into who the person is and then you have to go to other databases to get that information.

For example, IDENT is different than the NCIC, which is a name and date of birth entry kind of system. IDENT works, and it works very well. I don't think it is outmoded technology, and we are going to again, pursuant to the Congress's mandate, it is going to be married up with the IAFIS system, which is not, again, as I mentioned, a contradiction in terms of integrating with ENFORCE.

If I left you with the impression, Mr. Flake, that I am sitting here and saying that money is the only reason that we are in the

state that we are in, in technology in the INS, I apologize, because that is not my intent. The question just led that way.

It is clear to me that the real core of this problem is exactly what Mr. Hite said and what the IG said, and that is that we have lacked the development of an enterprise architecture plan which defined our mission, defined our goals, and defined the platform on which we were going to operate. That has been a lack, frankly, of, as the IG said, that is a lack of leadership and vision.

Now I don't claim to have leadership and vision, but I was a businessman for most of my career, and I understand about technology coming from Wall Street, and I know that Wall Street wouldn't be what it is today, but for technology. So I have a natural inclination to look at how can we leverage our business the best, how can we get force multipliers. So, if I gave you that impression, I apologize.

Mr. FLAKE. The Residez Ramirez case is the one that just strikes everyone as just the best example of what is wrong, I guess. Information simply wasn't shared, and as a result more people are dead. What—can we be assured today that the same thing would not happen? What measures have been taken since that to ensure the same thing doesn't happen today?

Mr. ZIGLAR. Congressman, that case was not a function of the technology breaking down. That was a case of the information not being put into the system, and that really is a matter of training of our people. That was a breakdown.

Now, as we build these databases and the interaction with other databases and bring them into one place, we will have more and more immediate access to information about these people, and it will come from other sources. So the likelihood of that happening grows less and less. But unless your people don't put the information in there, and we have to train them how to handle these systems and they're complex, that will happen again. But it's not a technology, that was not a technology breakdown problem.

Mr. FLAKE. That is more a function of leadership and vision than than of appropriation?

Mr. ZIGLAR. You betcha. You betcha.

Mr. FLAKE. And that culture is changing, you are telling us.

Mr. ZIGLAR. I have got to tell you. I like what I see over there. I see some people that really want to do a good job. I see some people that want to be motivated. I see people that want to be led, a need they understand the importance of what they do. And I tell you, it is a good bunch of people. They have taken a lot of criticism, they have taken a lot of beating, but these are good people, and they are good Americans, and they want to do their job.

Mr. FLAKE. Thank you.

Mr. GEKAS. The chair recognizes the gentleman from Texas for a round of questioning.

Mr. SMITH. Thank you, Mr. Chairman.

First of all, Mr. Chairman, I would like to thank you for having this hearing which is very much appreciated by those of us on the Committee, and I also want to thank you for a very informative memo in which it was pointed out that any number of immigration reform programs that should have been implemented have not been

implemented, and I know that is the subject of today's hearing as well.

Hopefully, though, with a new Administration and with a new Commissioner of the INS, we will do a better job than we have in the past several years of implementing some of these overdue immigration reform measures.

Mr. Fine, I would like to direct my first question to you, but also say I really appreciated your candid and honest testimony today, which indicates to me that the Inspector General's office is off to a good start.

My question is this, and you may well have answered it already in your testimony, but I wanted to ask you about the current status of INS computers being able to interface with the computers of other law enforcement agencies. As we know, part of the problem in the past has been a lack of compatibility between the databases. What is the status today and what are the prospects of having a fully integrated database system?

Mr. FINE. They do interface, to some extent. There is a sharing of information about lookouts through the interagency border inspection system, which is a system that the INS uses, along with the Customs Service, and the Department of State. That has always existed.

I think the big problem we have discussed today is some of the internal INS systems, particularly IDENT, interfacing with criminal information and other information from the FBI. That was—the INS and the FBI developed their systems on parallel tracks, but they never integrated them. And, quite frankly, the Resendez case spurred the development of an integration plan. It has not been implemented yet. It is still in the process. It clearly needs to be done so that those systems talk together.

Mr. SMITH. Thank you, Mr. Fine.

Mr. Ziglar, what I want to do is ask you about a number of immigration programs that should have been implemented, the deadline has passed, and ask you if you can give us an indication of when you think they might be fully operational, whether it is this year, next year or perhaps the year after.

Let me start with something that you have already mentioned a couple of times, and that is the student ID system, the student tracking system. You have mentioned I think twice, that the deadline was 2003. Actually, under the 1996 law, there was an initial deadline of December 1998 for the Attorney General to designate five countries from which we would track all students enrolling in United States or American schools and universities. To my knowledge, that 1998 deadline was missed, and my question for you, therefore, is when do you expect the Attorney General to designate those five countries, and that should be able to be accomplished I would think fairly quickly.

Mr. ZIGLAR. If you don't mind, Mr. Chairman, I don't know the answer to that question about the '98 deadline. What I know is that the Congress extended the deadline for the implementation of the system to December 20th, 2003. Obviously, I wasn't around in '98, but if you will let me ask somebody back here.

Mr. SMITH. Okay. Mr. Ziglar, let me explain that 2003 was the deadline for the full implementation of all students going to any

American university or school. The 1998 deadline was to track students from five countries to be designated by the AG. There is no reason that can't be effectuated in a matter of days, and that was my question as to when——

Mr. ZIGLAR. I understood your question, Congressman, and I was trying to say I didn't know the answer, but that deadline I wanted to ask someone to give me the answer.

Congressman, frankly, I wasn't aware of that deadline. I have been focused in 2 months on a lot of things, and I don't know the nuances, but if that deadline passed and hasn't been done and is still sitting there, by golly, I'm going to see to it that we get it done.

Mr. SMITH. Okay. Hopefully, within the next few weeks?

Mr. ZIGLAR. I'm going to see to it that we get it done, and I'll try to see that we get it done in that next 2–3 weeks. I don't do the designation, the Attorney General does, so I have to go through some layers of bureaucracy like we all do.

Mr. SMITH. You've mentioned the new-found cooperation on the part of universities and colleges. All you have to do is get the AG to designate five countries, and I think we can all guess what those five countries would be, and the system would be up and going.

Mr. ZIGLAR. Sure. But, of course, Congressman, we want to do this for all students, foreign students, coming in, in terms of knowing they're here and knowing whether they're living up to the terms of their matriculation and know when they leave.

Mr. SMITH. Right.

Mr. ZIGLAR. I mean, that's the real goal of this thing.

Mr. SMITH. Right. And that is what I think can be done fairly quickly and easily. Let me ask you about some other programs very quickly.

What about the entry-exit system at airports, which is also not fully operational, though it should have been?

Mr. ZIGLAR. I think I mentioned to Congresswoman Jackson Lee that that system we've got, as you know, has a series of deadlines. The first one is for airports and seaports for December 2003, I believe it is. We are developing that system, as we speak. We will use, I believe, the IBIS system or whatever its successor is eventually as the platform for doing that, and we believe we can meet that deadline.

Mr. SMITH. Mr. Ziglar, if you will check, I think you will find that there is an earlier deadline in 2003 for that as well.

What about the border crossing cards the Chairman asked you about a while ago? I heard you say shortly and use various descriptions like that. When do you think we might have that system fully operational? As you know, the deadline has been postponed twice, and as you said several days ago, it was supposed to be implemented and was not and individuals were turned away. When will we have that in effect?

Mr. ZIGLAR. Well, there are two or three points on that system. One is the deadline that we were talking about, of course, is the deadline for the use of the old border cards, and therefore the new border cards needed to be in place.

