IMPLEMENTING THE 9/11 ACT MANDATES FOR ENHANCING THE VISA WAIVER PROGRAM

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JULY 16, 2008

Serial No. 110–127

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

45–173 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

I. LANIER LAVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

LORETTA SANCHEZ, California, *Chairwoman*

JANE HARMAN, California
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
AL GREEN, Texas
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MARK E. SOUDER, Indiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
MIKE ROGERS, Alabama
PETER T. KING, NEW YORK *(Ex Officio)*

ALISON ROSSO, *Director*
DENISE KREPP, *Counsel*
CARLA ZAMUDIO-DOLAN, *Clerk*
MANDY BOWERS, *Minority Senior Professional Staff Member*

CONTENTS

Page

STATEMENTS

The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Chairwoman, Subcommittee on Border, Maritime, and Global Counterterrorism 1
The Honorable Mark E. Souder, a Representative in Congress From the State of Indiana, and Ranking Member, Subcommittee on Border, Maritime, and Global Counterterrorism 2

WITNESSES

PANEL I

Dr. Richard C. Barth, Ph.D., Assistant Secretary, Office of Policy Development, Department of Homeland Security:
Oral Statement 4
Prepared Statement 6
Mr. Robert A. Mocny, Director, US–VISIT Program, Department of Homeland Security:
Oral Statement 9
Prepared Statement 6
Mr. Stephen A. "Tony" Edson, Deputy Assistant Secretary for Visa Services, Bureau of Consular Affairs, Department of State:
Oral Statement 11
Prepared Statement 12

PANEL II

Mr. Douglas E. Lavin, Regional Vice President for North America, International Air Transport Association:
Oral Statement 24
Prepared Statement 26
Mr. Greg Principato, President, Airports Council International—North America:
Oral Statement 32
Prepared Statement 33
Mr. Nathan A. Sales, Assistant Professor of Law, George Mason University School of Law:
Oral Statement 36
Prepared Statement 38

APPENDIX

Questions From Chairwoman Loretta Sanchez 49

IMPLEMENTING THE 9/11 ACT MANDATES FOR ENHANCING THE VISA WAIVER PROGRAM

Wednesday, July 16, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to call, at 10:08 a.m., in Room 311, Cannon House Office Building, Hon. Loretta Sanchez [Chairwoman of the subcommittee] presiding.

Present: Representatives Sanchez, Harman, Langevin, Cuellar, and Souder.

Ms. SANCHEZ. The Subcommittee on Border, Maritime and Global Counterterrorism will come to order.

The subcommittee is meeting today to receive testimony on implementing the 9/11 Act mandates for enhancing the Visa Waiver Program. Welcome to today's hearing.

Our first panel today consists of State and Homeland Security officials familiar with the US–VISIT and Visa Waiver Program. I am anxious to hear their testimony in regards to the implementation of the 9/11 Commission Act with regards to the Visa Waiver Program.

Our second panel includes members of airport and air transport associations that are affected by the implementation of the Visa Waiver Program. I am equally anxious to hear their testimony in regards to the changes to the Visa Waiver Program, and particularly the implementation of the US–VISIT Exit piece.

The goal of this hearing will be to examine the US–VISIT Exit proposal and the Electronic System for Travel Authorization implementation. We will also look at the demands both of these programs will place on the two Departments implementing them and the effects on the airlines and the ports of entry that will need to adhere to them.

Because of the possibility of potential terrorists entering the United States through a visa waiver country, this committee has required several new security measures through the 9/11 Commission Act. US–VISIT Exit is also an essential tool to identify visa overstays and to ensure that visitors who enter the country actually leave, by obtaining their biographic and biometric data upon departure.

However, recent GAO reports have shown that the Department of Homeland Security's US–VISIT pilot program had a low compliance rate, was poorly planned, and had inadequate evaluations by senior officials.

Last April, DHS issued a notice for proposed rulemaking that would require the airline industry to be in charge of collecting and maintaining travelers' sensitive biometric information. Chairman Thompson and I have fully opposed this rulemaking, as we believe that it not only imposes an additional burden on an already-stressed industry, but that it will also cost the industry over $12 billion to implement the program and to train their employees.

Last month, Chairman Thompson and I submitted written comments addressing four key concerns about the proposed rulemaking.

First, collecting biometric data on travelers leaving and entering this country, I believe, is inherently a governmental responsibility. CBP collects the information for incoming travelers, so there is really no reason to hand off that responsibility to the airline industry.

Second, this proposed rule offers no training for the 80 to 138 airlines that will be affected by this rule. So penalizing these airlines for not adequately transmitting that biometric data I think would be highly inappropriate.

Third, the proposed rule asks for airlines to collect and store fingerprints and digital images. DHS is asking the airline industry to store and to transmit information that requires very high privacy safeguards.

Fourth, the Department of Homeland Security should consider a combination of alternatives that adequately meets every performance standard, such as the alternative proposed by Mr. Thompson and me. That would require the Department of Homeland Security, through the use of a kiosk, to collect travelers' biometrics at the TSA checkpoint and verify their departure with the airlines.

Although the US–VISIT Exit notice of proposed rulemaking is a major concern, it is not the only concern that we have in this subcommittee. The implementation of the Electronic System for Travel Authorization also must be looked over carefully. We must ensure that that program is introduced to the public through an intensive outreach program. This should be done in conjunction with the development of contingency plans in case the ESTA does not meet performance standards. We must also ensure that the Government does not duck its responsibilities with respect to these programs by placing the burden on private citizens or on private industry.

So I look forward to hearing from our witnesses today, and now will yield to my Ranking Member, Mr. Souder, for his opening statement. Thank you.

Mr. SOUDER. Thank you, Madam Chairwoman. I appreciate your leadership of this committee and for holding this important hearing.

One of the most important charges that the Committee on Homeland Security has is to ensure that the Department of Homeland Security has the tools, resources and authority to continually address new terrorist travel threats.

The two programs that we are discussing in today's hearing promise to add important security layers, once fully implemented. The United States' national security depends on a robust system of screening and tracking foreign visitors. The establishment and implementation of the US–VISIT biometric screening program is a cornerstone of border security and border management.

The Data Management Improvement Act of 2000 first set specific deadlines for the implementation of an entry and exit system at all air, land and sea ports of entry. According to this law, the entire system was to be complete by the end of 2005. After 9/11, additional legislation was passed to require the system to include biometrics.

I applaud the Department for completing the entry portion of the requirement according to the mandated deadlines. Albeit significantly past the deadline, I am encouraged that progress is being made on the air and sea exit programs.

I am sure that the notice of proposed rulemaking issued in April will be one of the major discussion points during this hearing, and I have a number of questions on the methodology DHS used to select the proposal for the carriers to collect and transmit exit data, as well as the kiosk alternative.

Unfortunately, similar progress has not been achieved implementing land exit. I have been extremely disappointed that very little effort has been dedicated to an exit solution, and there appears to be a lack of will within the Department to address this security vulnerability. I hope that DHS witnesses will be able to provide an update on the land exit solution.

In fact, one of the most discouraging things to me is that 9/11 occurred in 2001; we are now to 2008; airports should be the easiest to implement, as opposed to all the water entries and all the land entries. There are finite numbers. Yet here we are still battling on how to do it at the airports.

I am also concerned that the spending bills moving through both the House and Senate contain language that could significantly delay the US–VISIT Exit solution. I am interested in hearing from the witnesses about the impact the required pilots in the House bill and the reduction in funds in the Senate bill could have on the program. I believe that with the absence of a DHS authorization bill, this committee has little opportunity to legislatively address problems and policies within the Department and is abdicating our responsibility to the appropriators.

The other program on the table for today's hearing is the Visa Waiver Program. Approximately 15 million travelers come to the United States each year under the Visa Waiver Program. Under the VWP expansion authority included in H.R. 1, that number would increase by 6 million. None of these travelers need apply for a visa at a U.S. consulate prior to coming to the United States.

To address the diplomatic pressure to expand VWP and add important new security measures to the program, the administration requested language that was included in H.R. 1 to waive the strict requirements that nations must meet before they are eligible for VWP participation.

There are several criteria in the legislation that must be met before the Secretary can use the waiver authority, which promised to

add important security measures to that program. This includes a new requirement that VWP travelers use a new electronic system of travel authorization. This will allow DHS to vet passengers coming into the United States under the VWP several days in advance. Additionally, the legislation requires new VWP nations to share lost and stolen passport data with Interpol and increase security cooperation with the United States.

I look forward to hearing from the witnesses about the program's progress in implementing these additional security measures.

Thank you, Madam Chair, for calling this hearing, and I join you in welcoming the witnesses on both panels, and yield back.

Ms. SANCHEZ. I thank my Ranking Member.

I will remind the rest of the Members on the subcommittee that, under committee rules, opening statements may be submitted for the record.

I now welcome our first panel of witnesses.

Our first witness, Dr. Richard Barth, was appointed Assistant Secretary for the Office of Policy Development in the Department of Homeland Security on August 28, 2006. He is the principal action officer for coordinating policy among Department entities, State and Federal agencies, and foreign governments.

Our second witness is Robert Mocny, director of the US–VISIT program. He has served in several senior Federal Government positions related to U.S. immigration policy and operations, including director of the Entry/Exit Project and Acting Assistant Commissioner and Assistant Chief Inspector with the former Immigration and Naturalization Service.

Welcome.

Our final witness is Steven Edson, Deputy Assistant Secretary for Visa Services in the State Department's Bureau of Consular Affairs. Mr. Edson served as managing director of visa services and senior advisor for strategic planning to the Visa Services Directorate from 2001 until 2005. Mr. Edson entered the Foreign Service in 1981.

So, welcome.

Without objection, your full statements will be inserted into the record. I will now ask each of you to please summarize your statement in 5 minutes or less.

Let's begin with Assistant Secretary Barth.

STATEMENT OF RICHARD C. BARTH, PH.D., ASSISTANT SECRETARY, OFFICE OF POLICY DEVELOPMENT, DEPARTMENT OF HOMELAND SECURITY

Mr. BARTH. Thank you. Chairwoman Sanchez and Representative Souder and distinguished Members of the committee, I would like to thank you for the opportunity to appear today to discuss how the Department of Homeland Security is implementing the 9/11 Commission Act, signed into law last August.

A modernized Visa Waiver Program that strengthens our country's national security, law enforcement and immigration interests is a top priority for this administration. We are enhancing security for the United States and our VWP partners in many ways that I will address today, while also enabling the entry into the program

of new member nations. I would note that these goals are mutually reinforcing.

The first point I would make is to thank you and other Members of Congress who joined forces to pass a VWP Modernization Act that enhances our security and gives the President flexibility in admitting new members. The Congress also is to be commended for providing adequate funding for a significant new security tool, the Electronic System for Travel Authorization, or ESTA.

The next point I would like to make is that we are on track to improve security and welcome new members into the VWP this year. Despite the claims that assert the opposite, DHS will facilitate travel for key allies, and they are excited about the partnership that has led to this likely outcome this year.

I would like to spend a few minutes reviewing the complexities of the VWP program and the way DHS and its partner agencies, including the DNI, the State Department, and Justice Departments primarily, are dealing with these complexities. Then I will focus a little on where we are with the nine countries with whom we have had an active dialogue to enter the VWP program, possibly, as I said, as early as the end of this year.

The chart on the screen above you there shows the many steps that are required to achieve VWP status for the aspirant countries and, also, what has to be done with current VWP countries to ensure that we are managing a single VWP program with all the security enhancements called for in the new law.

This chart basically starts on the left, with the passage of the new law by Congress last August, and then the funding of the ESTA at the end of December. The color code on the upper-right corner highlights whether these steps in the flow chart relate to new members or to all VWP members. A couple key steps I will point out.

One important one is that the DNI, the Intelligence Community, needs to report to us on the threat posed by new entrants particularly. To date, we have these reports on three countries and are on track to complete all the DNI reports this year.

Comprehensive reviews of the security of the aspirant countries is also a critical factor. That is largely spelled out in the chart. As you can see, we have completed eight out of the nine reviews. Our very extensive reports on border security in those countries are being finalized and, again, are on target for delivery this year.

Data-sharing on key aspects of CWP travelers is critical to this program. We are in active discussions with all nine countries on data-sharing agreements for known and suspected terrorists; criminal information, up to and including that which would be a felony here in the United States; and date on asylum rejections and asylum applicants.

ESTA, of course, is another core requirement that is on track for implementation on August 1 of this year and with full-capability rollout in October of this year. We intend to require ESTA approvals for all VWP travelers as of January 12, 2009. Let me emphasize: All VWP travelers. That includes travelers from France, Germany, the United Kingdom and Japan, as well as all the other VWP travelers from existing VWP members.

ESTA is essential to transforming the VWP program from evaluating security threats on a country-by-country basis to a capability that allows us to make traveler-by-traveler judgments. In addition to enhancing security, ESTA will provide for greater efficiencies in the screening of international travelers, and reduce traveler delays at the ports of entry.

As discussed in other hearings, we are also on track to be able to certify that there is matching biographic data on those who exit the country. This is a particularly complicated topic, but we commit to the Congress to share very transparently the way that we calculate the data that allow the Secretary of DHS to certify that this requirement in the statute has been met before admitting new member countries to VWP.

Allow me to mention some of the security enhancements that we are already benefitting from as a result of the effective implementation of this law.

First, we are concluding agreements with foreign governments to share data on known and suspected terrorists. Those data elements from some countries are already being used in our screening databases. That would not be the case if we hadn't had the new tools enabled by the legislation.

Second, we are already receiving significantly improved data from a number of countries on lost and stolen passports, even in advance of them coming into the VWP program. They have been sharing data on lost and stolen passports with us, whether issued or blank passports. These data are accessible to our Customs officers in real time to ensure that people who would do us harm cannot come into the country using a false identity or traveling under their own identity but on falsified documents.

Next, collaboration in the air marshal programs and airport security is also increasing due to the effective implementation of this law. There is a steady increase in our security, which directly relates to the passage of this legislation. We are committed by the end of the year to strengthening the VWP program in a substantive way, admitting new qualified members into the program, and meeting the security enhancements of the law.

As we have outlined, the Department is well on its way to achieving this, and we look forward to answering any questions you will ask today.

Thank you, Chairwoman.

[The joint statement of Mr. Barth and Mr. Mocny follows:]

PREPARED STATEMENT OF RICHARD C. BARTH AND ROBERT A. MOCNY

JULY 16, 2008

Chairwoman Sanchez, Representative Souder and distinguished Members of the subcommittee: We would like to thank you for the opportunity to appear today to discuss how the Department of Homeland Security (DHS or the Department) is implementing the provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110–53 (9/11 Act). A modernized Visa Waiver Program (VWP) that strengthens our country's national security, law enforcement, and immigration interests is a top priority for the administration. Section 711 of the 9/11 Act supports this objective by concurrently enhancing the VWP's security requirements and expanding opportunities for countries to become VWP members. Similarly, the 9/11 Act mandates the establishment of a biometric exit system to complement the entry system already in place. Our ability to measure and track those who overstay

their lawful periods of admission is necessary for immigration enforcement, and is a valuable homeland security tool as well.

Enhancing the VWP's security requirements and expanding membership opportunities are mutually reinforcing goals. As a result, both current and prospective VWP members will continue to contribute to a secure environment for international travel as well as deepen their cooperation with the United States on security-related issues.

As you know, the Department has formalized a number of security enhancements, including those mandated by the 9/11 Act, into memoranda of understanding (MOUs) and—in collaboration with our colleagues from the Departments of State and Justice—is actively discussing implementing arrangements and agreements that detail the terms of the new security measures. DHS is requiring each member and aspirant country to sign an MOU and to agree to the appropriate implementing arrangements or agreements, unless other arrangements or agreements already in place fulfill the new security requirements of the VWP legislation.[1]

We believe that the bilateral arrangements and agreements under discussion—which include requirements to provide certain information on air passengers, serious crimes, known or suspected terrorists, asylum and migration matters, and timely reporting of lost and stolen passport data, as well as cooperation on airport and aviation security—will provide our operators and analysts with new tools to secure our Nation as well as help prevent terrorist and criminal activities in our VWP partner nations. In fact, we are seeing tangible security benefits well in advance of adding new members to the VWP. As a result, the Department can more effectively screen arriving passengers to detect, apprehend, and limit the movement of terrorists, criminals, and other mala fide travellers.

The Department has also taken the appropriate steps to ensure that VWP expansion will not negatively impact U.S. security, law enforcement, or immigration interests. Over the past 4 months, DHS-led interagency teams have traveled to the Czech Republic, Estonia, Greece, Hungary, Slovakia, Latvia, Lithuania, and South Korea to comprehensively review their counterterrorism capabilities; immigration, citizenship and naturalization laws; passport production and issuance controls; efforts to combat crime; law enforcement cooperation with the United States; and border control mechanisms.[2] A country cannot be admitted into the VWP until it is designated for admission by DHS, in consultation with the Secretary of State. DHS has also commissioned the required independent Director of National Intelligence (DNI) assessment of these countries to inform the designation process.

As noted earlier in this testimony, the goals of security and expansion are complementary. The 9/11 Act gives the Secretary greater flexibility with regard to the level of the aspirant countries' nonimmigrant visa refusal rate, provided that the Department: (1) Certifies that an air exit system is in place that can verify the departure of not less than 97 percent of the foreign nationals who exit through U.S. airports; and, (2) certifies that an Electronic System for Travel Authorization (ESTA) is fully operational.

As to the first requirement, DHS continues to evaluate and consider various methodologies to verify the departure of at least 97 percent of foreign nationals who exit through U.S. airports. DHS will continue to review these options to ensure the accurate and timely receipt of passenger manifest information and to improve the methodology underpinning air exit calculations. DHS expects to make this certification later this year.

The development of the ESTA program is also well underway. The ESTA program will strengthen substantially the security of the VWP by providing DHS with the capability to conduct enhanced advance vetting of VWP travelers. Under the ESTA, VWP travelers will be required to submit electronically biographic and other information as required by the I–94W Nonimmigrant Alien Arrival/Departure Form to DHS prior to their departure for the United States. ESTA applications will then be queried against appropriate databases, enabling DHS to make a determination on each individual's eligibility to travel to the United States under the VWP. Travelers denied a travel authorization via ESTA will be referred to the appropriate U.S. embassy or consulate to apply for a visa.

In support of ESTA, DHS is developing a Web-based application and screening mechanism for direct access by VWP travelers. The system is designed for future

[1] To date, eight countries have signed MOUs—the Czech Republic, Estonia, Hungary, the Republic of Korea, Latvia, Lithuania, Malta, and Slovakia. Talks are also underway with several current VWP members on compliance with the new requirements.

[2] Although DHS is actively engaged with each of the roadmap countries, Greece is the only VWP-candidate country that has been formally nominated for designation by the Department of State.

volume increases and for peak periods of travel. DHS published an Interim Final Rule on June 9, 2008, following a June 3, 2008, announcement by Secretary Chertoff outlining the new system. DHS intends for ESTA to go on-line on August 1, 2008, in English only and with limited capacity. This fall, DHS anticipates that ESTA will have full capacity and will be available in multiple languages. On January 12, 2009, DHS anticipates that all VWP travelers will be required to have a travel authorization via ESTA to travel to the United States under the VWP. With support from the Departments of State and Commerce, as well as from the travel and tourism industries, DHS has initiated an extensive public outreach campaign to promote ESTA awareness among VWP travelers.

ESTA is essential to transforming the VWP from one that evaluates security threats on a country-by-country basis to one that is capable of making traveler-by-traveler judgments. In addition to enhancing security, ESTA will provide for greater efficiencies in the screening of international travelers by reducing traveler delays at the ports of entry.

Equally critical to DHS efforts to promote secure and legitimate travel is the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) Program. The establishment of US–VISIT and the creation of an integrated immigration and border screening system represent major achievements, not only in efforts to reform the Nation's immigration and border management system, but also in the enhancement of our Nation's security. Through its use of biometrics, the US–VISIT Program collects, stores, and shares digital fingerscans and photographs for subsequent verification. This biometric information is paired with biographics pertaining to a particular individual to verify that person's identity.

US–VISIT's Automated Biometric Identification System (IDENT) plays an important role in biometric screening and verifying the identity of non-U.S. citizens for other Federal agencies. For example, US–VISIT directly supports the DOS' BioVisa program and shares information with the Federal Bureau of Investigation (FBI) on expedited removals.

US–VISIT deployed biometric entry procedures to airports and seaports on January 5, 2004. The original scope of this effort covered only those individuals applying for admission with nonimmigrant visas. Starting on September 30, 2004, US–VISIT expanded biometric entry procedures to include those individuals applying for admission under the VWP. US–VISIT's deployment of biometric capabilities focused on entry for security reasons but also because infrastructure and processes on which to build already existed. In contrast, the exit process at air, sea, and land ports has little or no established infrastructure, processes, or available Government personnel. As a result, deployment of biometric capabilities for recording exit requires substantially more planning and innovation.

To that end, DHS has performed significant planning and testing over the past 3 years, examining possible solutions for integrating US–VISIT biometric exit requirements into the international air and sea departure process. The options of deployment at airline ticket counters, TSA checkpoints, and airline boarding gates, and in airport terminals were considered. Between 2004 and 2007, US–VISIT ran biometric exit pilots at 14 air and sea locations. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. The pilots ended in May 2007. While the pilots demonstrated that the technology works, they also revealed the need to embed biometric exit procedures into the traveler's existing departure process to address low voluntary compliance by travelers.