We have replaced about 4 million of those. Some people just, notwithstanding the extension that the Congress offered before, some

people didn't show up to get their approvals for them. They are still out there. Some people are being turned back at the border now because of that. The question of whether or not that part of it is extended is certainly a question for the Congress to decide, not for us. I don't have the ability to extend that part—that statute.

With respect to the question of how we fully implement the system, what I think you are referring to are the readers, and we had a—

Mr. SMITH. Right, we had a conversation about the scanners and the readers. When do you actually think that will be up and going, as it should be?

Mr. ZIGLAR. Congressman, if the Congress will lift its moratorium on the expansion of the IDENT system and if we can get the funding for that, we can deploy the rest of the IDENT cards. We can use the biometric database that came out of the approval process that the State Department went through. We can put those up as fast as we can get the manufacturer to deliver us those machines.

Mr. SMITH. Mr. Ziglar, the question of funding may be more appropriate for another time. I do know in the past the INS has been given all of the funding it has requested, and sometimes more, and still it hasn't gotten the job done. So I assume in your funding request you will do so.

Let me move on.

Mr. ZIGLAR. Congressman, may I address that? The INS, in its budget request within the Administration, in 1999, 2000, 2001, asked for money. The OMB cut it out of the budget. INS never got the money, but the INS itself has asked for that money consistently to buy those readers and to put that technology in place. I don't mean to pass off blame, but it is not like they didn't ask for it.

Mr. SMITH. Okay. I will take your word for it that they asked for it—

Mr. ZIGLAR. I looked at the budget submission just to prove—just to make sure I understood that.

Mr. SMITH. Well, I'm sure they will get it this year.

The last question goes to the section 110, as amended. This is the entry-exit system. As you know, when we amended it last year, a task force was supposed to be appointed by the Attorney General, and the Judiciary Committee of the House and the Senate were supposed to get reports. None of that has been accomplished. When do you think it might be accomplished?

Mr. ZIGLAR. I have advanced to the Attorney General our recommendations on the task force. It is pending approval. I have been pushing that, Congressman.

Mr. SMITH. Good. Thank you. My last question is this: What is the visa status of the 19 terrorists, specifically, and what is the visa status of some of the other individuals who have been detained? But more specifically I know the Committee asked you several weeks ago for the immigration status of the 19 terrorists. When will we get that information?

Mr. ZIGLAR. My understanding—of course, Congressman, I can't make that decision unilaterally. The FBI and others have to be part of that decision. But it's my understanding that you will have that information within 24 hours.

Mr. SMITH. Okay. Thank you, Mr. Ziglar.

Thank you, Mr. Chairman.

Mr. GEKAS. We thank the gentleman. Although we are not going to have a second round of questions, I want to give the lady from Texas time to complete her colloquy with Mr. Papademetriou.

Ms. JACKSON LEE. I thank you very much, Mr. Chairman.

I must have been mistaken. I thought we were in a second round, but let me try to quickly finish my questioning of Mr. Papademetriou and to say to the Commissioner we have got to have that information with respect to the terrorists, keeping in mind all of the security requirements. We are respectful of that, but in order to be part of the solution, as you've indicated, it is extremely important that we begin to fix this very severe problem. I hope the time frame of 24 hours is an accurate one.

I asked you about solutions, I believe, and as you well know, we have looked at the restructuring of H.R. 1562 to sort of fix the brokenness of the INS in terms of one hand not knowing what the other hand is doing. Service is part of the INS not being strengthened and then enforcement not being given the resources that it needs. You had some solutions, and I would appreciate it very much if you would provide them.

I do have a final question for Mr. Fine to be an aid to the Commissioner, and that is, and you can begin thinking about that, does the moratorium release or ceasing help us at all? Is that a solution to part of what we are talking about? I am going to let him speak first. Thank you.

Mr. PAPADEMETRIOU. Thank you, Ms. Jackson Lee.

Ms. JACKSON LEE. And thank you for your work.

Mr. PAPADEMETRIOU. Thank you. I appreciate the question. As you know, we have, for several years, engaged the issue of how the INS is organized and how it performs its various functions.

What I think I should say at this time is that I am extremely relieved to know that Commissioner Ziglar has a plan, that this plan is in the last stages of approval, and that in the days and weeks ahead we will all have an opportunity to look at what he has in mind in order to meet precisely the requirements that you have set, the objectives that I believe we all share.

Let me say a couple of things and reiterate a point that I made. A lot of the discussion that we have had about individual data systems or individual acts in which the INS has been engaging with regard to better security and better systems over the years, over the decades, I would say, bring to my mind the fundamental question, particularly with regard to this hearing at this time, of what is the precise policy objective of each one of those systems?

And I think that we have to be very careful to make sure that we understand what the primary objective is if we are to evaluate whether the investments on a particular new system or additional investments in an old system are justified. Let me give you an example. If, indeed, the objective of a better exit-entry control system is to know with greater or perhaps even far greater confidence who comes and goes out of the United States, I assure you that none of the things that we have discussed today will actually accomplish that.

Most of the things that we are talking about, including all of these, you know, the new machinery, the entry cards and all of that, I did a very quick calculation here, back of the envelope, will probably account for somewhere between 75 and 100 million entries. That assumes that the 4 million people who have those cards enter a certain number of times into the country.

What happens to the other 400 million entries? Ditto the same exact thing, in terms of tracking systems from within the country. I would like to know, and I have absolutely no objection whatsoever to developing tracking systems, whether it is foreign students, temporary employees or any other category of nonimmigrant or immigrant entry that presumably we all find necessary in order to increase our security, but I would like to know exactly what it is that we think we are going to accomplish with this. Are we going to send an FBI agent to investigate when a foreign student drops out of status because only he or she registered for three courses rather than five courses?

What are we going to do with all of these things? So it occurs to me that I want to emphasize—this is probably the last opportunity that I may have to speak on this issue—I want to emphasize what is it that we are trying to accomplish and how it relates to other policy priorities for our country. It is an issue that you have always raised in different words. You never hear that I have either been a participant or an observer.

And if I were to make, and I know it is not exactly today's focus, if I were to make a general global observation or recommendation it is that we should really pay much more attention in terms of controls where controls can happen most efficiently, most cheaply, and with fewer problems with regard to other things that we all consider very important—freedoms, liberty, and what have you—and those happen at the visa issuance process, before people even gain the initial right to travel to the United States because a visa only gives you that right. A visa does not give you a right, an absolute right to enter the United States. It gives you a right to basically get to a border post.

And I am suggesting that we should add another bite at the apple. So far we have, in a sense, three bites. The first one is issuing the visa, the second one is the border check or the check at the airport, the third one is trying to get control of people inside the country. I am proposing that we should add a fourth one that goes between visa issuance and a border check, which is thinking prospectively about how we might work with our immediate neighbors, our contiguous neighbors to develop a concept of perimeter defense because that allows us to check people not only before they get the visa issued, but actually before they reach North American space.

And I think that some investments, both in terms of thinking about this and how we invest in money, may be necessary in order to do far better, I think, than some of the systems that we are talking about here.

Ms. JACKSON LEE. Thank you.

Mr. GEKAS. We thank the gentleman.

Mr. ZIGLAR. Mr. Chairman, could you indulge me just one moment? Would that be possible?

Mr. GEKAS. Yes.

Ms. JACKSON LEE. Mr. Fine has a question outstanding to him.

Mr. ZIGLAR. Oh, I'm sorry. Pardon me.

Ms. JACKSON LEE. We would be happy to indulge you. I hope Mr. Chairman will, but I just hope Mr. Fine can answer his question.

Mr. GEKAS. We will let Mr. Fine answer.

Mr. FINE. I can answer that briefly, Congresswoman Jackson Lee. I would be in favor of lifting the moratorium on IDENT. I believe IDENT is a valuable system, a good system. The problem with IDENT is how it was deployed throughout the INS, how people were trained on it or weren't trained on it, and their understandings of the system. So they didn't use the system properly. It wasn't a problem with the system.

And, in addition, the INS needs to move forward with, in my view, integration of IDENT with other law-enforcement systems. The moratorium affects that. I believe the INS needs to develop, along with the Justice Management Division of the Department of Justice and the FBI, a careful, cost-effective plan that has measures by which to judge that process of integration, but I think that should go forward.

Ms. JACKSON LEE. Commissioner?

Mr. ZIGLAR. Mr. Chairman, I just have two things. One, my friend, Mr. Papademetriou, makes a very good point about intelligence and cooperation among agencies. What we have been talking about here today is the end product—the information, where it goes and how it's distributed, but how it is gathered originally is really important to our being able to enforce it. That wasn't the focus of this, but he is right on, on that position.

Secondly, Mr. Chairman, while we were sitting here, we got notice that we can release that information you wanted about the nine hijackers. I happened to have brought it with me just in case we could release it. I got the permission. I have a letter for you and for the Congresswoman.

Let me give you just a very quick summary. The evidence shows this, that 10 of the individuals came here in legal status, came here legally, and were in legal status at the time of September 11. Three of them came here legally and were out of status, had overstayed, on September 11. Six of the individuals we can find no record of them, period. That is not just INS, that's everywhere.

Understand that we had names of people. We don't know whether those were their names or not, and I suspect one of the reasons the FBI issued the pictures and the names, as you may recall a week or so ago, was to find out if anybody out there knew whether this person was the person who had that name. So we don't, you know, it's a problem about knowing who these people were and being able to match these names and these faces, but that's, in essence, what this says.

So I have these for you, and as soon as you gavel us out, I will hand them to you.

Ms. JACKSON LEE. Could he repeat them again, Mr. Chairman? Could you just repeat that again, just the breakdown. You said what—10?

Mr. ZIGLAR. Ten of them came here legally and were in legal status on September 11. Three of them came here legally and were

out of status on September 11. Six of them we have been unable to find any records relating to them. The names don't appear anywhere.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. GEKAS. That concludes the formal hearing. What I would like to do now is to ask the members of the panel if they would, in their kindness and good will, offer to answer any written questions that might be submitted by Members of the Committee pursuant to their testimony. If so, we will declare that the record is open, continues to remain open for Members of the Committee to submit any written questions they may have to each of the panelists.

Ms. JACKSON LEE. I would just ask if the Chairman would yield just for a question just for a moment.

Mr. GEKAS. Proceed.

Ms. JACKSON LEE. I did not pick up on Mr. Papademetriou's point about the problem being partly at the issuance of visas, and we all realize that that is a State Department issue, but it has become one of great concern to me. And I think the report that you just gave—ten legally here, three legally, meaning visas came in, et cetera and then overstays, and then of course we've got to find where the six were, really emphasizes the problem, and that is working with our State Department friends. I understand there is a task force. I am unhappy with where that is, and my question will be, to be able to get back with you on what I think is a mounting problem, and that is the issuance of visas in an appropriate manner. Thank you, Mr. Chairman.

Mr. GEKAS. We now extend our gratitude to the members of the panel and declare this hearing closed.

Mr. ZIGLAR. Thank you, Mr. Chairman.

[Whereupon, at 11:50 a.m., the Subcommittee was adjourned.]

A P P E N D I X

STATEMENTS SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE
IN CONGRESS FROM THE STATE OF TEXAS

INTRODUCTION

Thank you Mr. Chairman. This oversight hearing on Using Information Technology to Secure America's Borders: INS Problems with Planning and Implementation is important for two reasons. First, this hearing will help us understand what we can do to prevent events such as September 11th.

Second, this hearing is so vital because the mission of INS—to provide immigration services to aliens, citizens, and business and to enforce the nation's immigration laws—is absolutely dependent on information technology.

With poor information technology we are making our Immigration Inspectors, Border Patrol Officers, and Investigators work too hard. INS's border security enforcement systems do not work effectively. We need systems that are versatile.

Instead of hastily appropriating more money to INS whose budget has increased from \$1.4 billion in fiscal year 1992 to over \$5 billion in fiscal year 2001, we need to pursue other options. It is clear to me from my many dealings with INS that the main fix that is needed is a radical shift in the mentality of the Immigration and Naturalization Service. For years, I have struggled with the Agency who is unable to meet Congressional deadlines. After pouring in massive amounts of revenue Congress has not seen the improvements it desires. However, with better planning, structure, organization, and most importantly management, there is no question that the Agency will be able to meet its goals.

CONCERNS

It is unclear how many different types of border security enforcement systems exist. INS has been auditing what systems it has in place since January of 2000. In addition it is unclear what the purpose is of each system and how they operate. I hope Commissioner Ziglar that you will be able to inform us about the different systems that exist and how they operate.

Furthermore, I would like to highlight some of the concerns I have with the current structure of information technology.

1) A current snapshot of INS' management and investment of information technology as well as its information security management, show that INS cannot ensure (a) that the money it spends each year on information technology will be able to support the functions of the agency or (b) that its information technology resources are adequately protected from unauthorized access or service disruption.

2) There are simply too many different Border Security Enforcement systems to be used or managed effectively. Serious consideration needs to be given to consolidating as many of these systems as possible or creating one system so that all relevant data becomes available.

3) One major system, (the IDENT system) which is used to track recidivist aliens along the border between ports of entry has been badly implemented despite an investment exceeding \$80 million. DOJ's Justice Management Division is moving forward with an addition \$27 million integration effort. Serious consideration should be given to declaring a moratorium on spending more money on IDENT and instead replacing it with a new system that is truly integrated with all INS and FBI criminal databases.

I worked very closely on the Resindez Ramirez case in Houston. This was a failure of INS to adequately track a known criminal. Such a situation cannot happen again. And hopefully this hearing will lead the way in correcting that.

4) Currently some of INS's systems require biometric cards, some do not. Some cards have bar codes others have laser media. Some systems do not even use biometric data. There should be some discussion as to creating some conforming system so that all the information can be used for a single type of card-reading technology.

CONCLUSION

The recent terrorist attacks have seriously impeded legitimate international travel and commerce. At high-volume traffic land border ports of entry on both the Mexican and Canadian borders, efforts to increase border security have resulted in long waits, underscoring that the infrastructure and procedures at the land border ports of entry were not designed to allow inspectors to inspect thoroughly the travel documents of each and every person entering the United States. Just as the reduction in international air travel has reduced commerce and hurt the airline industry, long waits at land border ports of entry will also reduce commerce and hurt multi-national commercial interests in Mexico, Canada, and the United States. This is just another reason why we information technology is so important to INS.

INS's duties are completely dependent on information technology. INS must work effectively. Furthermore, I would like to reiterate that while funding for the INS has increased, INS has not become effective in managing information technology.

The lack of system versatility has a direct impact of those trying to carry out the mission of the Agency. The lack of system versatility compounds the complexity of people trying to do their job at the border and elsewhere.

Radical shifts in how INS manages information technology must be made. Furthermore, these issues should not be solved by pouring more money into the agency. What we need is a drastic change in the planning, structure, organization, and personnel not only of the Information Resource Division (the department within INS which handles information technology) but of the Agency itself.