Based on the analysis of these pilots, review of a range of other potential options, pre-existing biometric exit requirements, and the 9/11 Act's mandate to establish a biometric air exit program by June 2009 or face suspension of the Secretary's VWP waiver authority, DHS published a proposed rule on April 24, 2008 to establish a biometric exit system at all air and sea ports of departure in the United States.[3] The proposed rule would require commercial air carriers and cruise line owners and operators to collect and transmit international visitors' biometric information to DHS within 24 hours of their departure from the United States. Carriers are already required to transmit biographic information for these passengers to DHS.[4]

[3] On April 24, 2008, DHS published a Notice of Proposed Rulemaking (NPRM) requesting public comment. This will be followed by a Final Rule addressing public comments, as required by the Administrative Procedure Act, 5 U.S.C. 553. Depending on the final decisions resulting from the NPRM, the Final Rule will need to amend the Code of Federal Regulations in a number of places.

[4] The NPRM relies on section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA), Pub. L. No. 107–173, as does the collection of information from carriers through the Advance Passenger Information System (APIS). EBSVERA revised section 231 of the Immigration and Nationality Act (INA) (8 U.S.C. § 1221) to make statutory that each commercial vessel or aircraft taking passengers on board at any seaport or airport in the United

DHS is committed to protecting the privacy of international visitors and will require that any new systems meet the Department's transmission capability and data security requirements. The proposed rule does not designate a specific location within the port of departure for biometric collection and does not apply to small carriers or vessel owners and operators or to general aviation.

The proposed rule does not require carriers to process exit data but only to collect and forward that information to DHS. The ultimate shape of the Air/Sea Biometric Exit solution will be the result of an open and thorough vetting through the public rulemaking process. During the comment period that ended on June 23, 2008, DHS received numerous and detailed comments in response to the NPRM, both in written form and during a public hearing on June 13, 2008. The Department is in the process of reviewing these comments and will publish a final rule this year, in accordance with the Administrative Procedure Act, other applicable statutes, and established policy.

Once DHS begins receiving the biometric exit data, it will pair that data with corresponding biographic exit data; match entry and exit records; determine overstay status; vet against, and update, watch lists; and forward information that may be appropriate for further investigation to U.S. Immigration and Customs Enforcement. In addition to identifying those individuals who have not left the country in accordance with the terms of their admission, overstay information is important for other purposes. For example, information on individuals who overstayed but then departed the United States is relevant to future immigration determinations, such as a subsequent application for admission to the United States, visa renewal, or other immigration benefits. Overstay information also plays a role in counterterrorism. A critical aspect of counterterrorism efforts is recording the arrival of travelers from areas of the world with significant terrorist or criminal activity. Awareness of travelers from these areas coupled with knowledge about the terms of their admission, including overstay information, is essential to assessing risk and to enhancing the integrity of the immigration and border management system. Finally, comprehensive trend analysis is likely to assist DHS and DoS in identifying specific visa-issuing posts, visa categories, VWP countries, and other criteria that might be common to an unacceptably high overstay rate. This knowledge will enable DHS and DoS to increase scrutiny and to focus efforts according to any identified threat.

DHS is committed by year's end to strengthening the VWP in a substantive way, admitting new, qualified members into the program, and implementing the biometric exit system. As we have outlined today, the Department is well on its way to achieving these goals. We appreciate your continued support of programs that help secure U.S. borders, strengthen the U.S. economy, improve relations with our closest allies, and promote a safer international travel environment.

Chairwoman Sanchez, Representative Souder and Members of the subcommittee, we want to thank you for the opportunity to present this testimony today. We would be pleased to respond to any questions you might have at this time.

Ms. SANCHEZ. Thank you.

Our next witness will be Mr. Mocny, for 5 minutes or less.

STATEMENT OF ROBERT A. MOCNY, DIRECTOR, US–VISIT PROGRAM, DEPARTMENT OF HOMELAND SECURITY

Mr. MOCNY. Madam Chairwoman Sanchez, Ranking Member Souder, distinguished Members of the committee, thank you for the invitation to discuss how US–VISIT is improving our Nation's security and working to fulfill a mandate from Congress and the 9/11 Commission to biometrically record the departure of international visitors from the United States.

States destined for any place outside the United States provide certain manifest information concerning each passenger, crew member, and other occupant to be transported. Subsection 231(c) of the INA, as revised by EBSVERA, expressly identifies certain items of identifying information that carriers must provide to DHS, including: (1) Complete name; (2) date of birth; (3) citizenship; (4) gender; (5) passport number and country of issuance; (6) country of residence; (7) U.S. visa number, date, and place of issuance; (8) alien registration number, as applicable; and (9) U.S. address while in the United States. Paragraph (10) requires carriers to provide "such other information the . . . [Secretary of Homeland Security] determines as being necessary for the identification of the persons transported and for the enforcement of the immigration laws and to protect safety and national security."

Madam Chairwoman, I think it is safe to say that we all agree that exit control is a priority for the securing of our Nation's borders. From the inception of the US–VISIT program, we have sought to apply the power of biometrics to an automated exit capability. Today I would like to focus specifically on our efforts at the airports and the seaports.

Generally speaking, collecting biometrics from visitors upon departure presents many more hurdles than collecting biometrics upon entry. Unlike at entry, our airports and seaports have little or no established governmental infrastructure, processes or available Government personnel to collect biometrics from departing travelers. As a result, deployment of biometric exit capabilities has required significantly more planning and innovation than entry.

Over the past 3 years, DHS has examined possible exit solutions for the airport and seaport environments. From 2004 to 2007, US–VISIT evaluated the use of both automated kiosk and mobile devices in port terminals in 14 air and sea locations. While the pilots demonstrated that the technology works, with no Government infrastructure or processes in which to embed the procedures, traveler compliance was low. Our final evaluation of the pilot determined that to achieve 100 percent compliance, biometric exit procedures need to be incorporated into the current departure process for international travelers.

Within 12 months of completing our pilots at airports and seaports, we were ready to publish a notice of proposed rulemaking to establish a biometric exit system. DHS's proposal would require airlines and cruise lines to collect biometric data from departing visitors and transmit it to DHS, as they currently do with biographic data.

As part of the NPRM, we examined our proposal's economic impact, its impact upon the ports, its impact upon travelers and their privacy. The NPRM also outlined a number of alternatives to generate discussion about other possible approaches. During the public comment period, we heard from carriers and others, both in writing and at a public hearing, and we were gratified by the number and substance of the responses. We are currently considering and analyzing all 110 comments as we chart a path forward.

We have always said that a comprehensive, long-term biometric exit strategy for the United States is an exceedingly complex and costly challenge. The NPRM acknowledges that meeting this challenge will require the commitment of significant investments and close coordination between DHS, the airlines, the cruise lines and our intergovernmental partners.

Let me be clear: We are committed to deploying the best solution available within the timetable Congress has outlined in the 9/11 Act.

Thank you for the opportunity to address you today. I look forward to your questions.

Ms. SANCHEZ. Thank you, Director Mocny.

Now I would like to recognize Deputy Assistant Secretary Edson to summarize his statement for 5 minutes or less.

STATEMENT OF STEPHEN A. "TONY" EDSON, DEPUTY ASSISTANT SECRETARY FOR VISA SERVICES, BUREAU OF CONSULAR AFFAIRS, DEPARTMENT OF STATE

Mr. EDSON. Thank you, Chairwoman Sanchez, Ranking Member Souder and distinguished Members of the subcommittee. I am delighted to be here this morning and appreciate this opportunity to discuss the role the Department of State plays in the Visa Waiver Program and the Electronic System for Travel Authorization under the new legislative requirements of section 711 of the Implementing the 9/11 Commission Recommendations Act of 2007.

We welcome the congressional initiative to modernize the VWP and the passage of the 9/11 Act last summer, particularly the additional VWP security measures. The new law not only strengthens the security framework of the program, but it also creates a path for expansion for the Visa Waiver Program to include some of our closest allies. These enhancements will help secure U.S. borders and promote a safer international travel environment.

As my DHS colleagues have noted, the USG is negotiating memoranda of understanding with all VWP governments, both existing and prospective. The USG has now signed MOUs with eight VWP roadmap countries and is negotiating one with Greece. We will be negotiating similar agreements with the current VWP countries next.

We are working closely on the second part of the MOU process, the expansion of information-sharing with VWP members and aspirant countries. Terrorist and criminal information-sharing is a high priority.

As part of the Department of State's responsibility to obtain terrorist screening information from foreign partners, pursuant to Homeland Security Presidential Directive 6, we have signed agreements with five visa waiver countries and four roadmap countries. We are in varying stages of negotiations with 25 additional countries, including 17 VWP countries and six more roadmap countries. We anticipate that several more agreements will be signed within the next few months.

The Secretary of State has delegated authority to negotiate agreements to exchange criminal history information to prevent and combat serious crime jointly to DHS and DOJ. The successful conclusion of operational arrangements for an increased level of cooperation in both areas has been stimulated by the dialogue on the Visa Waiver Program.

We are fully engaged with DHS on the implementation of their ESTA, the electronic system through which visa waiver travelers will apply online for preapproval to board a ship or plane bound for the United States. Those travelers denied an ESTA are instructed to make an appointment at their nearest embassy or consulate to apply for a visa. DHS has provided us with data simulations that indicate that the number of ESTA denials will likely be less than 1 percent. We have used that data to project potential workload changes to VWP member country and aspirant posts.

We anticipate that we would generally be able to absorb an increase in workload of 1 percent without additional resources in most VWP countries, with the exception of Japan and the United Kingdom, which send the largest numbers of visa waiver travelers

to the United States. Even in the United Kingdom and Japan, however, only minor adjustments to resources would be needed to handle the workload caused by an ESTA denial rate of 1 percent or less, as predicted by DHS simulations.

We worked closely with the Government Accountability Office on their recent report on workload planning for visa waiver, and we are doing contingency planning for ESTA denial rates much higher than those predicted by DHS. We have looked at resource requirements for rates of 2 and 3 and up to 10 percent. We agree with GAO that an ESTA denial rate above 3 percent would cause greater difficulty at some of our larger posts. But all the models we have seen from DHS indicate that a refusal rate that reaches even the 1 percent level is unlikely.

The Department already responds to staffing needs with a flexible and responsive workforce. These increased staffing needs for this purpose can be met with various staffing tools and strategies already in use, both in the short term and in the long term. We will closely monitor post workload as ESTA is implemented and adjust resources and temporary assistance as needed. We will also send our posts additional guidance about managing their applicant streams to assist those who are denied ESTAs and need to apply for visas.

We have worked closely with DHS in the planning process and will continue this collaboration.

In closing, the Department appreciates Congress's passage of the VWP provisions of the 9/11 Act. We see the new requirements as a positive means to strengthen the security of visa-free travel, permit some of our closest friends and allies to join the Visa Waiver Program, and thereby enhance our cooperation and ties with those countries over the long term. The Department is committed to working with our partner agencies and with this committee toward that goal.

Of course, I am happy to answer your questions.

[The statement of Mr. Edson follows:]

PREPARED STATEMENT OF STEPHEN A. "TONY" EDSON

JULY 16, 2008

Thank you, Chairwoman Sanchez, Ranking Member Souder, and distinguished Members of the subcommittee. I am delighted to be here this afternoon and appreciate this opportunity to discuss the role the Department of State plays in the Visa Waiver Program (VWP) and the Electronic System for Travel Authorization (ESTA) under the new legislative requirements in Section 711 of "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act).

While visiting Tallin, Estonia, in November 2006, President Bush announced his initiative to revamp and strengthen the VWP. As I have testified before, we welcomed the congressional initiative in modernizing the VWP and the passage of the 9/11 Act last summer, particularly the additional VWP security measures. The new law not only strengthens the security framework of the program but it also creates a path for expansion of the VWP to include some of our closest allies. These enhancements will help secure U.S. borders and promote a safer international travel environment.

Together with our colleagues at the Department of Homeland Security (DHS), we strive constantly both to protect America's borders and to preserve America's welcome to legitimate international visitors. Section 711 of the 9/11 Act, "Modernization of the Visa Waiver Program," supports these efforts by making clear that the security provisions of the VWP must be enhanced before VWP participation can be extended to any additional countries.

With the advancement of both new security technologies and new security risks, we can and must ensure that for VWP participants and aspirant countries, we are able to assess the risks posed by individuals, not countries, as threats. The changes in the VWP in the 9/11 Act give us the tools to do this. The Department of State believes these enhanced security measures promote safer international travel.

I want to discuss briefly the role of the non-immigrant visa refusal rate in the context of VWP. Provisions requiring a non-immigrant visa refusal rate of less than 3 percent remain in the law, but the 9/11 Act gives the Secretary of Homeland Security a new waiver authority for countries with a refusal rate of at least 3 percent but less than 10 percent in the previous fiscal year. This waiver authority is conditioned on a number of factors, including DHS implementation of the Electronic System for Travel Authorization (ESTA) and an air exit verification system, and the aspirant country's fulfillment of the enhanced security requirements of the new law. The Department of State monitors and reports on these visa refusal rates annually on our Web site at *www.travel.state.gov*.

For purposes of the VWP, the nonimmigrant visa refusal rate is based only on the number of visitor ("B") visa applications submitted worldwide, by nationals of that country. (B visas are issued for short-term business or pleasure travel to the United States.) The Department adjusts the refusal rate to exclude the number of visa refusal cases that are overcome and subsequently issued. Adjusted visa refusal rates for nationals of current VWP countries reflect only visa applications submitted at U.S. embassies and consulates abroad. They do not take into account persons who travel to the United States without visas under the VWP. VWP country published refusal rates therefore tend to be higher than they would be if the VWP travelers were included in the calculation, since such travelers would in all likelihood have been issued visas had they applied.

The revised VWP legislation also gives the U.S. Government (USG) the means to increase security information-sharing with our closest allies. The USG is negotiating memoranda of understanding (MOUs) with all VWP governments, both existing and prospective. The USG now has signed MOUs with eight "VWP roadmap" countries (The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Slovakia, and South Korea) and is negotiating one with Greece. We will negotiate similar agreements with current VWP countries next.

We are working closely on the second part of the MOU process, the expansion of information-sharing with VWP members and aspirant countries. Terrorist and criminal information-sharing is a high priority. As part of State's responsibility to obtain terrorist screening information from foreign partners, pursuant to Homeland Security Presidential Directive 6 (HSPD–6), we have signed agreements with five VWP countries and four "VWP roadmap" countries. We are in varying stages of negotiations with 25 more countries, including 17 VWP and 6 roadmap countries, and we anticipate several more agreements will be signed within the next few months. The Secretary of State has delegated authority to negotiate agreements to exchange criminal history information to prevent and combat serious crime jointly to DHS and DOJ. The successful conclusion of operational arrangements for an increased level of cooperation in both areas has been stimulated by the dialog on VWP.

By statute, DHS has the lead for the VWP program and works in close coordination with the Department of State on all aspects of the program. The Department of State must consult with DHS regarding the designation of a VWP program country. We formally document this through the Secretary of State's nomination of a country for consideration for VWP membership. We are the primary conduit for guidance on VWP issues to our posts abroad. State Department officers at these posts, in turn, are the primary interlocutors with host governments, the travel industry, the media and public on issues related to VWP. We provide input on DHS's evaluations of a VWP aspirant country's law enforcement, immigration, and security cooperation, as well as during DHS's statutorily mandated country reviews for both initial and continuing participation in the VWP. We have participated in the negotiations throughout the year with the "roadmap" countries on the VWP accession process, and have given them guidance on meeting the new statutory requirements.

We are fully engaged with DHS on the implementation of their ESTA, the electronic system through which VWP travelers will apply on-line for pre-approval to board a plane or ship bound for the United States. Those travelers denied an ESTA are instructed to make an appointment at their nearest embassy or consulate to apply for a visa. DHS has provided us with data that indicate that the number of ESTA denials will likely be less than 1 percent. We have used that data to project potential workload changes at VWP member country and aspirant posts. We anticipate that we would generally be able to absorb an increase in workload of 1 percent without additional resources in most VWP countries with the exception of Japan and the United Kingdom, which send the largest numbers of VWP travelers to the

United States. Even in the United Kingdom and Japan, only minor adjustments to resources would be needed to handle the workload caused by an ESTA denial rate of 1 percent or less, as predicted by DHS.

We worked closely with the Government Accountability Office (GAO) on their recent report on workload planning for VWP. We are doing contingency planning for ESTA denial rates much higher than those predicted by DHS and have looked at the resource requirements for rates of 2 and 3 percent. We agree with the GAO that an ESTA denial rate of above 3 percent could cause greater difficulty at some of our larger posts, but all of the models we have seen from DHS indicate that a refusal rate that reaches even 1 percent is unlikely. The Department already responds to staffing needs with a flexible and responsive work force, and these increased staffing needs for this purpose can be met with the various staffing tools and strategies already in use, both in the short-term, and in the long-term. We will closely monitor post workload as ESTA is implemented and adjust resources and temporary assistance as needed. We will also send posts additional guidance about managing their applicant streams to assist those who are denied ESTAs and need to apply for visas. We have worked closely with DHS in the planning process for ESTA and will continue this collaboration. DHS has indicated they would consult closely with us on the need for changes to ESTA operations if screening outcomes are significantly different from those predicted.

We realize that with ESTA being a new and unknown process, some people may choose the surety of having a visa in their passport instead of applying for an ESTA. However, the number of people who take this approach—and the size of the resulting workload increase—will depend largely on public perception of the certainty, effectiveness, convenience, and cost of the ESTA program. Therefore, we have worked closely with DHS, CBP, and Commerce to create a widespread and robust outreach program. ESTA information is posted on embassy Web sites in both English and local languages, and is prominently featured on our public Web site, *www.travel.state.gov* with a link to CBP's official ESTA Web site. We have conducted significant press and travel industry outreach through our embassies abroad. Embassy public affairs sections, consular sections, and DHS offices abroad are collaborating to hold meetings with and make presentations to travel stakeholder groups and news media. Staff members are utilizing DHS/CBP's fact sheets and sample screens of ESTA to communicate not only that ESTA will increase the security the program provides for all travelers, but also that ESTA is user-friendly, quick, and secure. We have been monitoring our posts for increases in volume from "just-in-case" applicants, and have yet to see any significant up-tick in applications.

We are working hard to ensure that the visa process is a complement to the ESTA process. We have coordinated with our colleagues in CBP and DHS as the ESTA system has been planned and are ensuring that we expand State's already robust information-sharing arrangements with DHS to include ESTA information. DHS advises that our consular officers will be able to see whether an applicant for a visa has been denied an ESTA, and why. This will assist us in determining eligibility for a visa. There may be cases when the visa interview resolves the reason for the ESTA denial and therefore the traveler will qualify for a visa. In other cases, the applicant may need to apply for a waiver of ineligibility. And in a few cases, that person may not be allowed to travel to the United States. It is important to clarify that the visa process is an entirely separate process from the ESTA process; travelers denied an ESTA would not be able to resolve their ESTA case at an embassy or consulate. What they will be able to do is apply for a visa, at which time we will include the ESTA information to assist us in determining eligibility.

In closing, the Department appreciates Congress' passage of the VWP provisions in the 9/11 Act. We see the new requirements as a positive means to strengthen the security of visa-free travel, permit some of our close friends and allies to join the VWP, and thereby enhance our cooperation and ties with those countries over the long term. The Department is committed to working with our partner agencies and with this committee toward that goal. I will be happy to answer your questions.

Ms. SANCHEZ. I thank you, Mr. Edson.

I now thank all the witnesses for their testimony.

I will remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize myself for some questions. My first one is for Mr. Mocny.

Some people in Congress have suggested that we should suspend the Visa Waiver Program altogether, in the interest of national se-

curity. However, I think that this subcommittee has tried to balance the critical national security concerns with, obviously, the workload and efficient flow of travelers coming to and from the United States. It also, of course, has implications with those nations that we have this Visa Waiver Program with, with respect to visas required for our citizens when they go to visit.

So my question to you is, what are the contingency plans that are in place if Congress decides to suspend the Visa Waiver Program altogether?

Mr. MOCNY. I don't know that I am the best person on this panel to answer that question. I mean, the contingency plans would, of course, have a large effect on the Department of State, so I would like Mr. Edson to talk about what would happen in the event that it were to be suspended.

Ms. SANCHEZ. Mr. Edson.

Mr. EDSON. We have, both on our own and then in cooperation with GAO, we have looked at this issue.

The numbers themselves point out the difficulty here. We will probably receive about 8.6 nonimmigrant visa applications this year. The number of visa waiver travelers to the United States in a given year exceeds 14 million. So we would effectively be tripling our workload if the Visa Waiver Program were to end.

Immediately, we would have to respond by dealing with it as best we could. These missions in visa waiver countries, many of them are fairly small physical plants. We have had the Visa Waiver Program in place for enough years now that the physical plant in these European capitals and in Japan has not expanded, has never dealt with huge volumes of visa travelers. So it would be—the contingency plan has involved muddling through, to be honest with you, as best we can.

Ms. SANCHEZ. So you have no contingency plan.

Mr. EDSON. No, we have run all the numbers, but there is no way for us to triple facilities and staffing in any reasonable amount of time. It would take years, and it would impact travel and commerce in this country.

Ms. SANCHEZ. So you wouldn't be ready for a large increase in number of visa applications.

Mr. EDSON. Correct. Tripling the number of visa applications is not something we could handle.

Ms. SANCHEZ. So, do you have a plan? Do you actually have a written plan if we should suspend the Visa Waiver Program? I mean, do you have a written plan, or do you just—I mean, I understand that you have gone through the numbers and you said it would triple, you know, our requirement of personnel and resources in France, let's say.