MATERIAL SUBMITTED FOR THE HEARING RECORD



**USING INFORMATION TECHNOLOGY TO SECURE AMERICA'S
BORDERS: INS PROBLEMS WITH PLANNING AND
IMPLEMENTATION**

Expert Testimony

Demetrios Papademetriou
Co-Director, Migration Policy Institute
Washington, DC
October 11, 2001

IMMIGRATION AND NATIONAL SECURITY

In the wake of the terrorist attacks in New York and Washington on September 11, the US government and people are looking for every possible avenue to improve our security at home. Among the avenues being examined are immigration policy and border control. Given the extremely large numbers of people who enter and leave the United States each year, broad-brush immigration and border control measures will be extraordinarily costly and cumbersome, and run the risk of violating civil liberties. Their ability to reduce terrorist threats is unproven at best. Any such measures must pass an effectiveness test before we invest heavily in them.

The best instruments for combating terrorism are intelligence measures. Some of these can effectively be implemented in our immigration system, just as others will be implemented in our communications system or our banking system. Immigration itself is not the issue, although some immigration and border control measures can improve our ability to gather the intelligence needed to identify and obstruct terrorist plans.

The first step toward sensible security measures in immigration and border control is to understand the nature and the size of the traffic across our borders. The US government issued more than 7 million visas in the year 2000—7,141,636 to be exact. But this number is only a fraction of the number of people who enter the country. In fiscal year 1999, the last year for which data are available, some 31.4 million temporary admissions were recorded. These were tourists, business visitors, students, temporary workers, and such. They include visitors from the twenty-nine countries whose citizens do not need a visa for visits to the United States lasting less than 90 days under the Visa Waiver Program. Daily, there are tens of millions more who cross into the United States legally from Mexico or Canada, some on a daily basis. Since it is estimated that there are some 500 million entries and exits each year (a single individual may account for several entries and exits), it is our view that using immigration and border controls to stop terrorists is a needle-in-the-haystack approach to homeland security. The more effective route to greater security lies in the use of intelligence measures applied through immigration channels in ways that allow surveillance and law enforcement to target high-risk individuals and groups.

In this background paper, the Migration Policy Institute identifies immigration programs and procedures that lend themselves to better application of intelligence measures, and recommends changes that may increase security. We

1400 16th Street, NW Suite 300 Washington, DC 20036-2257 www.migrationpolicy.org 202 266 1945 202 266 1900 fax

are specifically concerned with those aspects related to entry (and to a lesser extent departure) and with internal control procedures. We advise against some of the anti-immigration measures, which we believe to be both costly and ineffective, that have been proposed in the House and Senate. Finally, we examine practices in the European Union that may offer useful lessons to the United States.

THE VISA REGIME

Legal entry to the United States for one who is not a citizen or legal permanent resident requires authorization. Some visitors, namely those from countries with which we have special agreements, are authorized simply by the passport they carry. But for many, authorization comes in the form of a visa issued by a US consular authority, responsible for screening applicants for legal entry into the United States.

Any system is only as good as the information on which it is based. The US has a visa system that admits people for permanent or temporary periods along a vast array of entry categories (see Tables 1, 2, 3 and 5, Appendix). Before a visa application can even be considered by a US consular official at a US embassy, the applicant must have a valid passport issued by the authorities of his or her country. Passports are among the most secure documents a state can issue, but they are not fraud-proof. Although still relatively rare, stolen or fraudulently obtained (but otherwise "valid") passports and identity switches are among the most problematic issues faced by consular officials who attempt to screen would-be travelers. In order to address this concern, applicants for visitor and immigrant visas are required to attend a personal interview with a US consular officer prior to receiving a visa in addition to presenting supporting documentation such as job letters, bank statements, and family records to support their claim of identity. Applicants for nonimmigrant visas must also prove that they are only planning to stay in the US for a finite period of time.

While reliable intelligence is at the very heart of the response to such problems, timeliness is equally of the essence. The Bureau of Intelligence and Research (I&R) is the Department of State's link to the US government's intelligence community and, in effect, the Consular Affairs (CA) Bureau's access point to the government's world of intelligence information (CA in fact contracts out that function to I&R). If intelligence is not shared with I&R in a timely fashion, the visa officer will not have the tools to deny a visa to an individual who should be excluded. Hence, the collection and timely sharing of relevant information is the first line of defense against the entry of excludable individuals into the United States.

The system relies also on several unique procedures to defend itself from security failures. For instance, since the 1993 bombing of the World Trade Center, visa officers are required personally to check each visa applicant against the Consular Lookout and Support System (CLASS) database, currently containing about 5.7 million records. Newly identified potential threats to US security are reviewed under the Visa Viper program, a system of domestic and international interagency committee coordination. The INS provides about 1.17 million lookout reports, with an additional 330,000 coming from the DEA, 20,000 coming from customs, and 500,000 provided by Consular Affairs (CA). Furthermore, applicants from certain countries and certain classes of applicants regardless of origin, must first be vetted through the State Department (I&R) for a security advisory opinion. In addition, other members of an embassy's country team—which typically includes a substantial representation of US intelligence agencies—are relied upon proactively by visa officers for information in detecting fraud and other problems in visa applications. (US embassy staffs collect all forms of intelligence information on a regular basis and send that information both to their respective agencies and to I&R.)

The **student visa system** operates somewhat differently. Individual institutions are authorized to grant visas to incoming and continuing foreign students. Prospective foreign students must present an I-20 form, obtained from the school that they will attend, a valid passport and a non-immigrant visa application form. Students may be requested to present further documentation, providing transcripts, financial statements, and standardized test scores. Student visas are valid for the duration of the applicant's *full time* student status. Once inside the country, it is often difficult to track students. The mammoth task of updating the status of thousands of foreign students to determine whether their current enrollment status is one that few university administrators would deign to undertake. Yet,

following the events of September 11, foreign student advisors "suspended" their opposition to "tracking" foreign students through the still evolving Student and Exchange Visitor Information System (SEVIS). (Until 2003, SEVIS will remain an "operational prototype" and schools that participate in it will continue to do so voluntarily.)

Finally, as a precaution, the visa system has certain built-in redundancies. Principal among these is that obtaining a visa authorizes only transport to a US port of entry, not necessarily entry. To come into the country, one must pass Immigration and Naturalization Service (INS) inspection. The INS inspector at a port of entry has the authority to deny an individual admission virtually irrespective of one's visa status. Although this authority is abused at times, it gives US authorities an additional opportunity to stop an inadmissible person on the basis of information that the INS may have in its own lookout database. Other, less frequently used but nonetheless important system checks and balances include the authority to revoke a visa after it is issued (hence enabling the INS inspector to deny someone's admission automatically) and to remove an individual after s/he has been admitted. (The latter is obviously much more complicated than the former.)

THE ASYLUM SYSTEM

The US government offers its protection to some people who have a well-founded fear of persecution in their home countries. People who find their way to the United States and seek refugee protection may apply for asylum at a port of entry or file an application with the INS within one year of their arrival. In fiscal year 2000, 49,462 asylum cases were filed or reopened. A case may represent more than one individual; in 1999 the average was 1.34 individuals per case. If the same formula is used for the year 2000, over 66,000 individuals sought asylum that year. Of the cases decided, 38 percent were approved in 1999 and 52 percent in 2000.

Asylum Procedures

The information sources available to asylum adjudicators when processing asylum claims include the individual asylum application, interviews, and a country-of-origin database. Country information is supplied by the Resource Information Center (RIC), which compiles information from a variety of sources, including but not limited to the UN High Commissioner for Refugees (UNCHR) and nongovernmental organizations. The RIC also responds to particular queries from asylum adjudication officials. Information supplied by the RIC does not necessarily coincide with US government opinion, nor does it reflect US foreign policy concerns.

In addition, asylum applicants may be screened through the FBI's Joint Terrorism Task Force, in which the INS and other federal law enforcement agencies participate. The Task Force has 18 offices in major cities around the world, with the aim of investigating and prosecuting terrorist organizations and their members.

During the asylum interviews themselves, applicants are asked many questions relating to present and past group affiliations and activities. The interviews rely not only on the honesty of the individual being interviewed but the skill and experience of the interviewer. The goal of the interview is to "verify the applicant's identity and determine basic biographical information." Questions addressed during the interview include:

- Nationality at birth and present nationality;
- Race, tribe, or ethnic group;
- Religion;
- Reason why the applicant is seeking asylum;
- What organizations or groups the applicant has been a member of or associated with;
- Whether or not the applicant has been threatened or mistreated by his government or by groups that the government is unwilling to control;
- Whether the applicant has ever been arrested, detained, or interrogated by any government agencies;
- In what other countries, if any, the applicant stayed before coming to the US;
- Whether the applicant has ever applied for or been granted refugee or asylee status in any other country;

- Whether the applicant has ever caused harm or mistreated others as a result of affiliation with a particular group or organization.

All asylum seekers are required as part of the asylum application process to submit fingerprint cards to the INS; additional fingerprints are taken at several stages of the process to continue to confirm identity. (The INS submits nearly 2 million fingerprint cards per year to the FBI to be checked against the Criminal Justice Information Services Division (CJIS) criminal history database in order to determine whether an applicant has a criminal history in the US.) One year after asylum is granted, an asylee may apply for permanent residence; if he does so, his files are checked with both the FBI and the CIA. If an asylee applies for citizenship when he becomes eligible, he undergoes an additional FBI check.

The US asylum system underwent major reforms in 1995 and 1996. Perhaps most importantly, substantial new resources were invested in staffing and training a dedicated Asylum Corps and providing its members with better information. Prior to the reforms, the back-log of asylum cases had reached 425,000 cases. Post-reform, about 80 percent of cases are decided within 60 days; prior to reform, asylum applicants often remained in the country for years awaiting a decision. Before 1996, applicants were allowed to apply for work authorization 30 days after filing for asylum; since then, application is only permitted if the case has not been adjudicated within 150 days—a measure intended to deter frivolous claims that are filed only to obtain permission to work.

Background checks on asylum seekers are more thorough than those on most other immigrants or visitors. Moreover, if asylum seekers are detected trying to enter the United States without proper documentation, they are routinely detained until their identity can be determined and they are judged unlikely to abscond, or their case is decided. Since the 1995-96 reforms, the number of people applying for asylum in the United States has declined dramatically, from 154,464 in 1995 to 49,462 in 2000. At the same time, asylum claim approvals increased, from 15 percent in 1993, to 38 percent in 1999. Many observers see in these figures evidence that reform of the asylum system has discouraged those without sound claims from using the asylum system to remain in the country.

LEARNING FROM OTHERS: THE EUROPEAN EXPERIENCE

The 15 European Union Member States have made efforts to develop data systems and to share immigration, asylum, and crime related information with one key point in mind: that the total territory of the 15 Member States is in the process of becoming a single territorial entity for the purposes of the movement of people (as well as capital and goods), while the Member States each maintain their distinct culture, governmental and institutional processes, and national interests.

The gradual development of common rules and regulations on immigration and asylum; establishment of shared databases; cooperation in tracing cross-border criminal activity; and arrangements for extradition are all advancing on paper. However, there is no common implementation of those rules. Immigration and asylum policies are still developed and implemented at the national level, albeit (in principle) in line with European Union-level guidelines. Their implementation will remain at the national level, because the principles of subsidiarity and proportionality (meaning that policies are developed and implemented at the most appropriate level for the subject matter involved) indicate that that is the most effective level for immigration and asylum controls and adjudications to be carried out. Police forces cooperate more and more, particularly on major criminal issues such as drug trafficking networks, and on issues that are seen as not only common but also mutual problems, such as football hooliganism. However, there is no European level police force of any sort.

EU Data-Sharing

1. Schengen Information System (SIS)

- The **SIS**, regarded as the cornerstone of Schengenland, is a computer database that can be accessed by all Member States with the aim of furthering police cooperation. It lists individuals who have been involved in cross-border crime, and stolen or missing goods. The UK and Ireland have also sought access to the SIS.
- Member States supply the system with information through national networks (N-SIS) which are connected to a central system (C-SIS) and supplemented by the SIRENE network (Supplementary Information Request at the National Entry), made up of representatives from the national and local police, customs, and the judiciary. The SIRENE contract was set to end on August 23, 2001, and due to be replaced by a new communication system called SISNET, which will become the European Information System and contain data on immigration also.
- The Schengen system provides for the collection of data related to immigration irregularities. However, since the entry into force of the **Dublin Convention** in September 1997, the Schengen system has formally had no role in the collection of data or movement of asylum seekers.

2. Visa Regime

- Both Schengen and the EU are involved in the European visa regime.
- Schengen put in place international instructions on the extension of a visa, which have been adopted by each state and thereby gained a national character. The countries involved have agreed to pursue a common visa policy, meaning they (theoretically at least) use the same conditions in assessing whether a visa should be issued or not, bearing each other's interests in mind during the procedures.
- Where a visa traditionally was necessary only for entry to the state which issued it, under the Schengen system, it has become essential for free movement among a number of states after entry via the borders of one of those states.
- The EU has drawn up a uniform visa, and a list of third countries whose nationals require a visa in order to enter the EU territory as a whole. Various sorts of visas can be given—for transit, onward travel, travel and temporary residence, and each of these for single or multiple entries.

3. Fingerprinting: Dublin/Eurodac

- The drafting of the **Dublin Convention** was completed in 1990 but the treaty did not enter into force until September 1997. The Convention determines which of the signatory states (all EU Member States) is responsible for assessing a given asylum claim. A study by the European Commission, published in June 2001, showed that transfers of individuals seeking asylum take place in only 0.4 percent of all cases. Claims are made in a significant number of cases, however, the Member States seem not to follow through on transfers even when another state has accepted responsibility. This lack of follow through might be due to the "friendship" between the states involved, but might also have financial and/or humanitarian motives.
- The **Eurodac** system, established December 11, 2000, aims to establish a centralized computerized database of the fingerprints of asylum applicants and certain other non-EU nationals collected by Member States and provide electronic transmission between the Member States and the central system. The system will theoretically allow states to establish the identity of asylum applicants and persons apprehended while illegally crossing borders into EU territory, so that each Member State has information about the individual's route and previous presence within national territory.
- The fingerprints of all asylum applicants above the age of 14 will be collected, as will that of all irregular entrants aged 14 or older, who are not turned back.
- Data collected in Eurodac will be stored for 10 years, but data relating to individuals admitted and recognized as refugees will be blocked by the Member State concerned. Data pertaining to individuals who gain citizenship in a Member State is also to be erased.

- While only Member States can carry out the input and blockage of data, the Central Unit, where the data are stored, is based in the European Commission.

4. Europol

- The establishment of Europol was agreed to in the Maastricht Treaty on European Union (1992). On January 3, 1994, it started limited operations focused on the fight against drugs, from its headquarters in the Hague (Netherlands). On July 1, 1999, the full activities of Europol commenced.
- The mandate of Europol is to support law enforcement activity regarding immigration networks; trafficking in human beings; and terrorism in situations in which an organized criminal structure and two or more Member States are involved.
- Europol carries out its mandate by:
 - Facilitating the exchange of information between Europol liaison officers (ELOs). ELOs are representatives of national law enforcement agencies, including police, customs, gendarmerie, and immigration services. Forty-four of Europol's 242 staff members are ELOs;
 - Providing operational analysis;
 - Generating strategic reports and crime analysis on the basis of intelligence from Member States, generated by Europol or gathered from other sources;
 - Providing technical support under the supervision of the Member State(s) concerned.
- Europol is developing a computerized system (The Europol Computer Systems) which will allow the input of, access to, and analysis of data. Strict human rights, data protection controls, supervision, and security measures are laid out in the Europol Convention. The analysis and index components of the system are in place, while the information system is under development and planned to be operational by 2002.