Mr. EDSON. Right. We have projected what it would mean for facilities and officers and local national staff in each of the countries where we now have the visa waiver in place.

In terms of responding to that, however, at that level, we are funded by fees, and so we would go into that increasing workload without capital to make the investments to meet that demand in resources.

Ms. SANCHEZ. The roadmap countries' entrance into the Visa Waiver Program would be delayed if the Department of Homeland

Security does not meet the June 30, 2009, deadline for the implementation of the US–VISIT biometric exit system.

What kind of difficulties would that pose, diplomatic-wise, on the State Department if we could foreseeably see that these roadmap countries would not get visa waiver?

Mr. EDSON. Thank you for the question.

The roadmap countries—in each of these roadmap countries, visa waiver membership is a prominent domestic political issue and, in most cases, a key issue in their bilateral relationships with the United States. They expect and hope, they have expected and hoped for a couple of years, that they might be in the Visa Waiver Program in the immediate future.

If there are further delays, then we will work closely with them to help explain, make sure they understand why those delays are necessary.

Ms. SANCHEZ. I was just at a Helsinki Commission OSCE meeting in Kazakhstan, where we had a lot of our European allies, some who are in the Visa Waiver Program, obviously some who want to be. They are very angry about this whole issue of the Visa Waiver Program, you know, especially those who deem themselves in the European Union, that some have it and some don't.

Mr. EDSON. Right.

Ms. SANCHEZ. So I think it is really high on their list when our counterparts talk to us up there.

I have one last question for Mr. Barth and Mr. Mocny. If your rulemaking is rejected, what plan do you have? If we decide, for example, if the Congress says it is unacceptable for you to lay all this work on the airlines.

Mr. MOCNY. We don't have a plan. We don't have a contingency plan if it is not. I mean, we are trying to follow the APA, the Administrative Procedures Act. We published the NPRM. We have the comments now. We are taking a look at what the final rule would look like. We want to publish the final rule in a timely fashion. We do want to meet the congressional deadline of June of 2009, to give the Secretary of Homeland Security the ability to waive the visa refusal rate. It is a large part behind some of the thinking.

So if that doesn't go forward, we would have to, of course, replan, retool, reschedule and look at it from a budgetary standpoint and from a deployment standpoint.

But we are, at this point, moving confident that we can publish a final rule in the time frame. But we have no alternative plan, other than to look at—and, again, in the NPRM, I think as you know, we did put several other alternatives in there. We costed those out, as well. We may pull from one of those. I think we would have to go back into planning mode and see what we might be able to put out there in the time frames that we have been given by Congress.

Ms. SANCHEZ. Mr. Barth, do you have anything to add to that?

Mr. BARTH. No. I think the Department is very much committed to meeting the timetables. It is going to be a challenge, the longer it takes to implement the final rule and give airlines adequate time to adjust to what is required in that rule.

We are still, as Mr. Mocny mentioned, we are still reviewing the over a hundred comments that came in, some of them very sub-

stantive, with alternative scenarios provided. So once that review is completed, we will be in a better position to, I think, answer your question, both primarily will we be able to do it and when we will be able to do it and how we will be able to do it.

Ms. SANCHEZ. Thank you, Mr. Barth.

My Ranking Member for 5 minutes, Mr. Souder.

Mr. SOUDER. Thanks.

I want to focus on the US–VISIT question. If somebody comes in through land and exits air—Mr. Mocny, I guess you would probably take the lead; Mr. Barth, if you have any comment—that if somebody comes in land and exits air, will you be able to pick them up?

Mr. MOCNY. If we implement the final rule as we have in the proposed rule, yes.

Mr. SOUDER. But if they come in land illegally, because we don't quite have it all sealed yet, and then try to exit—and that was an understatement—if they come in illegally and then try to exit through an airport, would we catch them?

Mr. MOCNY. We would. In the pilot programs we did. Because the infrastructure is there, the people are kind of funneled into the process, then that is how our guarantee of capture of the information is. They can't get on board the plane without getting the biometrics taken.

So, yes, if they came in illegally and left through the airports, if the airlines do what is required of them per the final rule, if it goes the way as the NPRM goes, then, yes, they would be so identified.

Mr. SOUDER. If they come in air and exit land, we would have no proof.

Mr. MOCNY. At this point, no, we don't have a land exit in place.

Mr. SOUDER. Which shows the importance of the interrelationship of the programs.

Mr. MOCNY. Absolutely.

Mr. SOUDER. Clearly, the kiosk alternative is the lowest cost. There are challenges, because the airlines are in financial distress, would be the best way to say it. Not as though the Government isn't in financial distress either; we can just print money to cover our financial distress. This is an incredible challenge.

What I am having trouble understanding from the beginning—and this whole process has been very educational. First off, the American people need to understand that we are safer than we were. Just because we don't have it done doesn't mean that the financial tracking, the intelligence tracking, the clearance, where the Visa Waiver Program was. I mean, we have made incredible progress. But we are not where we need to be.

In the challenge of looking at the different airports—I went behind the scenes in Miami, which is the highest percent international, and, I mean, every gate in every place has international wings. The airports are saying, look, where are you going to put this stuff? It depends how we redo the airport. So some of them have gone ahead and had to make certain assumptions.

The different airports are jammed at DHS clearance, different ones where you check in, different ones at the gate. There is no uniform system that is going to be easy. Our indecision here has complicated that.

I personally feel that the data is the responsibility of the Government. What I have—and as we have had these hearings, the airlines have pointed out that, yeah, I get some of my tickets on-line, some of them I do at a kiosk, some of them I do at the manual check-in, particularly if it is at the last minute.

What I am having trouble understanding is why in a Government interconnected system in the computer era we can't have an automatic pop-up that feeds in, whether you are going on-line or at a kiosk or through the airlines, that says you have a problem, and then it moves.

Why are we spending so much time arguing about the method? Because it could be done by the airlines if the data is in the Federal Government, but there is a flag if there is a problem, and then it kicks over. What is the problem with that?

Mr. MOCNY. Well, you certainly outlined a series of the challenges that we are faced with.

If I can somewhat break that down, I mean, the scenario that you paint basically says that all of these 70-some-odd airports from which people can leave internationally from are not all the same size. They are different configurations. They are different locations where TSA can be present. Some can leave from various gates, as you outlined.

So the thinking was, and given the time frame that the Congress had given to us of June 2009, we are going to have to use existing infrastructure. We can't make it up in the time. We can't put departure control booths, like we have in Europe and Asia. We don't have the personnel to automatically stand these situations up.

So the thinking behind it was that the airlines today are required to validate the information on the passport. Anybody leaving internationally, whether you check in on-line at home or you check in at the counter at the airport or you go through TSA and check in perhaps at some point beyond that in the gate area, wherever else you might do it, or transfer in the gate area, the airlines are the ones that are going to have to validate that individual's passport information.

Given that fact and given the fact that the airlines are required to submit manifest information to us, we were of the mind that it was that process, that known process, so as least disturbing to the traveler so that they don't get confused of where am I supposed to go, something different than what I am used to, that that known process is the best place to capture the information.

The airlines are required, as I said, to capture the passport information. They are required to submit manifest information. So what we are asking the airlines to do is append to that manifest biometric data. Given the time frame, it seems to us to be the most efficient way of dealing with biometrically verifying the individual.

So, given the complexity you outlined, the various different airports, the various gates, the various ways in which someone can go through a different airport, the known process, what is known, the known process is someone goes from point A to point B and then gets on-board the plane.

It is through those various touch points that the airlines have the most control of the individual with respect to information that

they are required to give. So that is why we have the proposed rule written as we do.

Mr. SOUDER. If we have more questions, I have a follow-up.

Ms. SANCHEZ. We will do a second round.

Ms. Harman, are you ready for 5 minutes of questioning?

Ms. HARMAN. Yes. Thank you, Madam Chairwoman.

Welcome to our witnesses.

I was a member of the National Commission on Terrorism, which wrote a pretty lengthy report before 9/11. One of the things that we highlighted was our flawed visa system. We were focusing mostly on visas to study in the United States. But there is no question that on 9/11 our visa system was exploited by people who wanted to kill as many of us as possible.

So I care a lot about this, and I care a lot about doing it right. I commend you for holding the hearing, and I commend our witnesses for struggling with some good answers.

The 9/11 Act enables the Secretary of Homeland Security, in consultation with the Secretary of State, to increase membership in the Visa Waiver Program if certain criteria are met. That is why we are having this conversation.

One of them is the ability to get your arms around who is leaving our country. That is a critical part of the Visa Waiver Program, because if we don't know who leaves, we aren't having a program that is granting temporary rights to visit the United States.

So I have been listening to this conversation. I understand that there are all kinds of problems with technology and time and resources and people, but it doesn't seem to me that the right answer is to say, oh, the airlines, who are struggling with incredible fuel costs and survival, ought to take on this project.

My question is whether you have thought as creatively as possible. For example, if the kiosks in airports where you get your ticket—and maybe this has been explored, Madam Chairwoman; I apologize if it has—where you get your ticket that also has some other feature that included, you know, push here for entering biometric data, and you had to do this on entry and exit, then you would have that data, and the airlines would just verify that the ticket was properly embossed and had this little box checked.

Why wouldn't that be an answer to this problem?

Mr. MOCNY. Thank you for the question.

That may very well be an answer to the question. In fact, what we have told the airlines is that we don't really care how or where you collect the information. It might be at the counter for those people who are checking baggage. It might be at a kiosk for those people who use a kiosk. It might be at the gate. It could be in one of the lounges.

So we are agnostic as to where the biometrics are collected by the airlines. We are simply saying that, as part of this departure process, collect that biometric, append it to the departure manifest, and then send that information to us.

Ms. HARMAN. Well, as I am thinking about this, I wasn't assuming they would bear all the freight for putting this feature on the kiosk. I think it is a Federal responsibility—it certainly is under the 9/11 Act—to have this information.

So why couldn't you put this feature on kiosks, either the ticket-printing kiosks or some other easy-to-use piece of technology at the airports?

Mr. MOCNY. I think the short answer is, ma'am, that we don't have the funding for that. So we don't have the dollars to do the up-front costs of putting out the actual devices themselves.

Mr. Harman. How much would this cost?

Mr. MOCNY. Our estimates range somewhere in the $60 million amount for the deployment of biometric exit at all the airports. That is a rough figure, and I wouldn't want to be quoted on that for the end of the day. But it is approximately what we determined a couple of years ago. It might be as high as $70 million or more.

But, again, we have broken down the costs in the NPRM, so I would, I guess, use that as the definitive. We did put several alternatives, and kiosks are in there. We did cost these out according to the cost-estimating processes, did it over 10 years. So that is the best place, I think, to determine what it really would cost us to do the work.

Ms. HARMAN. Well, I don't want to minimize the value of $60 million or $70 million, but I think the cost of having—let's just be bold about this—another terrorist attack because this program has been abused are a lot greater than $60 million or $70 million. I don't think it is fair to have the airlines bear the whole freight. I do think it is a Federal responsibility to make sure that our immigration laws are observed properly.

Madam Chairwoman, I am glad you are pushing on this. I think we need better answers here. If we have to give up this Visa Waiver Program, which I would hate to do, because we can't implement it properly, that may have to be one of the costs here.

I yield back.

Ms. SANCHEZ. I thank the gentlewoman from California. I know you have a lot of experience in that. Again, there are many people on this committee who see the airlines struggling and wonder why we are pushing it off to them when really it is a Government responsibility.

Mr. Souder, you had a couple more questions to ask before we get to the second panel.

Mr. SOUDER. Yes, I wanted to follow up directly with that. Because the question here is who should bear primary responsibility for what is, in effect, Government data collection and implementation.

In looking at the options, did the administration ever propose to Congress that we pay this?

Mr. MOCNY. I don't believe that we submitted an air exit. We have for the land border, but we have not submitted as part of the President's budget an air exit budget.

Mr. SOUDER. Because, in the question, every kiosk wouldn't have to handle this. You could have a principle that you are not going to be able do this on-line. If you are going to exit, you are going to have to go to a kiosk.

You had an alternative for—I remember at Detroit, in their pilot program, even though the kiosks were tried at several locations, it wasn't necessarily easy to find them.

Mr. MOCNY. Correct.

Mr. SOUDER. I understand that challenge. It would be easy to find them if you said, this is international travel, this kiosk is cleared for this type of thing. At some airports it would be more expensive. For example, in my hometown of Fort Wayne, it wouldn't be very expensive.

You could even have in the smaller airports, where they have a lot of cooperative airline type of things already, have one kiosk that—because they are already doing all kinds of partnerships, that clears in if you are clearing international.

The question is, is that I don't believe, and we are finding this in several categories, that in order for the Government to save money, we merely cost-shift Government responsibility. We are seeing this in veterans health care. Oh, we are going to send them to the bigger cities. So even though gas mileage has gone up immensely, we are not going to give them local health care, we are going to make the veteran pay the cost of driving to a major city, we are going to make the veteran get the motel overnight. That saved the Government money, but it didn't save the individual money. We are seeing this cost-shifting occurring in general.

Look, I am a believer in this program. I am a believer that we need to have background checks. I am concerned about penetration in the European Union. Based on public information, Qadhafi clearly was trying to put people in the Caribbean as latent people to do his work, and try to get E.U. citizenship to penetrate. I have concerns about the program. But our international travel will drop. Our ability to trade will drop. In this type of world, it is not acceptable. We have to move ahead with these kind of programs.

But it has to be a fair way to do it, so we don't sink our airlines. I am disturbed that we are not hearing some kind of a compromise, creative way to do this.

Mr. MOCNY. I think it is fair to say that, again, we are letting the APA, the Administrative Procedures Act, kind of play out. We have not yet published a final rule. So I appreciate the comments, and we are certainly taking the comments, and those are not—I think many people share your concerns. So, as we move forward with the decision to put a final rule out there, all these comments have to be taken into consideration. So while I can't say for sure what that will look like, those concerns have been voiced, and in writing, and we are hearing them from you.

So it is, as I said, a challenge for us. We have the June 2009 time frame. We want to be compliant with the congressional mandates. I think we all recognize that we don't have the same type of departure control systems that many European and Asian countries do. So given those challenges, it was, "Well, gosh, then what is the best and most efficient and effective process, given that reality?" That is the fact that, since we don't have the budget for it, we could not commit to a time frame of June 2009, therefore we used existing infrastructure.

If I could, just to clarify my comment to Congressman Harman here, and I would like to use this for the record, $1.3 billion is the Government cost for kiosks, not the $60 million to $70 million. That is kind of an old number that we had for just buying kiosks out there. There are infrastructure costs, there is people to staff them. So $1.3 billion is what we have in the NPRM cost factor.

Mr. SOUDER. But that wouldn't necessarily be the cost of operating, because if you have kiosks—and depending upon the capability of the kiosk, we are really talking about software upgrades. If you used existing kiosks, you are basically talking about software upgrades inside kiosks that are already hooked up, that are already there.

Can I request on behalf of the committee that we get some kind of an estimate or understanding of whether that figure was fundamentally, you know, putting hard wire in? What does that figure mean, as opposed to try to use existing infrastructure and adapt the software?

Ms. SANCHEZ. We will ask Mr. Mocny to provide maybe a breakdown of whatever the figure is, the $1.3 billion or whatever you think it is at this point, and what that entails.

Mr. MOCNY. We can certainly do that.

That is new kiosks, Congressman Souder. It is new kiosks, with enough to be out there so people can't miss them. It is people to man and staff those booths.

So it did not contemplate taking the existing kiosks and putting what might be called a sidecar on there, which would be a biometric verification. So that was not considered as part of this. It was kind of a clean, new kiosk, with new software, and look and feel of the whole process.

Ms. HARMAN. Would the gentleman yield to me?

Mr. SOUDER. Be happy to.

Ms. HARMAN. I would just suggest that that submission also include other ways to achieve the same function. It doesn't have to be a kiosk. There might be three or four flavors here, so that we can assess what the range of costs is.

Obviously, we are not interested in doing the most expensive thing here. We are interested in getting a result.

I yield back.

Mr. MOCNY. I appreciate that. Again, I think the NPRM was fairly clear. We have four alternatives, which envisioned a series of alternatives, including mobile devices, as well, that the airlines might be able to use.

So it did look across the plane, as far as various technologies that are out there, but it did make some assumptions in the proposed rule, that the airlines would be the ones paying for and maintaining the system.

Ms. SANCHEZ. My suggestion to you, Mr. Mocny, would be that this committee—and I would assume once we educate the rest of our Members of Congress here—that we are not very interested in passing along these cost to the airlines at this point. So it would be wise to maybe start taking a look at costing out some of the alternatives either that Mr. Thompson and I proposed to you in our information we sent over or maybe some of the comments from this committee.

Because I have a feeling that if you decide to move forward with the rule that would require the airlines to take on the financial responsibility of doing this, you may get blocked pretty quickly by this body.

Mr. SOUDER. Could I ask for one further clarification?

Ms. SANCHEZ. Yes, Mr. Souder.

Mr. SOUDER. Because part of this is a question of how much of the burden falls to people who don't use air travel? All taxpayers of the United States. How much falls to the people who use air travel? Then how much does the general society benefit in their jobs and so on from the air travel? Because everybody benefits some. What is the trade-off here, in addition to this?

But when you said you looked at different alternatives, my understanding is, from what you said, you didn't look at a blended alternative, where you used existing kind of capability but the Government would enhance it. Did any of your alternatives include that? Or was it kind of like either/or?

Mr. MOCNY. No, the four alternatives other than the proposed rule, just very quickly, we said at the check-in counter, where the airlines pay for it, so that is purely check-in counter; at the security checkpoint, at the TSA, where the Government pays for that; and then at the location where the carriers want to do it, so at the gate or at a lounge or anywhere else in the airport, and we pay for it, the Government pays for it; and then the fourth was the kiosk solution.

So we did look at a combination of we pay for, they implement; we pay all for. That is where, again, just according to how the APA works out, we chose the most effective, least costly alternative. As you indicated, the kiosk for us, in our experience, wasn't the most effective, and so we went to then the most effective——

Mr. SOUDER. Let me clarify. Least costly for the Government?

Mr. MOCNY. Correct. Well, no, no, no, least costly all across the board. The kiosk was, in fact, the least costly, but it wasn't the most effective, because people weren't checking out, therefore people wouldn't check out. So which one was the next least costly that was effective? That was the carrier implements and carrier pays for. That was the least cost. It started getting higher with the Government costs, Government TSA, and others. So that is simply how the rule worked out.

Ms. SANCHEZ. Thank you, Mr. Mocny.

I have another question with respect to the Electronic System for Travel Authorization. How is DHS planning for countries that may not be Internet-savvy?

Mr. BARTH. Thank you. That is a question we have addressed, I think, pretty thoroughly in our plans for the ESTA rollout. You have countries like Estonia, which expects to be in the VWP program this year, that is extremely net-savvy, very high bandwidth and Internet user country. You have others that are not at that position at all. We expect over time to roll out capabilities to enable ESTA to be applied for at the time of purchasing a ticket through the airline, at the time of purchasing a ticket through a travel agent, or any other way that a traveler generally arranges to fly, that they will have a linkup to that ticket purchasing as the way to acquire an ESTA.

Ms. SANCHEZ. So if I am in a visa waiver country and I do ESTA and I go to my airline agent, my travel agent, your assumption is, because I don't have a connection at home, I am going to get it at the time that I am purchasing my ticket, I am going to give them my biographic information, et cetera.

Mr. BARTH. That is correct. That is what we call a third-party application for the ESTA. The current design of the system allows for that. I can't give you a specific time when that particular capability will be introduced, but it is part of the rollout plan.

Ms. SANCHEZ. When the program becomes voluntary on August 1, 2008, what are the steps that have been taken to ensure that foreign countries and their citizens are aware that this is a program and that it will actually become a requirement?

Mr. BARTH. That is a very good question, Chairwoman. We have already accomplished more than a dozen briefings in different foreign capitals around the world. We have been in media interviews around the world to brief, through the media, the public as to what this new requirement will be as it comes along.

At over 24 U.S. Embassy Web sites, when you go to obtain information on applying for a visa, we have a link to ESTA and what it will be like and what will be required when. We expect to ramp up, as we get closer to the August, September time period, advertisements in travel magazines, Travel & Leisure, you know, ways that will reach the entire general public.

I think we have an excellent public relations rollout campaign that is funded adequately to make sure the word gets out.

Ms. SANCHEZ. Thank you, gentlemen. Thank you so much for being before us. You are excused.

We will ask the second panel to come forward.

Our first witness is Douglas Lavin, Regional Vice President for North America, International Air Transport Association. IATA represents 230 airlines, comprising over 90 percent of the scheduled international air traffic, and Mr. Lavin joined IATA after the Federal Aviation Administration.

Welcome.

Our second witness, Greg Principato, is president of the Airports Council International—North America, which represents local, regional, and State governing bodies that own and operate commercial airports in the United States and Canada. His involvement with aviation and transportation infrastructure spans more than 25 years.

Welcome.

Our final witness, Nathan Sales, is an assistant professor of law at George Mason University School of Law, where he teaches national security law and administrative law. Before coming to George Mason, Mr. Sales held positions in the Department of Homeland Security and the Department of Justice.

Welcome.

Without objection, the witnesses' full statements will be inserted into the record.

I will ask Mr. Lavin to summarize his statement for 5 minutes or less.