CIVIL LIBERTIES/DATA PROTECTION

In general in the EU, personal data may be processed only:

- If such processing is necessary for the performance of a task which is in the public interest and carried out on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis of that Treaty;
- Where the Community institution or other body to which data are disclosed is legitimately exercising its duties;
- When processing is necessary for compliance with a legal obligation;
- When processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- And if the data subject has unambiguously given his or her consent, or processing is necessary in order to protect the vital interests of the data subject.

Eurodac stipulates that there be:

- No unauthorized access to data;
- A guarantee that the name of the person who inputted the data, the place and date of input can all be traced;
- There is no transfer to third countries of the data collected in Eurodac;
- The individual has the right of access to, and right to rectify, data collected concerning them.

It is unlikely that states will effectively comply with Eurodac fingerprinting, because fingerprinting asylum seekers or irregular immigrants would mean that the individual concerned would become the state's responsibility, and be transferred back from the state in which their presence became known.

OTHER EU ARRANGEMENTS

Airline Liaison Officers

- Several European Union states employ airline liaison officers (ALOs) stationed at airports in cities from which a number of (irregular) migrants are expected to arrive. ALOs carry out pre-boarding checks of passengers and try to prevent irregular immigration to the EU before it happens, and particularly to target human trafficking and smuggling.
- The Member States cooperate in various ways, either by sharing officers, or rotating them on a regular basis.
- ALOs are recruited generally from the management levels of the Member States' respective immigration services.
- The number of such officers is increasing rapidly: the UK, for example, had five ALOs in 1998, and in May 1999 had 11 officers. The five already in place in 1998 were based in Ghana, Kenya, India, Sri Lanka, and Bangladesh, all operating out of the British High Commissions in these Commonwealth countries.
- Concerns have been raised about ALOs preventing people with valid asylum claims from boarding planes. Also, when children and women who are victims of trafficking are prevented from boarding aircraft, there are concerns that those people will be victimized again for the failure to carry out the emigration element in the process of exploitation.

Privatization of Security/Immigration Controls

- At European airports, passport controls on exit are usually carried out first by the airline at the check-in desk (often also on Schengen area flights) and secondly, and more formally, by immigration service officers at passport control desks. For inbound passengers, the controls are carried out by the airline, potentially by an Airline Liaison Officer, and when the country of departure has such a system, also by officials of that state.
- Passport controls by airline staff are seen by many as being an illegitimate privatization of security responsibilities, but are a logical response by private companies to the imposition of carrier sanctions. Under carrier sanction regulations, airlines and ferry companies in the EU Member States can be fined \$1,500 per passenger who is found to have arrived without the correct documentation aboard their vessel. In some cases, fines have been waived in return for cooperation in carrying out post-arrival but pre-entry checks for certain 'suspect' flights. (This has been the case with KLM in the Netherlands. KLM has also agreed to photocopy passports and visas prior to departure, the copies to be turned over to immigration authorities on arrival in the Netherlands for comparison with the documentation provided by the passenger, or to demonstrate that documentation was presented in cases where it is destroyed by the passenger en route.)

LESSONS FROM EUROPE

The process of removing internal frontiers has been the engine of progress in regional cooperation on asylum, immigration, and related data collection issues in Europe. Many of the measures are being gradually extended to prospective new Member States in Eastern and Central Europe.

The new measures in the European Union, including all those mentioned above, have frequently been criticized as violating human rights, discriminatory, and in particular, as inhibiting people from seeking asylum. The political rhetoric surrounding the measures has included the limitation of asylum seeker numbers as a major aim. However, the measures do not need to be preventive of the right to seek asylum if those elements that provide information and intelligence support are extracted from them and the focus is on criminal activity (seeking asylum is of course not a crime).

As the internal frontiers have been abolished in the EU, legally resident third country nationals are being granted rights to freedom of movement and security of residence in line with those of citizens of the EU Member States, although progress on this issue has been slower than many might wish. The EU has demonstrated that when states' over-riding interest in cooperation is in fact the pursuit of their national interest then cooperation is possible, but is also a laborious process of negotiation and mutual respect.

In the European context, the ability to compromise has sometimes meant bargaining across policy areas (e.g. one state accepts more refugees from a major crisis in return for an increase in subsidies to its farmers). Such cross-issue compromises may only be possible in a situation of regional integration, rather than one of mutual interest in a single issue area.

If the United States and its allies see collection of information and the sharing of data with other states as being in their respective national interests, then such collaboration may be possible. However, no single state will be able to set the rules. Compromise will be necessary, based, in part, on varying traditions relating to privacy rights, civil liberties, and non-discrimination.

In terms of the information available, greater cooperation on data sharing and intelligence issues between the EU and the US might be possible in certain instances. For example, such cooperation could probably only occur via a centralized system that authorized agents in the EU to receive information requests from the US. Such agents would follow up on the requests (in terms of taking any action against the individuals under investigation) pending any extradition proceedings or other appropriate measures. Due to data protection regulations, however, the EU is unlikely to pool information with US authorities, and especially unlikely to pool immigration information, at least under the existing regulations, which stipulate that there is no access for third states or any unauthorized parties.

One area in which greater cooperation could be sought is in the issuance of visas to individuals who are applying via their embassy within a given EU state (and vice versa). If the individual already has a visa or immigration/asylum status in a third country, part of the background checks might legitimately be to ask questions about any suspicious activities which have drawn the attention of law enforcement authorities. Questions must be raised about whether such background information can lead to exclusion without appeals, unless there is an existing criminal case and/or conviction. Unfortunately however, such sharing of basic background information will never ensure that the net is fully closed.

RECOMMENDATIONS

The horrific events of September 11 have shaken the confidence of many Americans in our immigration system, an institution that has served our nation well since its founding. The fact that the terrorists were foreigners has raised some legitimate questions about whether we are managing our borders and our immigration system effectively. Our government will be required to take steps to address and redress these concerns.

However, before policy choices are made among the many ideas now being discussed, we must understand the operation of the current immigration system. Only then can we make intelligent decisions about the areas of the system that need strengthening and will serve our long-term interests. This requires that deliberateness in our choices. We should opt for courses of action that increase our security appreciably and measurably while meeting criteria of practicality and effectiveness. We should also be mindful of another requirement: that the course we take does not alter in fundamental ways who we are—our commitment to freedom and individual rights that makes us unique among nations.