STATEMENT OF DOUGLAS E. LAVIN, REGIONAL VICE PRESIDENT FOR NORTH AMERICA, INTERNATIONAL AIR TRANSPORT ASSOCIATION

Mr. LAVIN. Thank you, Madam Chairman, for allowing us to share the views of the International Transport Association on the 9/11 Act's Visa Waiver Program. IATA considers the Visa Waiver

Program to encourage millions of people to visit the United States that might otherwise have not done so. IATA and its 78 members that serve the U.S. market strongly support the VWP and initiatives to protect its continuing viability and expansion to additional countries.

Given this, we are very concerned that DHS is prepared to hold this important VWP hostage to its goal of forcing the aviation industry to implement a US–VISIT Exit program.

I am here today representing IATA and its member airlines. However, I am also here on behalf of the 21 U.S. regional and global aviation, cruise line, and tourism associations that have joined IATA in our strong opposition to the US–VISIT Exit. This global coalition has fundamental concerns about the program as envisioned, many of which you have outlined in your previous questions.

First, IATA believes that border and immigration controls are core Government responsibilities that DHS should not be allowed to offload to the private sector. Simply arguing that fingerprints are another APIS field for airlines to fill out is both illogical and insulting. Airline employees cannot be drafted involuntarily to support what amounts to a DHS fingerprint dragnet.

Second, DHS does not have the authority to require airlines to design, implement, manage, and finance the US–VISIT Exit system. Since 1996, Congress made it clear that it wanted the U.S. Government to implement a system to better track people arriving and departing our country. Congress never gave DHS the authority to transfer this obligation to the private sector. We also believe that this program, as envisioned, would violate U.S. bilateral obligations, international law, and consumer privacy protection laws.

Third, a centralized Government collection process similar to that already trialed by DHS is vastly superior to a proposal that the airline industry collect biometrics as part of the current passenger processing system. DHS's own regulatory impact analysis favors Government-led and -financed programs.

Fourth, we believe that DHS has significantly underestimated the cost of this program to the aviation industry. Rather than $3.5 billion over 10 years, IATA estimates that it will cost airlines a total of $12.3 billion over that time period. Most of that cost increase is driven by the requirement that airlines deploy secure networks and storage facilities for what we anticipate will be between 350 and 800 times more data than is currently collected by APIS.

Fifth, as was noted earlier, industry is not in a position to fund the proposed US–VISIT Exit program. Over the next 12 months, IATA members could see an additional bill of $99 billion in fuel above that which they paid last year. Already, in 2008, we have seen 24 airlines go bust, a number we expect to grow substantially following the end of this summer travel season.

Whether it is $3.5 billion or $12.3 billion, the airline industry simply cannot afford to pay this bill. To require them to do so will only hasten the arrival of airline bankruptcies, reductions in international service, and resulting damage to the U.S. and global economy.

Madam Chairwoman, US–VISIT Exit would represent the sixth separate data exchange program that has either been implemented

or announced since 9/11. From PNR Access and APIS to the fast-approaching APIS Quick Query, TSA's Secure Flight and, most recently, ESTA, carriers are being forced to send essentially the same data about passengers to various DHS agencies at different times via nonaligned transmission formats.

Today, governments and the aviation industry are challenged more than ever to come up with the resources necessary to protect our infrastructure from threats. We can no longer tolerate Government's implementing different security programs to gather the same information on the same passengers in different ways. This is particularly galling when, as here, these programs are all being pursued independently by different agencies in the same Department.

We urge the Congress to direct DHS to harmonize all their passenger data programs to promote efficiency and reduce costs. The airlines would be pleased to consult with DHS on the best way to bring these programs together. Biometric identification should only be discussed in the context of developing such a comprehensive and consistent passenger screening system.

Then, finally, before I close, I would like to note for the record that, as you heard from Mr. Mocny earlier, DHS has not asked for the funding for this program. So absent congressional direction, they will implement a program and require the airlines to fund this program. So I urge you to consider very quick action in this regard.

Thank you.

[The statement of Mr. Lavin follows:]

PREPARED STATEMENT OF DOUGLAS E. LAVIN

JULY 16, 2008

Madam Chairwoman, distinguished Members of the subcommittee.

My name is Douglas Lavin. I am the Regional Vice President for North America for the International Air Transport Association (IATA).

IATA represents 228 carriers engaged in scheduled international transportation of passengers, mail and cargo by air. Seventy-eight of those airlines fly into and out of the United States on a scheduled basis. All of the major U.S. network carriers are members of IATA.

IATA appreciates the opportunity to brief the subcommittee on IATA's position relating to the proposal by the U.S. Department of Homeland Security (DHS) to require commercial air carriers to collect biometric data from certain foreign citizens upon exit from the United States at airports of departure (US–VISIT Exit). IATA and its member airlines are directly impacted by this DHS proposal.

IATA and its member airlines are strongly opposed to an industry-implemented and funded US–VISIT Exit program for the following reasons:

1. Border protection and immigration are core U.S. Government responsibilities that cannot be outsourced to private industry;
2. DHS does not have the legal authority to require airlines to fund this program;
3. Before introducing a new biometric collection program, DHS should harmonize its five separate and duplicative passenger data collection procedures;
4. The centralized collection by DHS of biometric data at a single point in the passenger flow is more efficient, secure and cost-effective than making significant amendments to every point of airline/passenger contact;
5. DHS has significantly underestimated the cost associated with airlines designing, implementing, running and maintaining a biometric collection process; and,
6. Airlines are not in a financial position to fund this program.

INTRODUCTION

Since 1996, Congress has on numerous occasions mandated that the Federal Government develop an entry and exit control system to collect the records of arrivals and departures of non-U.S. citizens leaving the United States. DHS' Notice of Proposed Rulemaking on US–VISIT Exit ("NPRM")[1] lists seven different laws since 1996 that call for the creation of an entry/exit program. In January 2004, DHS implemented US–VISIT as a Government-owned and -operated system and has fingerprinted over 100 million visitors entering the United States. From 2004 to 2007, US–VISIT also fingerprinted over 6.5 million visitors exiting the United States as part of the US–VISIT Exit Pilot Program. Between 2003 and 2006, DHS reports allocating $250 million for US–VISIT Exit-related efforts.

Rather than implementing this Government program on its own, DHS published an NPRM on April 24, 2008 calling for airlines to design, implement, manage and maintain a process to collect fingerprints from most foreign citizens leaving the United States by air or sea. The NPRM asked the public to provide extensive comments on the feasibility of the proposed airline collection process, a detailed review of the cost assumptions reached by DHS for this program, and any alternatives to the DHS proposed system. DHS denied more than 16 requests for a reasonable extension of time to complete these comments, offering instead the opportunity for interested parties to testify for 2–3 minutes in front of a panel of lower-level DHS technical experts.

Despite having worked on this program since 1996, the NPRM said that congressional deadlines make it imperative that DHS "establish" an Exit system by July 25, 2008 and have it up and running by July 1, 2009.[2] As discussed below, there is no congressional mandate that the airline industry meet these congressional deadlines. Indeed, it is ludicrous for DHS to now insist that the airline industry establish an Exit system 90 days after the publication of the NPRM when DHS and its predecessor agencies have failed to do so over the past 12 years. Equally troubling is the fact that US–VISIT Exit will be only one of five uncoordinated DHS passenger data collection processes that has either been implemented or proposed by DHS since 9/11.

As we demonstrate below, there are insurmountable physical, technological and financial challenges that make it impossible for the airlines to meet these unreasonable DHS demands. We therefore urge this committee and the Congress in general to step in and to prevent DHS from continuing to pursue this program as envisioned.

1. Border and Immigration Controls Are Core U.S. Government Functions

DHS has argued consistently that a US–VISIT Exit program is an essential tool in determining whether an alien has overstayed the terms of his or her visa. Indeed, in the NPRM, DHS suggests that several of the 9/11 hijackers would not have been able to carry out the attacks in the United States if a US–VISIT Exit system were in place.[3] Given this statement, it is not surprising that DHS has dedicated significant resources to develop and implement the US–VISIT program and, additionally, has initiated a 3-year trial of a U.S. Government-developed and implemented US–VISIT Exit program. We find it illogical for DHS to now propose that US–VISIT Exit, which according to DHS is a critical immigration control tool, be developed and implemented not by the Federal Government, but by untrained, ill-equipped and underfinanced airlines and their personnel. This outsourcing of core immigration and border control functions to the airline industry makes no sense and should be abandoned.

The NPRM and senior DHS officials have suggested that the collection of fingerprints by airlines is part of the cost of operating an airline in the United States and merely an extension of already existing data-gathering responsibilities under the Advanced Passenger Information System, or APIS program. However, US–VISIT Exit, as proposed in the Rule, would place new and unprecedented, onerous operational and legal obligations on carriers. Airlines and their employees cannot and should not be expected to accept these new responsibilities. Airline staff are not trained Government agents capable of undertaking law enforcement duties and air-

[1] Collection of Alien Biometric Data Upon Exit from the United States at Air and Sea Ports of Departure; United States Visitor and Immigrant Status Indicator Technology Program ("US–VISIT"), 73 Fed. Reg. 22065.

[2] According to the DHS NPRM, Section 711 of the 9/11 Recommendations Act directs DHS to establish an exit system within 1 year of enactment (July 25, 2007). It also notes that the DHS Secretary loses the ability to waive restrictions on the Visa Waiver Program (VWP) if it does not have the US–VISIT Exit system operational by July 1, 2009. 73 Fed. Reg. 22068.

[3] 73 Fed. Reg. 22066.

lines do not have the systems in place to meet the transmission, security and storage requirements set forth in the DHS proposal. DHS' own Regulatory Impact Analysis (RIA) demonstrates that U.S. Government-led and financed alternatives enjoy a better cost-benefit outcome than the carrier-led proposals outlined in the NPRM.[4] These Government-led alternatives also optimize data privacy and IT security and, depending on the alternative, minimize disruption to the passenger and the carrier. Simply passing off a bad proposal as a "cost of doing business" is not acceptable, particularly given DHS' own regulatory impact analysis.

2. DHS Does Not Have the Authority To Outsource This Program

There is no law, regulation, report language or congressional suggestion that US–VISIT Exit should be designed, implemented, managed and funded by the airline industry. Instead, the language of the laws cited by DHS as justification for their effort to outsource this core Government function makes it clear that the U.S. Congress intended DHS to be responsible for all aspects of the Exit program.

For example, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), states that "completing a biometric entry and exit data system as expeditiously as possible [was] an essential investment in efforts to protect the United States by preventing the entry of terrorists."[5] It seems logical to assume that had the Congress decided that the private sector should bear the cost and responsibility for this "essential investment," it would have drafted the law in such a way that would expressly and unequivocally reflect that intention. In fact, the same law states that "the [DHS] shall operate the biometric entry and exit system . . .".[6] The IRTPA does not include any language providing for a delegation of this statutory obligation in favor of third parties, which would be required before any such delegation takes place.

DHS argues that its authority to require airlines to fund US–VISIT Exit stems from Congress' requirement that airlines collect and provide DHS specific passenger manifest data under Section 231 of the Immigration and Naturalization Act.[7] However, DHS offers no legislative language or history to suggest that when Congress authorized DHS to require airlines to collect APIS information that it also authorized the collection of fingerprints from outgoing passengers. To the contrary, Congress passed separate legislation directing DHS (and no one else) to establish a US–VISIT program, distinct from the APIS program. IATA strongly believes that the inherent differences between the airlines' collection of biographical APIS information and the collection and transfer of fingerprints are significant enough that specific congressional authorization is required before moving forward with this program. Unlike APIS information, which is flight-specific, biometric information would be stored for up to 75 years and could potentially be used to impose sanctions during "subsequent encounters" with U.S. Government officials.[8] From a technical, operational and privacy perspective, this proposal envisions a totally new collection process that cannot be reasonably justified as simply another data element to be collected by the airlines.

In addition to a lack of any U.S. law authorizing outsourcing of this core Government function, DHS' proposal also raises significant implications in terms of U.S. bilateral and multilateral obligations. From a bilateral perspective, IATA believes that the transfer of responsibility outlined in US–VISIT Exit is contrary to the spirit of most U.S. air services agreements as it would, in effect, compel air carriers operating in this country to provide additional services and facilities, such as border control, that are an inherent Government responsibility. This would have the same effect as imposing unreasonable user charges on air carriers, something not allowed under our bilateral air agreements. On the multilateral level, ICAO has developed standards and recommended practices in the field of facilitation (Annex 9) that are binding upon all Contracting States to the Chicago Convention. Those internationally agreed provisions stipulate that facilities used for clearance controls should be provided at public expense.[9] In contrast, under the DHS proposal, carriers would have to procure the space and facilities at their own expense to carry out border control duties. Finally, one cannot discount the possibility that the DHS program as envisioned would violate a number of jurisdictions' data privacy laws, including EU Directive 95/46/EC which provides significant protections for passengers from this type of intrusive data collection. Further, airlines are not in the position to ac-

[4] Air/Sea Biometric Exit Project Regulatory Impact Analysis, April 17, 2008, at 80.
[5] Public Law 108–458, 3827 (December 17, 2004).
[6] Id at 3821.
[7] 8 USC 1221(c)(10).
[8] 73 Fed. Reg. 22067, 22071.
[9] Annex 9, Facilitation, Chapter 6, Section 6.58.

cept the liability associated with the collection and storage of this most highly private, personal data. Additionally DHS does not address the issue of refusal by a passenger—because of data privacy concerns—to give their biometric to an individual airline employee rather than to a Government agent.

3. Harmonize the Five Passenger Screening Programs

Since September 11, 2001, five separate passenger data exchange programs have been either initiated or announced by various DHS agencies. From PNR Access and APIS to the fast-approaching APIS Quick Query, TSA's Secure Flight and, most recently, the Electronic System for Travel Authority (ESTA)—carriers are being forced to send essentially the same data about passengers to various DHS agencies at different times and using non-aligned transmission formats.

In reality, each of these programs has essentially the same goal—enabling DHS to know more about passengers arriving in and departing from the United States. Unfortunately, as each program has been developed independently and has been designed to respond to a very narrow objective, little attention has been paid to ensuring that data being submitted under one regulation can or is used to satisfy requirements imposed under another.

We believe that it is time for DHS to reevaluate and rationalize its regulatory structure relating to passenger data exchange program requirements. The potential for up to five wholly separate programs designed to collect essentially the same data concerning the same passengers simply cannot be justified in today's environment of linked systems and instant communication. For the air transport industry, the costs—in terms of program development and operational impact—can no longer be borne at a time when both U.S. and foreign-flagged carriers are struggling for economic survival.

It is now time for a change in approach. We implore DHS to join with the industry to optimize and consolidate existing passenger data exchange systems and to ensure the most efficient use of carrier provided data, instead of continuing to introduce entirely independent niche programs. Biometric identification should only be discussed in the context of developing such a comprehensive passenger-screening rule.

4. Centralized Collection by DHS at a Single Point in Passenger Flow

Despite the fact the DHS RIA favors a Government biometric collection system, DHS proposes to require airlines to include this collection as part of the passenger check-in and/or boarding process. DHS justifies this conclusion in part by indicating they found it difficult to collect biometrics effectively during their 3-year US–VISIT Exit Pilot program. However, even a cursory review of the impact an Airline-implemented US–VISIT Exit program would have on airline passenger processing demonstrates that the introduction of biometric collection during the existing passenger check-in and boarding process would have significant negative impact on international air travel:

- *Airline check-in desk*.—IATA estimates it will take at least 1–2 minutes to collect a set of fingerprints, increasing processing time by up to 50 percent for those affected by the requirement and thereby lengthening line wait times for all passengers, regardless of nationality. Additionally, this delay raises airport capacity concerns and could result in increased security threats to passengers in the non-secure area of the airport.
- *Boarding gate*.—Airport boarding gates are not designed for the collection of additional passenger information. Adding any additional processes, such as biometric collection, would result in unacceptable delays.
- *Kiosk check-in*.—IATA and its member airlines have spent millions of dollars in recent years to automate the check-in process. Self-service check-in kiosks are increasingly the norm at U.S. airports, including for use by international passengers, and do not require the need for intervention by airline staff. Introduction of a biometric collection process here would disrupt the efficiency gains resulting from this self-service process.
- *Remote check-in*.—Today, as a result of airline technology investments and Web access, a growing percentage of passengers (domestic and international) check-in online, check their baggage via a common airport collection site, and interact directly with airline personnel only when presenting themselves for boarding at a gate. Requiring airlines to collect biometric information as part of this process will negate the positive impact self-service check-in has on the airport environment, the passenger experience, the efficiency of international aviation and U.S. competitiveness in that system.

DHS should implement a system, under Government control, that allows for the collection of biometrics at a single point in the passenger flow. A Government-run

biometric data collection process should utilize the existing infrastructure already in place at the 119 U.S. Airports where US–VISIT arrival processing occurs. We believe there are two alternative approaches that DHS can consider in this regard. In each of the following scenarios, additional benefits ensue once DHS consolidates its internal data systems to provide for real-time response.

Central Kiosks

As tested over a 3-year period, centrally located US–VISIT Exit registration kiosks in each of the 119 airports where US–VISIT is active today would provide for fairly widely disbursed collection of biometric data, and would respond effectively to concerns that biometrics should be collected only at the airport from which U.S. departure occurs. In addition to fixed kiosk installations, this method could also be supplemented by mobile registration facilities that could be located immediately adjacent to international departing flights. A centralized collection is efficient in many ways—the number of collection points is vastly reduced, thus providing a secure, cost-effective mode of data collection.

TSA Security Screening Points

Another option would be to incorporate biometric data collection as part of the TSA Security Screening Point activity. There are several benefits to this approach:

- TSA Infrastructure is already in place at all airports;
- All persons entering the aviation system at a U.S. airport could be checked;
- Collection at TSA Security Screening locations at all domestic and international airports, or at least in the 119 U.S. airports where US–VISIT is currently operating, would spread the impact of data collection across more airport facilities;
- Final APIS (or AQQ) manifests would confirm actual departure.

IATA believes that either approach described above effectively responds to the congressional mandate, which is to implement a biometrically based entry and exit system that can identify those who have violated the terms of their visas.

5. DHS Has Significantly Underestimated the Cost of Implementing This Program

The US–VISIT Exit NPRM estimates that carriers would incur costs ranging from $3.5 billion to $6.4 billion to fund the proposed US–VISIT Exit program. Unfortunately, DHS does not offer any methodology or expense categories to fully justify their calculations.

IATA has worked with our member airlines, network service providers and hardware manufacturers to scope out the cost of both the NPRM and the additional requirements set forth in the associated RIA. IATA believes that the proposed rule could cost the airline industry as much as $12.3 billion over 10 years. This represents an increase of approximately $5.9 billion above the highest 10-year cost estimate by DHS. A complete accounting of IATA's $12.3 billion estimate is attached at the end of this testimony.

One of the critical erroneous assumptions contained in the NPRM is the apparent DHS belief that airline networks have the same data transmission capabilities as Internet-based networks. In fact, airlines maintain or lease highly specialized networks, which are optimized to transmit character-based data and are not capable of transmitting biometrics. Thus, DHS' assumption that you could simply upgrade existing airline networks to support fingerprint transmission is incorrect.

In addition to this fundamental misunderstanding of airline networks, we are particularly concerned about three critical costs omitted by DHS in the NPRM:

- *Data transmission*.—Under this NPRM, carriers would be required to transmit 350 to 800 times more data to the U.S. Government per flight than is currently being transmitted to support the APIS program. IATA estimates that each year, impacted airlines would have to spend an additional $750 million to transmit the additional data.
- *Dedicated secure networks*.—The PIA indicates that DHS will require the airlines to operate secure and encrypted data transmission lines for the fingerprints. Airlines currently do not have this capability between airports and each airline's DCS and overseas data processing facilities. IATA estimates the installation and maintenance of these additional secure connections will exceed $150 million over 10 years.
- *Specialized secure data warehouses*.—The PIA indicates that DHS will also require airlines to operate secure fingerprint storage data warehouses to hold the fingerprints prior to their being transmitted to the U.S. Government. These facilities would need physical security and access controls, back-up capabilities and specialized data encryption hardware and software—costs for which that are not accounted by DHS in the NPRM. We estimate it will cost over $1 billion over 10 years to build, equip, connect and operate these warehouses.

The DHS regulatory impact analysis estimates that the gross 10-year benefits of US–VISIT Exit would be approximately $1.09 billion. Given DHS's own estimate of a $3.5 billion cost over 10 years, one must question how you could reasonably conclude that DHS has met the regulatory requirement for a sustainable cost/benefit analysis. This analysis becomes even less sustainable when you consider the 10-year cost is likely closer to IATA's $12.3 billion estimate.

6. Airlines Cannot Fund This Program

As noted above, IATA believes DHS has significantly underestimated the cost of the proposed US–VISIT Exit program. However, while one can argue whether the cost of the program would be $3.5, $6.4 or $12.3 billion over 10 years, no one can reasonably argue that the airline industry can afford to fund any such U.S. Government program.

The airline industry is today facing an unprecedented crisis with the advent of dramatically increasing fuel prices. IATA airlines are expected to face an additional financial burden of $99 billion over the next 12 months over our 2007 fuel bill. Furthermore, 24 airlines have ceased operations or filed for bankruptcy in the last 5 months, and many more are expected not to survive the year. Softening demand has also increased the impact of this crisis, and airlines have not been able to recoup oil costs in revenue. In the last 4 months, the 2008 financial forecast for the global industry has swung from a $5 billion profit to a $2.3 billion loss. IATA has called on governments around the world to refrain from imposing unnecessary and punitive costs on the industry. Any additional costs to the industry will only cause further, irreparable damage to cost management practices, to bottom lines and to the survivability of the industry.

In the best of times, airlines are limited in their ability to pass increased security costs on to their passengers. There is no business model one could envision that would allow airlines to pass between $3.5 and $12.3 billion onto their passengers to support fingerprint collection. Instead, if DHS is successful in outsourcing this Government program, we can expect this cost to increase the likelihood of airline bankruptcy (Chapter 11 and Chapter 7) and a reduction in international service from the United States. Today, the international airline industry contributes $3.5 trillion, or 7.5 percent, of global GDP and generates 32 million jobs. Is this the time to threaten this economic engine in order to alleviate DHS of its statutory mandate?

CONCLUSION

IATA appreciates the fact that DHS has been directed by the U.S. Congress to implement a system to collect biometric information from passengers as they leave by air or sea. IATA also accepts that collection of this information could provide some benefit in terms of border control. However, IATA cannot accept a proposal that suggests that the airline industry should take on this core Government function, particularly at a time when airlines are facing a financial crisis deeper than has been seen since before 9/11. We strongly urge DHS to withdraw this proposal and to work with Congress and industry to find a more reasonable solution to meet this border control data requirement.

First Year and Recurring Annual Costs of the DHS Proposed US Exit System
Composed by the International Air Transport Association

Expense Area	Description	First Year Costs	Recurring Annual Costs	Details
Data Transmission	Cost to transmit fingerprints from airline to US Government	$750,420,000	$750,420,000	**Current 3rd party vendor cost per passenger to transmit APIS data = $.036** **Estimated cost per passenger to transmit fingerprints = $22.74** (Basis: new transmission would be 350-800 times the size of data currently being transmitted) Estimate includes the cost of 3rd party vendor upgrading their networks
Hardware Acquisition	Purchase of fingerprint readers	$57,816,000		Estimates 9636 readers required at $6000/unit
Installation/Retro-Fit	Electrical rewiring and modification of counters/gates/kiosks	$19,272,000		
Secure Transmission Lines	New networks from airports to DCS	$75,000,000	$7,500,000	Includes ownership, leasing and maintenance
Separate Secure Storage	Data warehouse for fingerprint storage	$1,000,000,000	$200,000	Not included in DHS NPRM but required by DHS privacy office Recurring annual cost of $200,000 required for maintenance
Programming Enhancements	Cost to rewrite APIS systems to include biometrics	$64,000,000		
Additional Infrastructure	Departure delays, increased staffing, staff training	$300,000,000	$300,000,000	
Separate Biometric Transmission System	Cost due to carriers' need to build standalone systems	$500,000,000		Additional developmental and hardware costs if airline fingerprint data networks can not be integrated with APIS network system
	Total Costs per Annum	**$2,766,508,000**	**$1,058,120,000**	
	Total Cost Over 10 Years	x1	x9	Recurring annual costs are multiplied by 9 signifying the remaining nine years after the first year, thereby making 10 total years
		$2,766,508,000	$9,523,080,000	
		$12,289,588,000		Equals first year costs plus recurring annual costs for nine years

Ms. SANCHEZ. Thank you, Mr. Lavin.

Now Mr. Principato for 5 minutes.

STATEMENT OF GREG PRINCIPATO, PRESIDENT, AIRPORTS COUNCIL INTERNATIONAL—NORTH AMERICA

Mr. PRINCIPATO. Thank you, Chairwoman Sanchez, Ranking Member Souder, for the opportunity to testify on behalf of Airports Council International—North America.

We applaud both this subcommittee and the full committee for your work on the Visa Waiver Program and oversight of the proposed implementation of US–VISIT Exit. The requirement to verify the departure of foreign visitors who exit by air is a worthy goal that we support. However, we do not support the recent DHS proposal that airlines collect the biometrics of foreign visitors as they are departing the United States. This is an inherently governmental function that DHS should perform and fund.

The implementation of US–VISIT Exit is not only a challenge to air carriers; it is a serious challenge to airports. ACI—North America believes the adoption of six principles would create the best approach to a US–VISIT Exit system.

Principle No. 1: This is a DHS responsibility. Immigration and border control functions are inherently Government responsibilities. US–VISIT Exit is an immigration enforcement program. It should, therefore, be operated and staffed directly by DHS on a contractual program similar to the TSA screening partnership program.

Principle No. 2: It should be federally funded. We associate ourselves with Mr. Lavin's final comment there. DHS must secure additional staffing and funding resources to implement the program. Both TSA checkpoints and CBP arrival inspections already suffer from understaffing, congestion, and often unacceptable wait times. Shifting personnel from these functions to US–VISIT Exit will place an unacceptable additional strain on an already stressed system.

Principle No. 3: We believe that collection should occur at the final point of departure. This would greatly reduce the costs of the program by limiting the number of airports at which DHS needs to place biometric collection equipment. DHS acknowledges that such a system would reduce the number of impacted airports from 450 to 73. Likewise, this will reduce the number of air carriers impacted from 268 to 138 and, we believe, would be a more effective use of DHS resources.

Principle No. 4: The collection should occur in a sterile area to ensure the security and integrity of the US–VISIT Exit system. Conducting the exit process in a sterile area decreases the impact on those passengers who are not subject to US–VISIT Exit rules and ensures that those passengers connecting to their last point of departure from a domestic flight do not have to leave the sterile area in order to comply.

Principle No. 5: There should be consultation with airport proprietors and airlines. U.S. airports were not designed or constructed to accommodate such a departure process for foreign visitors. Cooperation between DHS and the aviation industry is vitally important for the success of the program.

Principle No. 6: We believe that fingerprint collection should be accomplished via mobile devices and should not be hardwired, which will permit them to be quickly and easily relocated should airport or airline operations necessitate a change of gate. Many gates are used for both international and domestic departures depending on the carrier and the time of day, and it is important that the US–VISIT Exit program is able to easily respond to changing situations. Mobile devices would reduce costs and increase efficiency, as well as minimize the impact on airport facilities.

Also, importantly, we recognize that once US–VISIT Exit is implemented, there may be changes to the program based on lessons learned. In light of this possibility, DHS should not take an approach which will require costly facility changes to implement those lessons learned.

In closing, ACI—North America would urge that DHS undertake an extensive public outreach and education campaign about the new Exit requirements when the final rule is issued. The economic benefits, as you have already discussed, from international visitors traveling to the United States are significant, and there are political benefits as well. We must ensure that US–VISIT Exit is an efficient system that does not endanger continued travel and tourism to our country.

ACI—North America and our member airports look forward to working with you as we move forward on this important program. Thank you again for this opportunity.

[The statement of Mr. Principato follows:]

PREPARED STATEMENT OF GREG PRINCIPATO

JULY 16, 2008

INTRODUCTION

Chairwoman Sanchez, Ranking Member Souder, thank you for the opportunity to testify before you today on behalf of Airports Council International—North America (ACI–NA). My name is Greg Principato and I serve as the President of ACI–NA. ACI–NA represents State, local, and regional government entities that own and op-

erate commercial service airports in the United States and Canada. ACI–NA member airports enplane more than 95 percent of the domestic scheduled air passenger and cargo traffic and virtually all scheduled international air traffic in North America. In addition, nearly 400 aviation-related businesses are also members of ACI–NA.

VISA WAIVER PROGRAM

We applaud both this subcommittee and the full committee on Homeland Security for its work on the Visa Waiver Program and oversight of the proposed implementation of US–VISIT Exit. Although a majority of my testimony today is dedicated toward US–VISIT Exit, it is important that I also take a moment to comment on the larger Visa Waiver Program, or "VWP," as it is commonly known, which has developed into a vital contributor to our Nation's economy.

To this end, ACI–NA is concerned regarding the potential suspension of the Secretary of Homeland Security's waiver authority to expand the VWP on July 1, 2009 if the biometric air exit system is not fully in place. The Department of Commerce ranks international travel as one of the United States' largest exports, exceeding even agricultural goods and motor vehicles. This includes money spent by international travelers on lodging, food, goods, services, gifts, and recreation. Travel receipts for 2006 were $107.4 billion, with more than $50 billion of that coming from 18 million VWP participants. In fact, of the top ten countries in expenditures in the United States, six were VWP participants in 2006. While we understand that existing VWP countries would not have their privileges revoked should the Department not meet the July 2009 deadline, we are concerned that the program would not grow. As Assistant Secretary Richard Barth testified on May 14 before the House Foreign Relations Subcommittee on Europe, the economic benefits of the Visa Waiver Program apply to each of this country's 50 States and will continue to grow as the program expands.

US–VISIT EXIT

The requirement mandated by the 9/11 Act of 2007 to verify the departure of foreign visitors who exit the United States by air is a worthy goal supported by ACI–NA. We understand the pressures that DHS is operating under to meet the mandate of the 9/11 Act to have a biometric exit system in place. Airports are prepared to partner with the airlines, with Congress, and with DHS in this endeavor as it is vitally important to ensure that there is a system in place to determine whether or not a foreign visitor has overstayed the terms of his or her visa or other travel authorization.

However, ACI–NA does not support the Department of Homeland Security's (DHS) recent proposal that airlines collect the biometrics of foreign visitors as they are departing the United States. DHS should perform the inherently governmental function of collecting the biometrics, implementing the system, and funding the associated costs. Additionally, airlines are simply unable to assume this substantial financial burden, especially in the current economic climate. For these reasons, it is now more important than ever before that airports, airlines, and the U.S. Government work together.

Additionally, we are concerned that DHS has no current plans for implementation of an equivalent biometric exit system at U.S. land borders. This will create a problem for visitors who arrive in the United States by air but depart via the land border to Canada or Mexico. For example, a foreign visitor may arrive in the United States by air, travel to Canada by car, and then return to their home country by air from Canada. As currently constructed, that visitor would likely be flagged as not having properly "checked-out" if they return to the United States on a subsequent trip. ACI–NA believes it is important that before an exit system is implemented, DHS must establish a protocol for how visitors in such circumstances could demonstrate their compliance with US–VISIT Exit procedures. Without a clear protocol, foreign visitors may face delays, confusion, or may be denied entry into the United States through no fault of their own. This clearly shows we must be conscientious in our approach and ensure that US–VISIT Exit does not degrade the travel experience of visitors to the United States to the detriment of the U.S. aviation industry, local and national economies, and the public image of the United States.

DHS COLLABORATION WITH INDUSTRY IS CRITICAL

ACI–NA, along with the rest of the aviation industry, has expressed strong concern over the lack of communication that occurred between DHS and industry stakeholders during the development of the recent Notice of Proposed Rule Making

(NPRM) entitled, "Collection of Alien Biometric Data Upon Exit from the United States at Air and Sea Ports of Departure." It is critical that we return to the level of frequent and productive communication that existed between the US–VISIT Program Office and the aviation industry during the earlier rollout of the US–VISIT Exit pilot program as the Department seeks to implement this important border security tool.

AIRPORT PERSPECTIVE/ACI–NA SIX PRINCIPLES FOR US–VISIT EXIT

The implementation of US–VISIT Exit is not only a challenge to air carriers; it is also a serious challenge to airports. We have a vested interest in seeing US–VISIT Exit implemented in an efficient, effective, and timely manner. Any solution by DHS must therefore be pursued in full consultation with airports, airlines, and other interested parties.

Unfortunately, there are no easy solutions to capturing the fingerprints of departing foreign visitors at U.S. airports. However, ACI–NA believes that the adoption of six principles would create the best approach to a US–VISIT Exit system.

PRINCIPLE NO. 1—DHS RESPONSIBILITY

First and foremost, we believe that immigration and border control functions are inherently governmental responsibilities. US–VISIT Exit is an immigration-enforcement program which would serve to confirm, based on biometric information, that foreign visitors to the United States depart in accordance with their visas or other authorizations for being in the United States. It should therefore be operated and staffed directly by DHS or in a contractual program similar to the Transportation Security Administration Screening Partnership Program, or "SPP."

PRINCIPLE NO. 2—FEDERALLY FUNDED

Second, all costs associated with procurement, implementation, operation, maintenance, and staffing of the program must be borne by the Federal Government, reflecting the national interest of the program. DHS must secure additional staffing and funding resources to implement the US–VISIT Exit process in order to avoid diverting Transportation Security Administration (TSA) or Customs and Border Protection (CBP) officers from their current duties at U.S. airports. Both TSA checkpoints and CBP arrival inspections already suffer from understaffing, congestion, and often unacceptable wait times. Shifting personnel from these functions to US–VISIT Exit will place an unacceptable additional strain on an already stressed system.

PRINCIPLE NO. 3—LAST POINT OF DEPARTURE

Third, the collection of biometrics from departing foreign visitors should take place at the airport where the traveler is ultimately departing the United States, or what we refer to as the "last point of departure." This would greatly reduce the costs of the program by reducing the number of airports at which DHS needs to place biometric collection equipment and staff to only those with non-stop international service. According to DHS, such a system would reduce the total number of impacted airports from 450 to 73. Likewise, this will reduce the number of air carriers impacted from 247 to 138. By only collecting biometrics at the last point of departure, the entire process will become more streamlined and consistent, helping to eliminate confusion for those visitors who will go through the exit process.

PRINCIPLE NO. 4—STERILE AREA

Fourth, fingerprints should be collected from departing visitors within the sterile area of an airport to ensure the security and integrity of the US–VISIT Exit system. Conducting the exit process in the sterile area decreases the impact on those passengers who are not subject to US–VISIT Exit rules and ensures that those passengers connecting to their last point of departure from a domestic flight do not have to leave the sterile area in order to comply.

PRINCIPLE NO. 5—CONSULTATION WITH AIRPORT PROPRIETORS AND AIRLINES

ACI–NA believes that it is critical that DHS consult with airport proprietors and airlines prior to the determination of specific solutions. U.S. airports were not designed or constructed to accommodate a departure process for foreign visitors. Such cooperation is vitally important for the success of the program not only for individual airports but for the entire US–VISIT Exit system.

PRINCIPLE NO. 6—COLLECTION VIA MOBILE DEVICES

Finally, we believe that the devices used to collect fingerprints should be mobile and should not be "hard-wired," which will permit them to be quickly and easily relocated should airport or airline operations necessitate a change of gate. Many gates are used for both international and domestic departures depending on the carrier and time of day, and it is important that the US–VISIT Exit program is able to easily respond to changing situations. Mobile devices would reduce costs and increase efficiency, as well as minimize the impact on airport facilities. Also importantly, we recognize that once US–VISIT Exit is implemented, there may be changes based on lessons learned. In light of this possibility, DHS should not take an approach which will require structural changes.

CONCLUSION

In closing, ACI–NA would urge that DHS undertake an extensive public outreach and education campaign about the new exit requirements when the final rule is issued. The economic benefits from international visitors traveling to the United States are significant, both for airports and for the U.S. economy. We must ensure that US–VISIT Exit is an efficient and effective system that does not endanger continued travel and tourism to our country.

ACI–NA and our member airports hope to work closely with this subcommittee and with the Department on this important program.

Ms. SANCHEZ. Thank you, sir.

Now we will hear from Mr. Sales for 5 minutes or less.

STATEMENT OF NATHAN A. SALES, ASSISTANT PROFESSOR OF LAW, GEORGE MASON UNIVERSITY SCHOOL OF LAW

Mr. SALES. Chairwoman Sanchez, Ranking Member Souder, and Members of the subcommittee, thank you for the opportunity to be here today to testify before you.

I would like to begin with a few thoughts on the continuing need to modernize the Visa Waiver Program. As you know, the 9/11 Act changed the program in two important ways.

First, it added a number of new tough security requirements to the program. Second, the legislation made it possible for certain close American allies to join the program for the first time. We have heard today that the administration has begun to make great progress in implementing these changes. It should continue to do so, and quickly.

Expectations in the roadmap countries are now extremely high.

Madam Chairman, you asked earlier in the hearing about delay. If American policymakers begin to get cold feet, these allies justifiably will feel that the United States has pulled the rug out from under them. That would be worse than if the reforms had never been enacted at all. This is no time to go wobbly.

Diplomatic considerations are important, but to my mind, they are secondary. What matters most is national security. Until the new security measures are deployed, the Visa Waiver Program will continue to represent a glaring vulnerability in this Nation's defenses. Consider convicted al Qaeda member Zacarias Moussaoui is a citizen of France. Shoe Bomber Richard Reid is a Briton. The attempted Heathrow bombers all held British passports. Each of them was able to exploit the Visa Waiver Program to fly to this country with little, if any, advanced scrutiny. DHS needs to act quickly to bring the new security requirements on line.

Next, let me say a few words about the other side of the coin, exit. Frankly, exit controls are less vital than entry controls. It is

more important to know whether we are keeping terrorists out of the country than to know whether terrorists have left the country.

So why develop an exit system at all? Well, for starters, that is what the law requires. Congress has been calling for a system that can track departures from this country at least since 1996. In the 9/11 Act, Congress began to turn up the heat. DHS is now required to deploy a biometric exit system by August 3 of this year. If it fails to do so by the following July, it can't add any new countries to the Visa Waiver Program.

Congress has been waiting for US–VISIT Exit a long time, and its impatience is understandable. But there are also sound policy reasons for exit controls. US–VISIT Exit helps Federal officials enforce the immigration laws. If authorities know that an alien previously overstayed his welcome in the United States, they can stop him if he later tries to return to the country. It is also conceivable that officers could use exit data in conjunction with other information to track down overstays who are still here and have them deported.

US–VISIT Exit isn't just about immigration; it is also about national security. According to the 9/11 Commission, at least three of the September 11 hijackers previously had overstayed in the United States, including Mohamed Atta, the plot's operational ring leader. If border officials had known this when those hijackers returned, they might have been turned away.

Finally, I would like to discuss the role of airlines and other private sector entities in DHS's new biometric system. My sense is the proposal doesn't break a whole lot of new ground. Instead, builds on existing legal rules that already direct carriers to compile different types of information and to share that information with the Government.

For instance, the law already requires airlines to collect and share a passenger's full name, birth date, gender, passport number, visa number, and a fairly wide range of other personal information. DHS is simply proposing to add another type of data to the list, fingerprints.

It might be appropriate to ask airlines to play a role, but that doesn't mean the airlines should be stuck with the tab. You have already heard today that the bill for US–VISIT Exit could run from $3.5 billion on the low end to as high as $12.3 billion. That is billion with a "B." In an era of record fuel prices and looming airline bankruptcies, it seems gratuitous to pile new costs on the travel industry.

If airlines help the Government track departures, the least the Government can do is help airlines foot the bill. There are at least as many ways to do that as there are people in this room. One approach would be for carriers to offset their costs by raising their rates. Or, Congress might authorize carriers to impose a separate exit surcharge, something like the 9/11 security fee. A third option would be for Congress to appropriate funds to reimburse airlines' costs.

Madam Chairwoman, thank you again for the opportunity to testify today. I would welcome any questions.

[The statement of Mr. Sales follows:]

PREPARED STATEMENT OF NATHAN A. SALES

JULY 16, 2008

Chairwoman Sanchez, Ranking Member Souder, and Members of the subcommittee, thank you for inviting me to testify on this important issue. My name is Nathan Sales. I am a law professor at George Mason University School of Law, where I teach national security law and administrative law. Previously, I was Deputy Assistant Secretary for Policy Development at the United States Department of Homeland Security. The views I will express today should not be attributed to any past or present employer or client.

My testimony will discuss the important steps that Congress and the administration have begun to take to secure the Visa Waiver Program, or VWP, against terrorists who might exploit it to gain entry to the United States. Among the most important new security standards are the measures that provide DHS with advance information about persons who are traveling to the United States from VWP countries. I also discuss DHS's efforts to develop an exit system capable of tracking whether or not visitors to this country have departed on time. In particular, I will examine some of the reasons to deploy exit controls, including their potential benefits for immigration enforcement and national security. Finally, I will consider what role private sector entities such as airlines should play in tracking alien departures, and will offer some suggestions to improve the DHS exit proposal.

I. TERRORIST TRAVEL AND THE VISA WAIVER PROGRAM

Before turning to the Department's specific biometric exit proposal, I'd like to spend a few moments discussing a more general issue: Congress's efforts to modernize the Visa Waiver Program and the recurring problem of terrorist travel. The VWP has served the United States and our allies well since Congress first established it on a pilot basis in the late 1980's.[1] The program was designed to encourage travel between this country and our partners, thereby spurring trade, economic growth, and cross-cultural interactions. It has lived up to Congress's expectations. Originally limited to just two members—Japan and the United Kingdom—the VWP was made permanent in 2000[2] and now includes nearly 30 countries, mostly in Western Europe but also around the Pacific region.[3] In 2007, some 13 million people entered the United States under the Visa Waiver Program.[4]

Despite its successes, the VWP in many ways is a relic of the September 10 world. The program suffers from two major flaws. First, it slights some of the United States' closest allies in the war on terrorism. Countries like the Czech Republic, Estonia, Poland, and South Korea have been steadfast partners in America's efforts to keep al Qaeda at bay. Yet these and other nations are unlikely to satisfy the statutory criteria for VWP membership in the foreseeable future. A country is not eligible to join the program unless, among various other requirements, it achieves a nonimmigrant visa refusal rate of 3 percent or lower.[5] (A country's visa refusal rate aggregates decisions by State Department consular officials on whether to grant visas to citizens of that country; it is a rough way of measuring the likelihood that a country's citizens might overstay in the United States.) Because some U.S. allies' visa refusal rates exceed 3 percent, their immediate prospects for membership are dim.