Visa security makes extraordinary demands on intelligence gathering, visa issuing, and border inspection agencies. This implies the need for the following: (a) better intelligence; (b) far greater coordination among intelligence-gathering agencies and the timely sharing of such information; (c) more and better use of technology; (d) on-going system integrity checks; (e) additional resources for personnel, technology, and related matters. Beyond this overarching imperative, some specific recommendations follow:

- **Technology** must be relied upon much more systematically and heavily than is now the case. Two areas of investment in technology require immediate attention. The first is decidedly “low-tech” in that it can be implemented with existing technology. It involves enabling INS inspectors at every port of entry to “read” a passport picture electronically and check it against the “lookout list” database—which should include pictures of those of particular concern to the government. The second requires reliance on more advanced technology. Specifically, digitalized three-dimensional facial recognition technology can be used to identify visa applicants who may be on a “lookout list” and/or those who might switch identities after a visa has been issued and attempt to enter the US at a port of entry.
- A concerted effort toward issuing only **machine-readable passports** will go a long way toward minimizing passport falsification and fraud. Governments currently on the US visa-waiver program are required to issue machine-readable passports by October 1, 2007.
- The INS and the Visa Office should explore development of a **shared database** for all decisions regarding visa applicants and petitioners for an immigration benefit. At a minimum, this will be an important efficiency measure; perhaps more importantly, it may allow either agency to detect fraud and other unusual or suspicious patterns that may be useful in the fight against terrorism. This database should be closely coordinated with those of the FBI and CIA, as appropriate. The efficiencies and possible security gains from such an initiative, however, must be measured against the immensity of the task and the potential civil liberties implications of matching of databases. Not the least of these concerns is that the INS database also includes extensive information on petitioners, who are overwhelmingly U.S. citizens and U.S. entities (in the case of employer petitions).
- Considering the need for much better information about who comes into and who leaves (or does not leave) our country, we recommend exploratory funding for a pilot program of **enhanced recording of entries and exits at airports** for all travelers who are neither US citizens nor legal permanent residents of the United States. We also recommend proceeding, if cautiously, with the next stage in the gradual implementation of the student and exchange visitor information system (SEVIS) that is now in the

“operational prototype” stage. **In both instances, however, we also recommend that the INS show how the availability of more robust data systems in these areas, and the costs associated with their full implementation, will enhance in measurable ways the security interests of the United States without damaging privacy and other civil liberties priorities.**

- The 1995 reforms of the asylum system give some indication of the kind of reform that might be considered for visa processing: a specialized and well-trained staff along the lines of the Asylum Corps; additional resources; and enhanced and more timely access to information. Currently, visa processing is assigned to the most junior foreign service personnel. There is little opportunity to build a cadre of knowledgeable and experienced officers skilled in the job of screening for security threats.
- Work closely with foreign governments to enhance the **security of the passport issuance** process. As a general rule, so-called feeder-document fraud is less of a problem in most countries than it is in the US, because of national registration requirements and generally much tighter internal controls. Many of the states of particular concern to us at this time are in fact among those that control their citizens—and foreign entrants—most tightly.
 - The US must enlist the active cooperation of Mexico and Canada in a coordinated effort against terrorists and other undesirable elements and practices. This effort must begin by rethinking how each party conducts its business in areas that may affect adversely the security (and economic) interests of its North American partners.
 - The three NAFTA partners must begin to explore systematically the concept of **perimeter “defense.”** Accordingly, each country must begin to evaluate how its various systems, and their delivery, can protect the North American space from security challenges from outside the NAFTA space while facilitating further the intra-NAFTA movement of goods and persons. Additional reliance on available technology will allow all three countries to make gains in both policy fronts.
 - Formal and informal cooperation between the US and Mexico should begin to emulate the models developed between the US and Canada. **Cooperation between Canada and the US, in turn, should become organic.** Specifically, the US and Canada should start discussions about “harmonizing” (rather than “standardizing”) their visa regimes and otherwise becoming more sensitive to one another’s security concerns when issuing visas. Over time, a better understanding of and even coordination of asylum policies should also be put on the table. Finally, discussions should start in earnest about sharing look-out lists, developing joint inspection regimes and facilities, and cross-training of intelligence and other enforcement personnel.
 - As part of a gradual and careful exploration of risk-management approaches to border controls, the three NAFTA governments should encourage frequent travelers to sign up for **pre-clearance programs** (known as INSPASS at airports and CANPASS or dedicated commuter lanes at land borders). Such programs allow the government to focus resources on unknown travelers while facilitating travel for those willing to provide advance information, submit to background checks, and pay a small fee in exchange for ease of travel.

TABLE 1

Nonimmigrants Admitted Under the Visa Waiver Pilot Program by Country of Citizenship: Fiscal Years 1998¹

	Number of Entries	
	For Pleasure	For Business
All countries	14,372,792	2,145,967
Latin America		
Argentina	329,470	23,770
Uruguay	3,607	195
Asia and the Pacific		
Japan	4,433,751	306,346
Singapore	3,931	1,705
New Zealand	128,791	22,565
Australia	360,454	90,704
Brunei	506	160
Europe		
Andorra	624	62
Austria	167,477	28,358
Belgium	172,229	51,732
Denmark	106,107	36,078
Finland	60,946	27,962
France	939,018	202,316
Germany	1,675,984	296,205
Iceland	20,902	3,111
Ireland	258,104	34,521
Italy	608,704	114,445
Liechtenstein	1,228	166
Luxembourg	11,404	1,413
Monaco	636	35
The Netherlands	456,855	123,068
Norway	104,288	30,822
Portugal	6,468	650
San Marino	470	52
Slovenia	11,924	3,014
Spain	323,211	48,366
Sweden	222,171	78,178
Switzerland	270,416	43,308
United Kingdom	3,522,797	565,253

North America

Canada - Businesspeople and vacationers do not require visas for stays of up to 90 days.

Mexico - With border crossing cards, Mexicans are limited to staying no more than 72 hours in the 5 border states with Mexico.

¹ Source: 1999 Statistical Yearbook of the Immigration and Naturalization Service.

TABLE 2**Visa Issuance:
Fiscal Year 1998****Total number of immigrant visas issued in consulates abroad: 376,701**

Of that, the total numbers issued by region are as follows:

- Asia (including the Middle East): 152,801
- North America: 120,000
- Europe: 49,478

Total number of nonimmigrant entries: 30.1 million

Major categories include:

- Tourists and businesspeople (28,696,911 admissions)
- Temporary workers
- Students, vocational students, and students' families (567,146 admissions)

By Region: Immigrant and Non-Immigrant Visas**Asia:**

- Non-immigrant visas: 2,047,626 (75,000 of these were from India, mainland China, or the Philippines)
- Immigrant visas: 152, 801

Middle East:

- Fewer than 20,000 total (1,072 from Iraq, 617 from Afghanistan, 211 from the UAE, and 168 from Saudi Arabia)

TABLE 3**Preliminary 2000 Visa Information from the Visa Office**

All Classes	7,141,636
Temporary Visitors	3,567,578
For business (B1)	75,919
For pleasure (B2)	509,031
Border crossings (mainly from Mexico)	1,510,135
Students	
Academic students (F1)	308,944
Vocational students (M1)	6,465
Temporary workers and trainees (H)	289,959
Exchange visitors (J)	273,959

TABLE 4

US Asylum Statistics, 1994-present

Year	Cases Filed	Cases Approved
1994	146,468	8,131
1995	154,464	12,454
1996	128,190	13,532
1997	91,381	10,509
1998	57,786	10,364
1999	42,530	13,510
2000	49,462	16,810
2001 (to date)	54,992	17,315

TABLE 5
Nonimmigrant (Temporary) Entries
 Non-immigrants Admitted by Selected Class of Admission: 1999

A - Foreign government officials ¹	133,005
B1 - Temporary visitors for business ²	4,592,540
B2 - Temporary visitors for pleasure ²	24,104,371
C, D - Transit aliens ⁴	385,788
E - Treaty traders and investors ³	151,353
F1 - Students	667,146
F2 - Spouses and children of students	36,641
G - International representatives ³	91,829
H1, H2, H3 - Temporary workers and trainees	457,346
H4 - Spouses and children of temporary workers and trainees ⁵	109,681
I - Representatives of foreign information media ³	31,917
J1 - Exchange visitors	275,519
J2 - Spouses and children of exchange visitors	43,841
K1 - Fiances(ees) of U.S. citizens ⁷	18,208
L1 - Intra-company transferees	234,443
L2 - Spouses and children of intra-company transferees	111,891
NATO - NATO officials ³	12,992
O1 - Workers with extraordinary ability or achievement	15,946
O2 - Workers accompanying and assisting in performance of O1 workers	3,248
P1 - Internationally recognized artists and entertainers	36,228
P2 - Artists or entertainers in reciprocal exchange programs	3,772
P3 - Artists or entertainers in culturally unique programs	8,471
Q1 - Workers in international cultural exchange programs	2,485
R1 - Workers in religious occupations	12,687
TN - North American Free-Trade Agreement workers ³	87,441
All Classes ^{1,2}	31,446,054

Source: 1999 Statistical Yearbook of the Immigration and Naturalization Service, Tables 36 & 37.