Even more importantly, the VWP's security standards are inadequate in an era of global terrorism. The 9/11 Commission has emphasized that, for terrorists, the ability to travel is "as important as weapons."[6] Yet the VWP was not designed as a national security tool. Instead, its traditional focus has been the threat of illegal economic migration—i.e., the risk that citizens of less prosperous nations might relocate to the United States in search of better financial prospects. Moreover, to the extent the VWP does try to measure security risks, the manner in which it does is quite imprecise. The program screens for threats on a country-by-country basis, not a passenger-by-passenger basis. In other words, it assumes that citizens of non-

[1] See Pub. L. No. 99–603, § 313, 100 Stat. 3359 (1986).

[2] See Visa Waiver Permanent Program Act, Pub. L. No. 106–396, 114 Stat. 1637 (2000).

[3] The 27 VWP members are: Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

[4] See Government Accountability Office, Report No. GAO–08–458T, *Visa Waiver Program: Limitations With Department of Homeland Security's Plan To Verify Departure of Foreign Nationals* 4 (2008).

[5] See 8 U.S.C. § 1187(c)(2)(A).

[6] *The 9/11 Commission Report* 384 (2004).

members represent a greater security risk, and that citizens of members pose a lesser risk.

Experience since 9/11 shows how wrong, and dangerous, those assumptions are. The terrorist threat from Western Europe—which accounts for the bulk of the VWP's membership—is chillingly real. Convicted al Qaeda member Zacarias Moussaoui is a citizen of France. Shoebomber Richard Reid is a Briton. The men who allegedly plotted to bomb planes flying between London's Heathrow airport and the United States held British passports. All of them could have exploited—and in some cases did exploit—the Visa Waiver Program to fly to this country with little, if any, advance scrutiny.

Fortunately, Congress and the administration have been working together to remedy these shortcomings. Last year, as part of the 9/11 Act, Congress enacted legislation that adds seven new security features to the VWP; it also gives DHS more flexibility to admit countries that have not reached the 3 percent visa refusal rate requirement.[7] Critically, DHS has announced its intention to apply the new security standards not just to aspiring members—the so-called "roadmap" countries—but to current participants as well. That seems reasonable from a fairness standpoint. VWP members should be subject to the same standards regardless of whether they happened to join the program in 1989 or in 2009. It seems even more reasonable from a threat standpoint. Western Europe is home to significant and increasingly assertive populations of radicals, and it is here that the new security measures have the potential to do the most good.

While each of the new requirements is important, my sense is that the most vital of all are the ones that provide DHS with more information about passengers flying to the United States. Unlike ordinary travelers, citizens of VWP members are not required to complete detailed visa application forms. They don't participate in interviews with consular officials. And there is no requirement that they provide fingerprints before traveling. As a result, authorities know very little about them before they arrive at a port of entry, seeking to be admitted to this country.

The VWP reforms help close that information gap. For instance, Congress has directed DHS to create an Electronic System for Travel Authorization, or ESTA. ESTA is modeled on a system pioneered by Australia more than a decade ago, and it enables visitors to give U.S. authorities certain basic information before they travel—for instance, their names, nationalities, passport numbers, and other types of data passengers currently provide when they complete a Form I–94 upon arrival in the United States. DHS can run this information against watch lists of known or suspected terrorists or analyze it to find ties between known terrorists and their unknown associates. The 9/11 Act also calls on VWP members to share more information about U.S.-bound travelers, such as their own terrorist watch lists, airline reservation data, and information about suspects who are wanted in those countries for serious crimes. By enriching the data available to U.S. border officials, the 9/11 Act enables them to make better decisions about which passengers should be allowed to board flights for this country, and which should not.

II. US–VISIT EXIT: LAW AND POLICY

Since 2004, the Department's US–VISIT program has overseen the collection of biometric identifiers—fingerprints and digital photographs—from most aliens who arrive at air or sea ports of entry.[8] In April of this year, the Department issued a Notice of Proposed Rulemaking outlining its plan to collect biometrics from aliens who are exiting the United States by air or sea.[9] Under the DHS proposal, airlines and other carriers would be responsible for taking the fingerprints of departing aliens and transmitting them to DHS within 24 hours of their departure. DHS would match the data against entry records to verify whether aliens who were admitted to the United States left on time.

Exit controls are not as vital as entry controls. It is more important to prevent a terrorist from entering the United States than to know whether a terrorist has left. So why develop an exit system at all? The short answer is: Because Congress has required one. In fact, Congress has been calling for a system that can reliably track the departures of foreign visitors for more than a decade. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 directed the Attorney Gen-

---

[7] See Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 711, 121 Stat. 266, 339 (2007).

[8] See *Implementation of the United States Visitor and Status Indicator Technology Program* ("US–VISIT"), 69 Fed. Reg. 468 (Jan. 5, 2004); *United States Visitor and Immigrant Status Indicator Technology Program* ("US–VISIT"), 69 Fed. Reg. 53,318 (Aug. 31, 2004).

[9] See *Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure,* 73 Fed. Reg. 22,065 (Apr. 24, 2008).

eral, within 2 years, to "develop an automated entry and exit control system that will . . . collect a record of departure for every alien departing the United States and match the records of departure with the record of the alien's arrival in the United States."[10] Congress's most recent instructions came in 2007, in the 9/11 Act. That legislation set a hard and fast deadline of August 3, 2008 for DHS to deploy a system that uses biometric data to confirm that aliens participating in the Visa Waiver Program have left the United States.[11] The 9/11 Act also forbids DHS from adding any new countries to the program after June 30, 2009 if it fails to deploy an exit system by that date.[12] At the risk of understatement, exit has been a long time coming.

Apart from the legal mandate that DHS develop exit controls, there are sound policy reasons for doing so. One of the principal advantages of exit has to do with immigration: An exit system enables the Government to verify that visitors to this country have departed on time and have not overstayed the terms of their admissions. Federal immigration officers could use exit data to locate violators who are still in the country and have them deported. State and local police could access Federal exit databases to check whether aliens they encounter during routine law enforcement activities—for example, aliens who have been pulled over for traffic stops—are out of status. And if border officials know that a particular visitor previously overstayed in the United States, they can bar him from entering if he later tries to return to this country.

While the most obvious advantages are immigration-related, an exit system also offers important national security benefits. Vigilant enforcement of routine U.S. immigration laws is an effective way of detecting and incapacitating terrorist operatives. According to the 9/11 Commission, at least three of the September 11 hijackers—including Mohamed Atta, the plot's operational ringleader—previously had overstayed in the United States.[13] Ziad Jarrah—who would go on to commandeer and then pilot United Flight 93—was out of status when a Maryland State trooper gave him a speeding ticket just 2 days before the attacks.[14] With an exit system, border officials might have been able to turn away Atta and other hijackers when they subsequently tried to reenter the United States. And if police had known that Jarrah was out of status, they could have taken him into custody in the course of a routine traffic stop.

A few caveats are in order. First, this is an argument for exit controls; it is not necessarily an argument for biometric exit controls. One could just as easily imagine an exit system that uses biographic indicators—e.g., travelers' names, passport numbers, and so on—to verify whether foreign visitors have departed on schedule. Biometric exit controls probably would be significantly more reliable than biographic ones. For instance, it could be difficult to match biographic entry and exit records if a traveler uses one passport when arriving and a different one when departing. (This could be the case with diplomats, travelers with dual citizenship, and others who legitimately hold multiple passports, as well as persons who have different sets of travel documents for less benign reasons.) Another problem could arise if a traveler's biographic data is corrupted when keyed into the system—for example, an operator might inadvertently type "George Maosn" instead of "George Mason." Biometric exit controls would reduce the difficulties with matching entry and exit records; it's harder to game the system when fingerprints are involved. Reasonable minds certainly could differ on whether the additional reliability of a biometric exit system is sufficient to justify the additional costs. But, since biometric exit is required by law, the point is probably moot.

---

[10] Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104–208, § 110(a), 110 Stat. 3009, 3558 (1996).

[11] See Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 711(d)(1)(F), 121 Stat. 266, 345 (2007) (codified at 8 U.S.C. § 1187(i)) ("Not later than 1 year after the date of the enactment of this subsection, the Secretary of Homeland Security shall establish an exit system that records the departure on a flight leaving the United States of every alien participating in the visa waiver program established under this section.").

[12] See ID § 711(c), 110 Stat. at 339 (codified at 8 U.S.C. § 1187(c)(8)(A)(iii) ("[I]f the Secretary has not notified Congress in accordance with clause (ii) by June 30, 2009, the Secretary's waiver authority under subparagraph (B) shall be suspended beginning on July 1, 2009, until such time as the Secretary makes such notification.").

[13] See *The 9/11 Commission Report* 564 n.33 (2004) ("Mohamed Atta overstayed his tourist visa and then failed to present a proper vocational school visa when he entered in January 2001 . . . [T]wo hijackers overstayed their terms of admission by 4 and 8 months respectively (Satam al Suqami and Nawaf al Hazmi).").

[14] See ID at 253; ID at 564 n.33 ("Ziad Jarrah attended school in June 2000 without properly adjusting his immigration status, an action that violated his immigration status and rendered him inadmissible on each of his six subsequent reentries into the United States between June 2000 and August 5, 2001.").

Second, the benefits of any exit system necessarily will be diminished by the absence of exit controls at the land border. DHS's decision to focus initially on air and sea is prudent, given the presently prohibitive costs of land exit. Yet that choice is not without operational consequences. A system that does not capture land exits can be expected to generate a significant number of false positives. For instance, an air/sea exit system would not record the departure of a European traveler who flies to New York, crosses the land border into Canada, and returns home on a flight from Toronto. Nevertheless, my sense is that deploying a limited exit system is still worthwhile, for several reasons. Experimenting with exit at air and sea ports might inspire new ideas for tracking departures at land borders. Also, many of the travelers who visit the United States under the Visa Waiver Program arrive and depart via air. If nothing else, air/sea exit controls would be a useful way of verifying departures for this subset of visitors.

III. US–VISIT EXIT AND THE PRIVATE SECTOR

Perhaps the most noticeable feature of DHS's exit proposal is that it asks the private sector to play a prominent role in monitoring the departure of aliens from the United States. One's initial reaction might be to wonder why air carriers, cruise lines, and other private companies are charged with collecting departing visitors' fingerprints on behalf of DHS. After all, maintaining control of the border is a quintessentially governmental duty; it is indeed one of the most basic functions that any government performs. Why should the Department be outsourcing that responsibility to the private sector? Moreover, other countries that operate exit systems—Japan and South Korea, for example—collect data from departing aliens themselves. They do not place that responsibility on private entities' shoulders. Why should the United States take a different approach?

On further examination, DHS's proposed reliance on the private sector seems justified—subject to an important qualification that I will offer in a moment. Part of the reason is legal. Federal law already requires private entities to gather a fairly wide range of information about the passengers they carry and to share it with the Department. For instance, Congress has directed airlines flying to or from the United States to collect, and provide the Government with, the "full name of each passenger and crew member," the "date of birth of each passenger and crew member," the "sex of each passenger and crew member," the "passport number and country of issuance of each passenger and crew member," the "United States visa number or resident alien card number of each passenger and crew member," and "[s]uch other information as the [Government] determines is reasonably necessary to ensure aviation safety."[15] Congress also has mandated that carriers provide DHS with passenger name record information, or PNR.[16] PNR can include, among other types of data, a passenger's phone number, home address, frequent flyer number, seat assignment, other names on the reservation, and so on. Seen in this light, the DHS exit proposal doesn't break much new ground. It simply adds another type of passenger information—fingerprints—to the list of data that carriers are already responsible for collecting.[17]

Part of the reason for involving the private sector is logistical. Realistically, it's difficult to operate exit controls in any other way. American airports simply weren't built with exit in mind. Unlike facilities in other countries that operate exit systems, U.S. airports typically do not have outbound passport control stations, and it probably would be prohibitively expensive to retrofit existing facilities with the requisite physical plant. Another unattractive option would be to take fingerprints at Transportation Security Administration passenger screening checkpoints. Not to put too fine a point on it, few travelers look forward to standing in the airport security line, and adding exit to the mix would make for an even less pleasant customer service experience. Moreover, asking already overburdened TSA screeners to collect departing aliens' biometrics potentially could distract them from their job of keeping weapons off planes. A final alternative would be to require aliens to give their fingerprints using kiosks located throughout airport concourses. This option has its shortcomings as well. Allowing aliens to check out at out-of-the-way airport kiosks—which DHS tried in an early exit pilot program—virtually guarantees low passenger

[15] 49 U.S.C. § 44909(c)(2).

[16] See ID § 44909(c)(3).

[17] To be sure, air carriers compile much of this information in the ordinary course of business (e.g., passenger names and credit card numbers), so the statutory collection mandates do not impose much of a burden. However, airlines probably would not compile other types of data (e.g., birthdates, passport numbers, and "other information to ensure aviation safety") in the absence of a legal requirement that they do so. Hence there is precedent for asking air carriers to gather passenger information that is useful principally, if not exclusively, to the Government.

compliance.[18] There are no good choices for air and sea exit, but involving the private sector might be the least bad.

It might be appropriate to ask airlines to help make exit a reality, but that doesn't mean they should be stuck with the tab. In an era of record fuel prices and looming airline bankruptcies, it seems gratuitous to pile new costs on the travel industry. Under the Department's proposal, airlines are on the hook for, among other responsibilities, buying fingerprint scanners, taking prints, and sending large data files to DHS. That won't be cheap. DHS estimates that the tab could run as high as $3.5 billion over 10 years; other knowledgeable observers put the figure at $12.3 billion.[19] If airlines help the Government track departures, the least the Government can do is help airlines foot the bill.

Such an arrangement could take any number of forms. The most basic way to reimburse carriers' exit-related costs would be for them to pass their expenses on to passengers in the form of higher fares. While this approach has the virtue of simplicity, the airlines may well balk at it, sensing that consumers who have already endured several rounds of fuel-related jumps in ticket prices might not tolerate yet another hike. Another disadvantage is that the costs of the exit system would be borne not only by the alien passengers who use it, but by American travelers who by definition are exempt from biometric exit controls. A second alternative would be for Congress to authorize carriers to assess a line-item surcharge, akin to the 9/11 security fee, on foreign visitors to the United States. One upside to this approach is that the cost of the exit system would fall squarely on those who use it. Airlines might find the user fee option unattractive for the same reasons as the direct pass-through. But since American citizens would not be subject to the exit surcharge, the effects on U.S. airlines' customer goodwill probably would be less. A third option would be for Congress to appropriate funds to offset carriers' costs. An advantage of this plan is that it makes the airlines whole with few, if any, consequences for their customer goodwill. An obvious downside is that this approach would amount to a subsidy of foreign visitors by American taxpayers. The costs of operating exit controls would be borne almost entirely by U.S. citizens; the foreign travelers who use the system would get a free pass. Of course there are many other options, and each will have its own unique advantages and disadvantages. My intention here is not to express an opinion on which approach is preferable, but rather to highlight the wide range of policy choices available to decisionmakers in Congress and at the Department.

Let me offer one final recommendation. In its current form, the exit proposal could engender confusion among travelers. The Department's plan gives carriers the discretion to choose the point in the departure process at which they will take exiting aliens' fingerprints.[20] This desire to give carriers flexibility is laudable, but it virtually assures they will adopt different solutions.[21] Passengers flying out of JFK might have their fingerprints taken at the check-in counter, aliens returning home from San Francisco might use a kiosk before the TSA screening checkpoint, and visitors leaving Dulles might give their prints at the gate. Even more confusion would result if different airlines adopted different practices at the same airport.

My suggestion is that Department, in consultation with Congress and interested parties from the travel industry, should pick a uniform standard on where departing aliens will have their fingerprints taken. Perhaps the best option is to do it at the departure gate. If aliens give their prints at the ticket counter or a kiosk, it would be possible for them to check out but then abscond from the airport without actually leaving the United States. It would be more difficult for an alien to trick authorities into thinking he has departed if travelers' fingerprints are taken as they board their planes. Gateside collection probably offers the strongest assurances that aliens in fact leave the country.

Chairwoman Sanchez, thank you again for the opportunity to testify this morning. I would welcome any questions you or your colleagues might have.*

---

[18] See *Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure,* 73 Fed. Reg. 22,065, 22,069–70 (Apr. 24, 2008).

[19] See Spencer S. Hsu, *Plan to Fingerprint Foreigners Exiting U.S. Is Opposed,* Wash. Post., June 22, 2008, at A08.

[20] See *Collection of Alien Biometric Data Upon Exit From the United States at Air and Sea Ports of Departure,* 73 Fed. Reg. 22,065, 22,072 (Apr. 24, 2008) ("DHS therefore proposes to permit the air carriers latitude in where they collect biometrics from their departing alien passengers.").

[21] See ID ("DHS expects that, in some instances, an alien will be directed to an air carrier's check-in counter or kiosk prior to security screening by TSA . . . In other instances, DHS expects that air carriers will choose to collect biometrics from aliens at their international departure gates.").

* Graphic has been retained in committee files.

Ms. SANCHEZ. Thanks.

I am now going to remind Members that they have 5 minutes to question our witnesses.

I will start with myself.

I wanted to ask Mr. Principato to go over No. 4. You said you had six principles. I didn't catch—you were talking about the sterile area, and I didn't—you went through it fairly quickly, so I couldn't envision what you were proposing.

Could you go over that one more time for me?

Mr. PRINCIPATO. Sure. The idea would be that the fingerprint collection would occur not out in the lobby someplace but actually occur in the sterile area where you have people going to their flights and be part of the travel experience that the customer is going through.

Ms. SANCHEZ. So it would be after we pass security but before you go to the gate?

Mr. PRINCIPATO. It could be at the gate. It really depends on the airport.

Mr. Lavin and I have discussed this often. We don't have exactly the same view, but depending on the airport, it could be at the gate. It could be right after the checkpoint. It depends really on the airport. If you did it just at the final point of departure, for example, one of the problems with just doing it at the checkpoint, let's say you start in Fort Wayne or let's say you start in Roanoke or something, you fly to Dulles to fly out. You come in to terminal C out there. You would have to take the people mover back to where the checkpoint is in the main terminal and do it and then go all the way back on the people mover back to get your flight, which might be just two gates down.

So that is why we are proposing doing it in the sterile area and also giving some flexibility, where it might be at the checkpoint in certain places; it might be just beyond the checkpoint or in the same footprint, or it might be closer to the gate or some other place but in the sterile area so you don't get—you don't end up with a backed-up lobby.

Ms. SANCHEZ. Great. Thank you for that clarification.

Mr. Lavin, could you explain what the effects of expanding the Visa Waiver Program would be on your industry?

Mr. LAVIN. In terms of the impact, certainly, especially in these troubling times, the more visitors we have come into the United States, when I think 30 or 40 percent of the world's traffic is between the United States and Europe in particular, would have a significant positive impact on our industry at a time when we desperately need it. So we would do anything we can to support it, absent funding a Government program to meet those deadlines.

Ms. SANCHEZ. If we suspended it, and said Congress would suspend that, how do you think it would affect your business?

Mr. LAVIN. Well, we estimate that for every additional dollar of the cost of fuel is a $1.6 billion cost for the industry. You know how the dollars have been going up over the last 6 months. So our estimate—and I don't have any exact figures, and we can certainly provide those in written response, but our estimate is that every penny counts. If there is a cutoff of that, and there is frankly, as you suggested before, some retaliation by the other governments

coming back to us, that would significantly slow down air travel at a time when we just cannot afford it.

Ms. SANCHEZ. Mr. Souder.

Mr. SOUDER. First, I want to thank Mr. Sales, because we get down into the nitty gritty, and we have to step back every so often and go, why do we want this program?

Quite frankly, visa programs were a disaster pre-9/11, particularly with Saudi Arabia and a lot of the Middle Eastern countries, the penetration in the European Union. I thought you made a terrific point that the entry is more critical than the exit, but it doesn't mean that the exit isn't important.

Mr. Lavin, the point where you say the Government doesn't have a right to oppose this. The Government has a right. The Government abuses its rights, that we make businesses collect taxes, all kinds of perspective data on safety in addition to already data on this type of thing. The Interstate Commerce Clause is so broad as to basically any more in this era to cover everything, even whether you can comb your hair because you crossed State lines. It is so elastic.

The question is: What is the reasonableness of Government to do it, and how we do this?

Mr. Principato, in looking at the costs, that I wanted to pursue, because I don't fully understand this. I am a big believer that everything is going to ten fingerprints at some point, including domestic travel. The immigration pressures, which are interrelated which all kinds of smuggling, which are interrelated with terrorism, we are headed there even for domestic flights.

You raised a question of hardwiring—and maybe this is Mr. Lavin, too—that, do the airlines currently not have the hardline capability that if the Government paid for upgrades in the software, particularly if we could get this down to the 73 airports? I mean, that seems like a logical stick thing, but you might have to not just do it at the gate; there may be other types of ways to do it. But if we could get the number of airports down, because I am certain that the problem is greatest, on my question, in the smaller airports. But I would assume, the bigger the airport, the more likely there is to be something, if not hardwired at each check-in, that at least some of the airlines would be hardwired, the bigger ones. There would be some way to maneuver this.

Mr. PRINCIPATO. I think Doug knows more about how the airlines are wired, and I am going to really let him deal with that.

But your point about the cost and the smaller airports. You talked about before about Fort Wayne. Tory Richardson does a great job there, and I have been with him several times with him, and they are working hard to keep the air service that they have and expand it. The costs for an airport like that would be very difficult to absorb. That is why we proposed the last point of departure.

But I think Doug probably has a more compete answer in terms of the technical part of your question. I am still trying to figure out how to set the time on my VCRs.