¹ Excludes the following classes of admission processed in the Nonimmigrant Information System: for all countries - 133,504 parolees; 17,653 withdrawals and stowaways; and 66,966 refugees.

² Includes admissions under the Visa Waiver Pilot program.

³ Includes spouses and unmarried minor (or dependent) children.

⁴ Includes foreign government officials and their spouses and unmarried (or dependent) children in transit.

⁵ Includes workers (and their spouses and children) under the North American Free-Trade Agreement (shown separately).

⁶ Includes People's Republic of China and Taiwan. A total of 699,234 nonimmigrant visas were issued to these two countries in fiscal year 1996: 379,355 to Taiwan and 229,879 to People's Republic of China (SOURCE: U.S. Department of State, Bureau of Consular Affairs, Visa Office.)



U.S. Department of Justice
Immigration and Naturalization Service

CO 703.785

Office of the Commissioner

425 I Street NW
Washington, DC 20536

RECEIVED

NOV 30 2001

Immigration and Claims

The Honorable George W. Gekas
Chairman, Subcommittee on Immigration
and Claims
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

NOV 21 2001

Dear Mr. Chairman:

I respectfully request permission to clarify information provided at the October 11, 2001, hearing of the House Judiciary Subcommittee on Immigration and Claims regarding "The Use of Information Technology to Secure America's Borders". As you know, at that hearing I testified and provided a written statement on several immigration-related technology issues. In both my oral and written testimonies, I wish to clarify the implementation dates for the Student and Exchange Visitor Information System (SEVIS). I hope that the clarifications provided herein will ensure that you have the most accurate information on which to base any legislative actions.

I. Testimony Transcript:

In my October 11, 2001 oral testimony, I indicated in my opening statement that with appropriated funds, the Immigration and Naturalization Service (INS) could deliver SEVIS a year in advance of the statutory deadline of December 20, 2003 - i.e., by December 20, 2002. Please correct that statement to reflect that with appropriated funds, INS would be able to deliver the primary system six months in advance of the actual statutory deadline of January 1, 2003 - i.e., by July 1, 2002. In addition, although the primary SEVIS system will be developed by January 1, 2003 - or sooner, with appropriated funds (including additional functionality for batch processing and interface capabilities developed by December 2003) - the system will not be fully in use by all institutions until (1) final regulations are in effect to establish which data are to be collected and the frequency of reports, (2) INS reviews and certifies schools that are currently permitted to accept foreign students, and (3) INS enrolls and trains approved schools and exchange visitor programs to use the automated system.

After the testimony of Inspector General Glenn Fine, you asked why the INS missed the 1998 statutory deadline by which it was to designate the five countries whose students INS would track. I responded that I did not know the answer but would follow up with a reply. My staff has advised me that during the 1997-99 school years, INS conducted a pilot for a limited

The Honorable George W. Gekas
Page 2

number of institutions to track nonimmigrant students from all countries. Since this pilot included many more than five countries, INS believed that it was in compliance and in fact had exceeded the statutory requirements.

II. Written Statement:

In my written statement presented for the hearing record, a correction is necessary for one of the dates referenced. Under the "Database Improvements" section [page 7 of my copy] the statutory due date for commencing implementation of SEVIS needs to be corrected from December 20, 2003 to January 01, 2003.

I apologize for any inconvenience this clarification may cause. Please be assured that the INS is committed to working with Congress to develop capabilities that will enhance our ability to monitor and track international students and exchange visitors in the United States. I would be pleased to meet with you to discuss further the continuing developments in the implementation of SEVIS.

Sincerely,



James W. Ziglar
Commissioner



U.S. Department of Justice
Immigration and Naturalization Service

CO 703.785

Office of the Commissioner 425 I Street NW
Washington, DC 20536

The Honorable George W. Gekas
Chairman, Subcommittee on Immigration
and Claims
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

RECEIVED
NOV 30 2001
NOV 21 2001
Immigration and Claims

Dear Mr. Chairman:

On October 11, 2001, in response to your request, I sent you a letter with information regarding the manner of entry and the legal status of the 19 suspected hijackers involved in the attacks on the World Trade Center and the Pentagon. The information was based on a search of the Immigration and Naturalization Service (INS) records systems, using data provided the INS by the Federal Bureau of Investigation (FBI) as a result of its continuous investigation.

Since then, I have received additional identifying information regarding the suspected hijackers from both the FBI and the Department of State. This information adds to the body of information gathered as this investigation has evolved and is based in part on photographic identification. Based on this material, we have developed the enclosed list confirming the admission data of all the suspected hijackers. In the case of two of the suspected hijackers, Ahmed Alghamdi and Waleed Alshehri, my previous report that they were in illegal status was based on erroneous dates of birth. With the assistance of the photographic confirmation, we have been able to search under a new date of birth and locate files relating to those individuals. We have confirmed these matches by cross-referencing them with information provided by the Department of State Consular offices.

We will continue to keep you apprised of any further developments concerning the immigration status of the 19 suspected hijackers. Please do not hesitate to contact me with any questions regarding this or any other immigration-related matter.

Sincerely,

James W. Ziglar
Commissioner

Enclosure

AMERICAN AIRLINES FLIGHT 11		
NAME	ARRIVAL	VISA
Alomari, Abdula	June, 2001	B-2
Alshehri, Wail M.	June, 2001	B-2
Alshehri, Waleed M.	May, 2001	B-2
Al Suqami, Salam M.A.	May, 2001	B-1 Overstay
Atta, Mohammed Mohamed	July, 2001	B-1 *
AMERICAN AIRLINES FLIGHT 77		
NAME	ARRIVAL	VISA
Alhazmi, Nawaf M.S.	January, 2000	B-2 Overstay
Al Hazmi, Salem M.	June, 2001	B-2
Al Mihdhar, Khalid M.A.	July, 2001	B-1
Hanjour, Hani S.H.	December, 2000	F-1 Overstay
Moqed, Majed M. GH.	May, 2001	B-2
UNITED AIRLINES FLIGHT 93		
NAME	ARRIVAL	VISA
Alghamdi, Saeed A. A.	June, 2001	B-2
Al-Haznawi, Ahmed Ibrahim A.	June, 2001	B-2
Alnami, Ahmed A. A.	May, 2001	B-2
Jarrah, Ziad Samir	August, 2001	B-2
UNITED AIRLINES FLIGHT 175		
NAME	ARRIVAL	VISA
Alghamdi, Ahmed Saleh S.	May, 2001	B-2
Alghamdi, Hazma S. A.	May, 2001	B-2
Alshehri, Mohand M. F.	May, 2001	B-2
Alshehhi, Marwan Yousef Mohamed R. Lekrab	May, 2001	B-2
Banihammad, Fayez Rashid Ahmed	June, 2001	B-2

Information as of 11/20/2001

* In addition, Mr. Atta had filed an application to change status to M-1, which was granted on 7/17/01. However, on 7/19/01 Mr. Atta sought admission and was admitted to the United States based on his then current B-1 visitor visa.