Mr. LAVIN. In terms of the technical side, your questions earlier about the kiosks themselves, the existing kiosks. The existing kiosks are designed to transfer data and not transfer images. Bio-

metrics are images. So the current hardwiring between the kiosks, the airline kiosks or the airport kiosks, they are owned sometimes by airlines and owned other times by airports, does not allow for the transmission of biometrics. So, therefore, I would be very interested in Mr. Mocny's analysis of that, because I think what they would come out with is that they should do it in their own kiosks, their own separate kiosks, again, in the sterile area.

The reason there is an advantage there for the U.S. Government on that, and for DHS in particular, is CBP already has hardwired at 119 airports to submit fingerprints as part of the US–VISIT program. So at 119 airports where there is US–VISIT, they have the capabilities to transmit biometrics. So we would recommend that they put their own kiosk system in place in the sterile area. We would like to keep it as far as away from the boarding area as possible, but we don't have a problem with whether it is mobile or fixed, and use the hardwires they already have existing to transmit that data.

We just don't have that. We also don't have secure lines. One of the costs of the $12 billion is we currently do not have secure lines that are required under the rule to provide the fingerprint data.

Mr. SOUDER. So, in my earlier question, this is what I have never understood, because the security question wouldn't be as great if it was just a popup on the screen. In other words, if it could be handled in—because if you are exiting and you don't have a security question, we have one question which is, how much would it cost to increase the capability of the hardwire, which you have to hardwire how much of the airport to expand the transmission capability to get fingerprints? That is one question.

So the fingerprints, though, that the only reason you would have to have a secure question would be if it got some kind of negative.

Mr. LAVIN. Well, no. Because, frankly, what they are proposing is to collect these fingerprints after the person—excuse me, collect them from the airlines after the person leaves the country and put them in an FBI database in local, State, and local authorities' databases for up to 75 years. So, they are not, at this point, they are not proposing to stop somebody. They say in the future they would like to. But the negative is not——

Mr. SOUDER. Here is what I am wrestling with, because we have this challenge in multiple places. So that information is secured, and let's say that is the Government's responsibility to secure it. But the transmission, if you have to secure the data, now all of a sudden you have to have a whole security question. But if the fingerprints go into that system that isn't yours and a flag comes up, then you don't have to store the data.

Mr. LAVIN. No. Well, we have to store—they would like us to establish our own secure data forms——

Mr. SOUDER. I know that is what they would like you to do. What I am asking is, if they had to store the data, what would be the problem if we could come up with a way where you put your fingerprints on, and then the only way you would have to go to TSA or a security point is if somehow it came up negative. That way, you wouldn't have to have the data.

I am assuming that this is what we are trying to do, it is secondary, at port entries. I mean, we are really wrestling with the

same question as to how we go through entry/exit at land ports. What we are going to have with your cruise ships is that most people—and this would be classic business management. Don't put one, two, three levels when 99-point-something percent of the people aren't going to hit that. Let's get the positives and the false positives and separate that, and then our biggest challenge is that there is a false positive.

Mr. LAVIN. Well, my understanding is that—I understand your question in terms of coming up as a flag or not. But what they propose to do is suck out all these fingerprints, put them in a database, their own—have us store them. Put them in their database. Five years later, a person gets caught for speeding and has a child support payment; they can use that fingerprint to match that person up. So that is what they are talking about here. This, as I described it, is a dragnet over the entire process. You know, the privacy issues there are substantial.

The only other thing I would mention on your kiosk example—I am certainly not here representing DHS, as you can imagine. But what they believe is that they don't want it, my understanding from the NPRM, is they don't want it at the check-in kiosks, because they want to make sure the person who gives the fingerprint actually leaves the country. So they want it as close to the boarding area as possible.

Mr. SOUDER. If I may ask one further question with that, because I have raised that question at an earlier hearing: How do you know it is the same person? There are different ways to do this, because I think at the security checkpoint, we are also going to wind up with fingerprints, by the way. Which leads to your question, how can we consolidate this type of thing? That as we move, how much is the wiring capability different at the original check-in point from that at gate?

Mr. LAVIN. Right now, they are very similar. All they provide for is data. The only people, the only organization that has secure capabilities is the US–VISIT program. So at this point—I mean, it is important to note that five fingerprints is more data than the entire 747 of data that we are transmitting now. So one person's fingerprints is more than a full 747.

DHS made the mistake of believing that we had Internet-based networks, and they just didn't look at it carefully, and, frankly, they didn't consult with us. A lot of these problems, frankly, could have been solved if 5 years ago or 10 years ago when they thought about this or a year ago when they knew they had to do it, they would consult with industry. All they told us, as soon as you passed the law is: We are going to do it this way. Airlines are going to pay. Next question.

Mr. SOUDER. That last comment was very helpful, because you are saying basically your broadband isn't anywhere near storage capacity. We are really looking at a huge challenge, and as I believe, particularly after we get another terrorist attack, which will happen at some point, there is going to be more demands than just this one, and we are going to have to figure out what burden of this falls on the private sector on security questions.

Mr. LAVIN. We don't have broadband networks, period.

Ms. SANCHEZ. Thank you, gentlemen.

I thank you for your testimony today.

I will remind the Members of the subcommittee that, if they have additional questions, they will put them forth in writing to you all.

I think that you will receive some, by the way. We would ask you to respond quickly in writing to those questions.

Hearing no further business, the subcommittee stands adjourned. Thank you, again.

[Whereupon, at 11:37 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRWOMAN LORETTA SANCHEZ FOR RICHARD C. BARTH, PH.D., ASSISTANT SECRETARY, OFFICE OF POLICY DEVELOPMENT, DEPARTMENT OF HOMELAND SECURITY

Question 1. Some have expressed concern about terrorists who are nationals of Visa Waiver Program (VWP) countries exploiting the VWP to enter the United States. Once all the security requirements mandated by the 9/11 Act have been implemented, how much confidence can the American people have that terrorists will be unable to enter the United States through the VWP?

Answer. The Department of Homeland Security (DHS) recognizes that terrorists or individuals with malign intent may attempt to exploit visa-free travel. That is why the Department is committed to transforming the Visa Waiver Program (VWP) from a program that evaluates security threats on a country-by-country basis into one that screens for risks on an individual passenger basis. To accomplish this objective, DHS is relying on four interrelated elements—advance passenger information, enhanced information sharing, secure travel documents, and intelligence-based VWP assessments—all of which are part of a secure, modernized VWP mandated by the 9/11 Commission Act. These elements have been at the forefront of national and international initiatives to combat crime and terrorism throughout the world and will provide our operators and analysts with new tools to secure the United States, as well as help prevent terrorist and criminal activities in VWP partner nations.

Advance Passenger Information

The Department receives Advance Passenger Information (API) from air carriers before a plane departs for the United States. This information is checked against watch lists and other relevant databases. DHS also collects Passenger Name Record (PNR) data from carriers pursuant to the Aviation and Transportation Security Act, and, in the case of flights to and from the European Union, pursuant to the 2007 U.S.-EU PNR Agreement. This information enables DHS to identify terrorists and criminals known to U.S. law-enforcement and intelligence agencies as well as make connections between known and suspected terrorists and unknown associates. As part of its efforts to implement the 9/11 Commission Act, DHS now requires Memoranda of Understanding (MOU) of VWP countries and aspirants. These MOUs reaffirm DHS's intent to collect both forms of information.

DHS will also receive advance passenger information on travelers through the Electronic System for Travel Authorization (ESTA). ESTA provides an additional layer of advance scrutiny that VWP travelers must undergo prior to boarding a carrier bound for the United States. ESTA was deployed for voluntary use on August 1, 2008, and is currently scheduled to become mandatory in January 2009. Starting in January, all VWP travelers will be required to submit to DHS electronically before departing for the United States. This information is the same as that currently collected via the I–94W Nonimmigrant Alien Arrival/Departure Form. ESTA applications are then queried against appropriate law enforcement databases and watch lists, enabling DHS to make a determination on each individual's eligibility to travel to the United States under the VWP before that alien's departure for the United States. Travelers denied an ESTA authorization are referred to the U.S. embassy or consulate to apply for a visa.

Enhanced Information Sharing

As required by section 711 of the 9/11 Commission Act, the governments of the 27 countries that currently participate in the VWP—as well as those of any new member countries—will enter into more robust data-sharing arrangements with the United States as a condition of membership. Under Homeland Security Presidential Directive—6, the Department of State has taken the lead in negotiating an agreement with both aspirant and current VWP member countries to share data from

watch lists of known and suspected terrorists that will also fulfill the terrorist information-sharing requirements in the 9/11 Commission Act for initial and continued VWP designation. To date, HSPD–6 agreements have been signed with five current VWP countries and four "VWP roadmap" countries. The State Department and the Terrorist Screening Center currently are engaged in negotiations with 17 current VWP and 4 VWP roadmap countries and anticipates that several more arrangements will be signed within the next few months. In March 2008, DHS and the Department of Justice initiated a ground-breaking fingerprint-sharing agreement with German authorities. This new agreement will deepen counterterrorism and law enforcement cooperation with Germany, where last September U.S. and German officials together dismantled a terrorist plot. A similar agreement will be a requirement for all VWP members and active negotiations are currently underway with several current and "VWP roadmap" countries.

Secure Travel Documents

Ensuring the security of travel documents is also integral to a modernized VWP. All VWP members report, within 24 hours, the loss or theft of both blank and personalized passports. In late 2007, DHS and Interpol successfully linked the Interpol Stolen and Lost Travel Document database to the screening of arriving passengers. This real-time sharing capability is now available at all U.S. ports of entry and strengthens the ability of frontline officers to identify and interdict illicit and mala fide travel documents and the travelers who use them. DHS is also working with countries to improve document security more generally. To be valid for Visa Waiver travel, a passport issued since October 26, 2006, is required to include an integrated biometric chip with the facial image and biographical data of the passport holder stored electronically. VWP countries intend to work toward issuing passports and travel documents through a central issuing authority that is subject to strict audit and accountability mechanisms. Similarly, they will agree to issue travel documents that have unique, non-recurring identifying numbers affixed at the time of manufacture.

Intelligence-Based VWP Threat Assessments

DHS Office of Intelligence and Analysis, on behalf of the Director of National Intelligence (DNI), leads—in coordination with other intelligence community member agencies—independent intelligence assessments of all VWP countries as well as initial threat assessments for all "roadmap" or prospective VWP member countries as required by the 9/11 Commission Act. These assessments are intended to determine whether U.S. security, law enforcement, or immigration interests are compromised by the country's involvement in the program. These assessments specifically analyze the potential for illicit actors, including transnational criminals, extremists or terrorists, to exploit the country's travel systems and security profile to gain entry into the United States under the VWP.

The above enhancements significantly strengthen the VWP. In addition, countries participating in the program will also be encouraged to enhance aviation and airport security, including permitting the operation of U.S. air marshals. These discretionary security measures will continue to be taken into consideration during the statutorily mandated VWP initial and continuing designation reviews conducted by DHS in consultation with the Department of State. During these reviews, DHS comprehensively reviews the following for each VWP member country: counterterrorism capabilities; immigration, citizenship and naturalization laws; passport production and issuance controls; efforts to combat crime; law enforcement cooperation with the United States; and border-control mechanisms. In addition to these thorough evaluations, DHS has consolidated its monitoring capability to ensure awareness of changing conditions in VWP countries, established protocols for direct communications with points of contact in the relevant embassies, and required periodic updates of law enforcement or security concerns related to the VWP.

Overall, these enhancements will mitigate substantially the vulnerabilities of visa-free travel to the United States, and will help secure U.S. borders and promote a safer international travel environment for our citizens and those of our VWP partners. The provisions in the 9/11 Act that gave the administration new flexibility to admit new countries into VWP has proven to be an extraordinarily effective tool for us in gaining cooperation from many governments, including some with no short-term prospect for qualifying for VWP, in implementing all of these new security measures.

Question 2a. Implementing a biometric exit system should improve the quality of the information the Federal Government has on overstay rates and travelers coming to the United States.

What does visa overstay information tell us about a country or an individual that "visa refusal" information does not?

Answer. "Visa overstay" is more accurately described as overstaying an authorized length of stay, as a visa is valid only as a entry document; the length of stay is determined by CBP inspectors. Overstay information is established after the individual has been in the United States and stayed beyond the permitted length of authorized stay (based on the type of visa ad permissible duration). Visa overstay information is currently calculated using biographic departure data compared with arrival information.

State collects visa refusal data based on its electronic records (Consular Consolidated Database) and provides it to DHS. Visas can be refused for numerous reasons unrelated to whether an alien might overstay his or her authorized period of admission. US–VISIT provides the additional compliance status of visitors to the United States, enabling Department of State adjudicators and Department of Homeland Security inspectors to more thoroughly evaluate the visa application and the validity of travelers' claims to have complied with the terms of admission during previous trips to the United States. Consequently, by providing reliable information on overstays, US–VISIT has provided an effective tool for United States immigration officials to take immediate action against this type of immigration violator, allowing DOS adjudicators to deny visa applications, CBP inspectors to deny entry, and ICE criminal investigators to deport an individual for violating INA § 237(a)(1)(B), being unlawfully present in the United States.

Refusal and overstay rates both can be determined with respect to an individual and with respect to a country (as with countries participating in or pursuing qualification in the Visa Waiver Program).

Question 2b. If DHS does not have a biometric exit system in place by June 30, 2009, what alternative plans does DHS have for improving the reliability of overstay rate information?

Answer. If DHS does not have a biometric exit system in place by June 30, 2009 US–VISIT will continue to perform biographic exit comparisons as it does today, refining and improving its existing operations as a matter of course.

Question 3a. According to your testimony, DHS is requiring each VWP member and aspirant country to sign a Memorandum of Understanding (MOU), which outlines a number of security enhancements that must be met to enter or stay in the program.

Are there any security enhancements that an aspirant VWP country will be required to meet that a current member country is not required to fulfill? If so, which enhancements and under what circumstances would they not have to be fulfilled?

Question 3b. What effect would the lack of a biometric exit system, as required under section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–53), have, if any, on countries that have signed MOUs and are working toward joining the VWP?

Answer. Both current and aspirant Visa Waiver Program (VWP) member countries will be required to meet the same security standards. A single tier VWP is essential because security threats are not confined to particular corners of the globe. Accordingly, the Department of Homeland Security (DHS) is requiring each member and aspirant country to implement the same requirements to join or continue to participate in the VWP. When necessary to achieve the same standard as aspirant countries, current VWP members must enter into new agreements with the United States.

Those countries seeking to join the VWP must comply with all of the new security measures before admission; for current participants, DHS has a target for them to meet those new requirements no later than October 2009. Staggering the times for compliance in this way best enables DHS to ensure a smooth and efficient path to uniform security standards for all VWP members.

The 9/11 Commission Act requires DHS to either establish a biometric air exit program by June 30, 2009, or face suspension of the Secretary's authority to waive the low nonimmigrant visa refusal rate requirement for VWP designation. If an aspirant country that requires a waiver has not been designated by that date, the lack of a biometric exit system would prohibit the Secretary from exercising his waiver authority.

Question 4a. The Interim Final Rule for the Electronic System for Travel Authorization (ESTA) did not require travelers to pay a fee to use the new system.

Why did DHS initially choose not to require a VWP applicant to pay a fee to use ESTA?

Question 4b. Under what circumstances would you consider requiring VWP applicants paying a fee to use ESTA?

Answer. The Electronic System for Travel Authorization (ESTA) was funded by Congress with $36 million via the Consolidated Appropriations Act of 2008. This funding has supported the development of ESTA, including the underlying ESTA information technology (IT) infrastructure; the establishment of an ESTA project management office; the hiring of staff to screen ESTA applications; and a communications and outreach initiative to promote ESTA awareness for affected VWP travelers and stakeholders, including the travel and tourism industries. As a result of this appropriation, DHS has been able to implement the ESTA program without initially requiring a fee.

Once ESTA is mandatory for all VWP travelers, DHS will be better able to evaluate and assess all costs associated with the ongoing administration of the system, and to determine what fees, if any, should be included in the ESTA application process. This assessment will examine the IT upgrades and other associated costs that will be necessary to incorporate a fee collection program into the ESTA application process. If necessary, DHS will implement a fee through a separate rulemaking action or such other manner as is consistent with the Administrative Procedure Act and applicable statutory authorities.

Question 5a. ESTA will be available for VWP travelers to use on a voluntary basis on August 1, 2008, and will be mandatory for all VWP travelers on January 12, 2009.

When does DHS plan to certify that ESTA is "in place," as required by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110–53)?

Question 5b. How does DHS intend to use the information supplied by visa waiver travelers on a voluntary basis between August 1 and January 12, 2009?

Question 5c. How will a VWP traveler receive an ESTA at an airport if their carrier does not yet have the necessary internet connections to provide an ESTA?

Answer. DHS anticipates that the Secretary will certify that Electronic System Travel Authorization (ESTA) is "fully operational" in November 2008, and further anticipates publishing a notice in the Federal Register on November 13, 2008, that will require all Visa Waiver Program (VWP) travelers to obtain an ESTA approval for travel to the United States effective January 12, 2009.

On August 1, 2008, DHS began to accept voluntary ESTA applications through the ESTA Web site. The period between August 1, 2008, and January 12, 2009, will allow DHS, in partnership with the Departments of State and Commerce, the governments of VWP countries, and the travel and tourism industries, to conduct extensive outreach and communicate ESTA requirements to affected VWP travelers and related stakeholders. During this period, all voluntary applications will be processed through ESTA and approved VWP travelers who receive an approved ESTA approval after August 1, 2008, will be eligible to travel to the United States under the VWP for the duration of time that their ESTA approval is valid.

Carriers are not required to submit ESTA applications on behalf of their customers. If a VWP passenger arrives at an airport en route to the United States without having already obtained an ESTA approval, and their carrier is unable or unwilling to connect to the internet to assist their customer, the passenger may seek to apply for an ESTA approval through any vendor that offers internet access, or the passenger may also apply for an ESTA approval with the assistance of any other third party, such as a relative, a travel agent or a friend. A third party may submit an ESTA application on behalf of a traveler directly to the ESTA Web site located at *https://esta.cbp.dhs.gov/*.

Question 6a. According to the Interim Final Rule for ESTA, it is estimated that 0.04 percent of ESTA applicants will be prevented from traveling to the United States as a result of the ESTA requirements.

How did DHS come to the conclusion that roughly 0.04 percent of ESTA applicants will be prevented from traveling to the United States as a result of the ESTA requirements?

Question 6b. For applicants that receive a "Travel Not Authorized" or "Authorization Pending," response from ESTA, what recourse will be available, particularly when travelers apply for the ESTA at an airport?

Answer. For the Interim Final Rule, DHS conducted simulated Electronic System for Travel Authorization (ESTA) queries using Advance Passenger Information System (APIS) data for Visa Waiver Program (VWP) travelers to the United States from July 2007 through September 2007. The APIS data was screened against the databases against which DHS screens ESTA applications; this simulation was unable to account for those VWP travelers who may affirmatively respond to the VWP eligibility questions on Form I–94W. This simulated query was designed to provide estimates that would accurately reflect the anticipated number of ESTA application denials during a peak travel period. Of the VWP passengers who were queried through this simulation, 0.0403 percent would have been found ineligible to travel

to the United States under the VWP had they applied for an ESTA approval. The results of this simulation closely aligned with the 0.0561 percent of VWP travelers who were refused admission at our ports of entry during fiscal year 2007.

On August 1, 2008, DHS began to accept voluntary ESTA applications through the ESTA Web site. Through August 13, 2008, ESTA has processed 38,860 applications and approved 99.53 percent of those applications. Twenty of the 38,860 applications (0.0515 percent) have been denied as a result of a law enforcement or terrorist watch list match and 163 applications (0.4195 percent) have been denied as a result of an affirmative response to a VWP eligibility question. DHS continues to work closely with the Department of State to carefully monitor the number of ESTA applications that are not approved, as well as the reasons that ESTA applications are not approved, and will coordinate any necessary system adjustments.

ESTA applications may be submitted at any time prior to travel to the United States, and DHS encourages VWP travelers to apply for authorization as soon as they begin to plan a trip to the United States. DHS recommends that the application be made at least 72 hours prior to traveling. If an ESTA application is denied and the traveler wishes to continue with his or her trip to the United States, the traveler will be required to apply for a nonimmigrant visa at a U.S. Embassy or Consulate. It is important to note that Embassy and Consulate employees will only be able to make a determination on visa eligibility; they will not be able to change or resolve the ESTA denial. Similarly, while the ESTA Web site will provide a link to the DHS Travel Redress Inquiry Program (TRIP) Web site, there are no guarantees that a request for redress through DHS TRIP will resolve the VWP ineligibility that caused an applicant's ESTA application to be denied. For those ESTA applications that are pending, the Web site provides the capability for applicants to use their application tracking number and passport data to query the system within 72 hours to check the status of their application.

Question 7a. Over the last few years, air carriers have been tasked with implementing a number of Federal security initiatives, including US–VISIT, ESTA, Secure Flight, and APIS Quick Query.

What type of overlap (e.g., similar information collected, vetted through the same watch lists or databases, same networks used, same personnel used), if any, exits among these five different programs?

Question 7b. How does DHS propose to manage, coordinate, and staff all of these different yet related programs?

Answer. US–VISIT, the Electronic System for Travel Authorization (ESTA), and the Advance Passenger Information System (APIS)/APIS Quick Query (AQQ) are screening systems through which DHS conducts checks of international passengers. Each system is structured differently, affects different populations, and is applied at different times in the travel continuum.

Secure Flight is a proposed air passenger screening program that, when implemented, will screen domestic and international air passengers against the No Fly and Selectee lists to deny the boarding of, and/or ensure additional screening is completed for, those travelers who pose a potential threat to aviation security.

As of January 12, 2009, Visa Waiver Program (VWP) travelers will be required to obtain ESTA approval prior to travel to the United States and are encouraged to apply for travel authorization via ESTA as soon as they begin to plan a trip to the United States. ESTA collects basic biographical data including name, birth date, and passport information, as well as travel-related details. ESTA applicants are also required to answer VWP eligibility questions regarding communicable diseases, arrests, and convictions for certain crimes, and past history of visa revocation or deportation, among others.

ESTA provides individual security screening in advance of a VWP visitor's travel to the United States, and a pre-departure determination of an individual's eligibility to travel to the United States under the VWP. Before the implementation of ESTA, travelers would learn of their ineligibility to travel to, or enter into, the United States under the VWP upon their arrival. ESTA will make VWP eligibility determinations before travelers depart for the United States, reducing the inconvenience for travelers who currently only learn of their VWP ineligibility upon arrival in the United States.

Initial APIS/AQQ checks are completed before an international flight departs for the United States and are performed on all travelers. Airlines submit APIS/AQQ manifest information to DHS, including, but not limited to, full name, date of birth, gender, travel document number, travel document country of issuance, and address while in the United States for designated non-U.S. citizens. APIS/AQQ data is collected to first enable DHS to quickly screen against the No Fly and Selectee lists to deny the boarding of, and/or ensure additional screening is completed for those travelers that pose a potential threat to aviation security. Additional APIS/AQQ

checks are performed by U.S. Customs and Border Protection (CBP) while the aircraft is en route to the United States, to identify those who warrant further scrutiny for all admissibility and law enforcement purposes upon arrival at a port of entry. Upon implementation, the Secure Flight program will conduct No Fly and Selectee screening for international flights, however, APIS/AQQ checks will continue to be performed by CBP for admissibility and law enforcement purposes at the ports of entry.

The US–VISIT program collects biometric information from designated non-U.S. citizens upon their arrival at a United States port of entry. The biometric data collected at the ports of entry is checked against derogatory data including, but not limited to, terrorism, criminality, and immigration status. DHS also has proposed a program that would require the non-U.S. citizens who currently provide biometric identifiers upon entering the United States in connection with the US–VISIT program to also provide fingerprints when they depart the United States from any airport or seaport. The biometric checks that are currently conducted under the US–VISIT program at entry, as well as those that DHS has proposed to collect at exit, are separate and distinct from the advance biographic checks completed under the ESTA, APIS, and AQQ programs.

The ESTA and APIS/AQQ programs are currently being integrated. Carriers will send passenger data through an interactive APIS/AQQ message prior to boarding a passenger, and DHS will send back a response to the carriers regarding both ESTA and APIS/AQQ indicating whether a VWP traveler has a valid travel authorization via ESTA and may board a U.S.-bound carrier. When implemented, DHS will also fully integrate the Secure Flight program into APIS/AQQ and ESTA, such that carriers will have a single set of consolidated requirements, common data transmission and messaging standards, and they will not be required to send the same information to different DHS components.

The DHS Screening Coordination Office works closely with all related stakeholders, including the US–VISIT program office, CBP, and the Transportation Security Administration to ensure that program requirements are aligned and that resources are managed effectively. We also work very closely with the airlines to implement these programs and address any concerns raised regarding coordination.

QUESTIONS FROM CHAIRWOMAN LORETTA SANCHEZ FOR ROBERT MOCNY, DIRECTOR, US–VISIT PROGRAM, DEPARTMENT OF HOMELAND SECURITY

Question 1a. Under the proposed rule for air exit, DHS analyzed a number of biometric collection alternatives, including a kiosk option, but ultimately selected an option that would require air carriers to collect and transmit a traveler's biometrics.

What progress has DHS made in overcoming the concerns voiced by the air travel industry?

Answer. The notice of proposed rulemaking (NPRM) provided a variety of alternatives with different risks and benefits, and the Department of Homeland Security (DHS) attempted to balance the risks and benefits in the NPRM. DHS is currently reviewing public comments and developing a final rule. DHS aims to complete the regulatory process and publish the final rule by the end of this year.

Question 1b. If DHS publishes a final rule that requires air carriers to collect and transmit a traveler's biometrics, what assistance will DHS provide to air carriers to meet the June 30, 2009 deadline?

Answer. If the final rule should require air carriers to collect and transmit biometrics, DHS would work with carriers to ensure understanding of the exit requirements. The types of assistance that DHS might consider providing are: (1) Training materials for employees on the standards applicable and how to meet those standards, including how to acquire the best fingerprint image; (2) best practices for collection of biometrics; (3) outreach to the public and various stakeholders; and (4) specific guidelines and standards for the collection of biometrics.

Question 2a. As you know, this committee has been very interested in DHS's transition planning, particularly because a number of programs at the Department, including US–VISIT, will be handed off to the next administration for completion.

How will the change of administrations affect the US–VISIT Program Office?

Answer. The transition to a new administration will be straightforward because US–VISIT has been intricately involved in the Department of Homeland Security National Protection and Programs (NPPD) transition planning effort, which is part of a larger Department-wide effort. The Director of US–VISIT is a career executive who has been responsible for the US–VISIT program since its inception. This continued leadership positively supports the transition.

US–VISIT will accomplish many of its planned goals by January 20, 2009, such as deploying the first increment of the Initial Operating Capability (IOC) with the FBI IAFIS database and completing 10 Print Full Deployment.

US–VISIT also has appointed a senior manager as a representative to work with NPPD to assure program stability during the transition. His expertise in contracts, funding, staffing, and logistics, will ensure the program office will operate unencumbered during the transition.

US–VISIT has been briefed on NPPD's transition plans and the Director recently participated in a Senior Leaders Transition Exercise held at the Federal Law Enforcement Training Center in Glynco, Georgia. US–VISIT will continue to participate in future exercises to assist in ensuring program stability during the transition. Additionally, all contracts, funding, staffing, and logistics are in place and will operate unencumbered during the transition.

Question 2b. What transition plans, if any, are in place to ensure that a biometric exit system is a priority in the next administration and is completed before the June 2009 deadline?

Answer. In light of the above measures that have been, and continue to be, put into place, including preparation of briefing books of important initiatives and issues, the biometric exit effort should not be adversely affected by the transition.

Question 3a. In February 2008, the Government Accountability Office (GAO) reported that the various exit pilots DHS conducted for US–VISIT exit between 2003 and 2007 were not well planned, defined, or justified. Equally troubling was the fact that DHS did not share the results of the pilots with the airlines or publically release the results of these pilots until June 2008.

Why did DHS wait so long to publically release the results of the air exit kiosks?

Answer. In response to two formal requests this past May—one from ATA's CEO Jim May, and the second from congressional questioning during Paul Schneider's confirmation hearing—DHS decided to release the Exit Pilot Evaluation Report. Since the document was "deliberative," it needed to undergo various Department review processes before public release.

Question 3b. How does DHS justify moving forward with an air exit biometric solution that has not been previously tested or piloted?

Answer. DHS has utilized the lessons learned from the pilot evaluation in developing the solution in the proposed rule. Additionally, DHS is utilizing the cost/benefit analysis that was developed as part of the regulatory impact analysis in conjunction with the notice of proposed rulemaking (NPRM). US–VISIT is completing its review of the comments to the NPRM and plans to publish a final rule later in 2008.

Question 3c. What improvements has DHS made to ensure that the latest air exit proposal is, in fact, well-planned, defined, and justified?

Answer. US–VISIT continues to develop a final rule to establish a biometric exit capability within the international air and sea passenger environments.

- In November 2007, National Protection and Programs Directorate Under Secretary Robert Jamison convened a departmental planning session to ensure a coordinated approach to implementing air and sea exit operations.
- On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) outlining its proposed solution for collecting biometrics from most non-U.S. citizens when they depart the United States from U.S. airports and seaports, along with a regulatory impact analysis, which includes a cost/benefit analysis.
- In conjunction with the NPRM, US–VISIT completed a regulatory impact analysis for air and sea exit implementation. This analysis includes the costs and benefits of five solution alternatives in the NPRM, providing decisionmakers and the general public with grounded information on which to comment regarding the proposed rule.
- US–VISIT is completing its review of the comments to the NPRM and will revise the draft final rule as appropriate.

Question 4a. The biometric collection alternative chosen by DHS is, by your own admission, "less favorable" from a privacy and IT security standpoint than a DHS collection method.

Why does DHS insist on moving forward with a proposal that is more vulnerable to security breaches and invasions of privacy?

Answer. The Department of Homeland Security (DHS) recognizes this privacy concern, which has also been expressed in the public comments received as part of the rulemaking process. DHS considered a wide range of factors in the development of the proposed rule, including security and privacy considerations. DHS considered and balanced current operations, technical requirements, confidence of departure, projected percentage of population captured, burdens imposed, costs, efficacy, convenience, development time, immigration and other enforcement policy, and many

other factors in administering DHS' mission. DHS has considered those comments and may make adjustments based on privacy and security risks that will be discussed in both the updated Privacy Impact Assessment and the publication of the Final Rule. The rulemaking process is naturally one of balancing competing interests and priorities while considering the magnitude and probability of varied risks. DHS will respond if any privacy breaches occur on this or any other systems.

Question 4b. The Notice for Proposed Rulemaking for US–VISIT biometric air and sea exit states that "carriers must take steps to protect the privacy of information collected." What steps do you envision the air carriers taking and at what cost?

Answer. If the proposed rule were finalized without amendment, we would expect to issue guidance to the carriers providing specific handling procedures. DHS and the carriers take privacy issues seriously, and carriers have as great a concern for privacy as DHS. Carriers routinely collect, as part of the carriers' reservation process, substantial personal data regarding all passengers, such as credit card, lodging, and rental car information, none of which would be transmitted to or used by DHS.

Under the proposed rule, the Regulatory Impact Analysis (RIA), published with the Notice of Proposed Rulemaking, embedded privacy compliance costs within the costs for application development, which includes planning, designing, building, testing, and deploying the proposed technical solution. These costs will be updated in the final rule's RIA.

Question 4c. If a breach occurs or a carrier is found to be putting a traveler's personally identifiable information at extreme risk, how would DHS respond?

Answer. Carriers currently collect substantial personal data as part of the carriers' reservation process for all passengers, such as credit card, lodging, and rental car information, none of which is transmitted to or used by DHS. Carriers currently provide DHS with manifest information. The only additional information that would be required under the proposed rule is the fingerprint image. DHS will treat any violation of an alien's personally identifiable information in the same manner as any other breach.

Although the Privacy Act, 5 U.S.C. 552a, applies only to United States citizens and lawful permanent residents (LPRs), DHS, as a matter of policy, administratively provides most of the Privacy Act benefits to aliens about whom information is maintained by DHS. DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, Memorandum 2007–1 (January 19, 2007), at *http://www.dhs.gov/xlibrary/assets/privacy/ privacy_policyguide_2007-1.pdf*. DHS will continue that policy for aliens subject to any final rule.

Question 5a. The Implementing Recommendations of the 9/11 Commission Act of 2007 requires the implementation of an air exit system as a condition to allowing the Secretary of DHS to use the waiver authority to expand the Visa Waiver Program. As an interim step, the Act allows a biographic system that can "verify the departure of not less than 97 percent of foreign nationals who exit through airports." GAO testified in February that the approach that DHS is taking for certifying an air exit system that can verify 97 percent of foreign nationals did not provide particularly useful information.

Please explain how DHS will meet the requirement and certify an air exit system that can track the departure of 97 percent of all foreign visitors?

Question 5b. When does DHS plan on notifying Congress that it can track the departure of 97 percent of all foreign visitors?

Answer. Department of Homeland Security (DHS) continues to evaluate methodologies to verify the departure of at least 97 percent of foreign nationals who exit through U.S. airports. DHS is committed to ensuring the complete, accurate, and timely receipt of departure manifests and to improving the methodology underpinning air exit calculations. DHS expects to make this certification pursuant to the statute's requirement later this year.

Question 6a. The US–VISIT biometric exit proposed rule outlined a number of biometric collection alternatives and even suggested that DHS is actively considering combining a number of the alternatives and using kiosks.

What kind of role do you envision kiosks and mobile biometric collection devices playing in US–VISIT Exit?

Answer. The Department of Homeland Security (DHS) has not precluded any options for the collection of biometrics; however, formulation of a final rule will not be completed until after review of the comments to the Notice of Proposed Rulemaking (NPRM). Under the proposed rule, carriers would be provided with substantial flexibility to use kiosks and only be required to meet performance standards.

Question 6b. What kinds of costs would be associated with modifying or adapting existing air carrier kiosks with a biometric collection capability (i.e., "sidecars")? How much would such an alternative cost?

Answer. Appendix F of the Regulatory Impact Assessment that was part of the NPRM, "Assumptions Used in Conducting the Assessment," stated: "The assessment of alternatives does not consider specific technical solutions." The complete *Air/Sea Biometric Exit Project Regulatory Impact Analysis* is available on the public docket through the administration's electronic docket system, *regulations.gov* at DHS–2008–0039–0003. Therefore, the proposed rule did not prohibit a "sidecar" approach to biometric collection, nor does it prohibit other configuration options, including counter-mounted, kiosk, gate devices, etc. This freedom of implementation approach for air carriers means there is a nearly infinite number of aggregate implementation configurations, including device choices and location combinations. To create an estimate, DHS assumed a specific combination of implementation approaches divided between gate and counter deployments with a certain number of post-screening point counter deployments; however, the implemented configuration of the proposed solution allows the airlines the flexibility to use any device at any appropriate location as long as the carrier meets performance standards.

Question 6c. What kinds of costs would be associated with placing new DHS-maintained and -operated kiosks in airports for biometric collection? How much would such an alternative cost?

Answer. Detailed cost estimates for a DHS-maintained and operated kiosk solution are provided in the Regulatory Impact Analysis, under Alternative 4.

QUESTIONS FROM CHAIRWOMAN LORETTA SANCHEZ FOR DOUGLAS E. LAVIN, REGIONAL VICE PRESIDENT FOR NORTH AMERICA, INTERNATIONAL AIR TRANSPORT ASSOCIATION

Question 1a. DHS's proposed rule for US–VISIT Exit at airports would require the airlines to collect, transmit, and store a passenger's biometrics. DHS maintains that air carriers will simply be collecting another "data point." However, according to the Notice for Proposed Rulemaking, collecting this data point will require air carriers to "upgrade their existing systems" and "create and enhance systems to handle the larger amount of data inherent in biometric transmissions," and will cost carriers roughly $3.5 billion over 10 years.

What will air carriers be required to "upgrade" or "enhance" and at what cost?

Answer.

Systems Changes

Carriers would be required to upgrade and enhance their departure control systems (DCS)—the systems that enable passengers to check in, allocate seats, transmit API data and issue boarding passes. However, many carriers' DCS systems reside on mainframes or on mini-computers. These legacy systems are character-based, complex and difficult to maintain. They are not designed to store or to display images. Indeed, many systems are not capable of such a function. Existing messaging formats, both within carriers' networks and for external transmission of data, are not designed for, or capable of, transmission of pictures of fingerprints (binary image) data.

The NPRM indicates that carriers will be required to transmit the biometric portion of the passenger manifest data to US–VISIT in an XML data format that contains biometric images. What the NPRM fails to acknowledge is that the SITA and/or ARINC communication systems used by the large majority of airlines operating in the United States do not support XML data format messaging. We are also not aware of any communications systems used to support international airline operations that can accommodate image transmission. No industry standard XML format exists today to support transmission of API data. Absent detailed technical information from DHS, we are unable to effectively evaluate whether existing systems will be capable of upgrade to accommodate this new data transmission or whether new networks would need to be installed to support this program.

Costs

For the reasons above, we believe that a wholesale upgrade to a new DCS platform would be required for many carriers, plus the acquisition of hardware capable of capturing fingerprint images, and the upgrade of all airport networks.

The NPRM estimates that carriers would incur costs ranging from $3.5 billion to $6.4 billion to fund the proposed US–VISIT Exit program. Unfortunately, US–VISIT does not offer sufficient methodology or expense categories to fully explain their calculations, nor does the NPRM adequately spell out even the high level elements that would drive implementation costs to this range.

IATA has worked with our member airlines, network service providers, and hardware manufacturers to scope the cost of both the NPRM and also the accompanying Privacy Impact Analysis (PIA). IATA believes that the proposed rule may cost the

airline industry as much as $12.3 billion over 10 years. This represents $5.9 billion above the highest 10-year cost estimate by DHS. We believe that technical issues highlighted previously in this document and certain critical erroneous assumptions largely drive this estimate.

One of the critical erroneous assumptions throughout the NPRM is the apparent DHS belief that airline networks have the same data transmission capabilities as Internet-based networks. As explained elsewhere in this document, airlines maintain or lease highly specialized networks optimized to transmit character-based data. Airlines do not transmit video or pictures as part of the reservation, booking, or departure control process.

We are particularly concerned about three critical costs omitted from the NPRM, two of which are mandated by the PIA. These costs include data transmission, deployment of new global dedicated secure networks, and deployment of specialized secure data warehouses.

Question 1b. If DHS publishes its final rule by December 2008, can air carriers make all the needed changes to their systems by June 2009?

Answer. No. Capturing a fingerprint picture, storing it in a legacy system environment, and then adding that image file to the API message is in no way comparable to simply adding an additional data field and would require a major upgrade to many airlines' systems. To put this into perspective, the amendment to capture the passenger's address for US APIS (that did not require new hardware or storage of anything other than character data) took airlines in excess of a year to complete. Any modifications to include biometric collection would take substantially longer and be significantly more expensive.

In addition to DCS upgrades, hardware would need to be acquired in all locations (which may not even be readily available in the quantities required to equip all points of check-in, transfer and boarding). Airport networks and power supplies would need to be upgraded and systems installed at all locations. The upgraded systems would need to be re-certified and tested, not only by airlines and DHS, but by network and systems providers, as is required of all systems in the airport environment.

We estimate that this may take in the region of 2 years; 6 months is in no way realistic for a project of this magnitude.

Question 2a. DHS outlined a number of alternatives in its proposed rule for US–VISIT Exit at airports and even suggested that it would consider combining a number of alternatives, including the use of a kiosk.

Is there a biometric collection alternative or combination of alternatives that IATA favors?

Answer. The centralized collection by DHS of biometric data at a single point in the passenger flow is far more efficient, secure and cost-effective than making significant amendments to every point of passenger contact (check-in desks, kiosks, gates and transfer desks.) The collection of data through DHS-supplied, stand-alone, dedicated kiosks positioned within the passenger flow is the preferred alternative.

Question 2b. If DHS publishes a final rule that is closely related to IATA's preferred alternative, do you believe it would be technologically feasible to implement it by June 2009?

Answer. Most likely not, but this is the fastest option available to Congress. DHS is asking to implement a significant program in unrealistically limited time frames. Feasibility would depend on the availability of hardware to create a sufficient number of kiosks, the ability to install kiosks in the airport environment, and the availability of the airline and airport resources needed to make changes to accommodate passengers affected by US–VISIT Exit. One major benefit in terms of deployment time is the existence of the DHS software developed for stand-alone DHS kiosks used in the US–VISIT Exit pilot trials. We believe that this could be immediately used with little modification by DHS in the kiosk model under consideration. Certainly, advantages of DHS kiosks would include the deployment of a fewer number of kiosks and the need to develop only a single software and hardware platform—as opposed to the many variations that would need to be produced if 120 individual airlines took on this task.

On this topic, the committee should note that the airline industry is committed to working with DHS to efficiently and effectively implement the 9/11 law. Once the industry receives sufficient information on any DHS kiosk alternative, we will be better-positioned to provide realistic time frames on hardware availability and programming needs.

Question 3a. Over the last few years, air carriers have been tasked with implementing a number of Federal security initiatives, including US–VISIT, the Electronic System for Travel Authorization (ESTA), Secure Flight, and APIS Quick Query, to name a few.

What are the different requirements of these five programs and what impact does each program have on your day-to-day operations?

Answer.

API

Advanced Passenger Information is required to be sent by airlines to CBP for each passenger on an international flight to or from the United States. Information is screened for customs, immigration, and border control purposes. In addition, it may be passed to TSA for additional security screening. API is also provided for crew.

The impact of API has been two-fold. Firstly, the iterative nature of the development of the program has meant that carriers have had to repeatedly make system changes to keep up with new requirements. For example, the project to gather address and other new data elements and to change the previously existing API messaging format to UN/EDIFACT in 2005 took many carriers in excess of a year to complete and incurred IT costs of up to $3 million U.S. per carrier. Systems changes were required to departure control systems, check-in kiosks, Internet check-in applications, messaging standards and networks for transmission of data between airlines. Indeed, some networks are still not capable of enabling API collection for through check-in of international passengers on multi-leg journeys involving more than one airline in the itinerary.

AQQ

No sooner than the project for enhanced API collection was complete, the APIS pre-departure program was initiated to gather API information, whether through the real-time AQQ system or in a batch transmission sent 30 minutes in advance of departure. The AQQ program provides real-time processing and response to API information. Passenger data is automatically screened for immigration, customs, and no-fly purposes, and a board/no board decision is then sent the airline.

This has meant either for another significant upgrade to airline departure control systems to transmit and receive API on a per-passenger real-time basis, or for carriers to close flights 30 minutes before departure (which is not, in most circumstances, possible for any scheduled carrier.)

Operationally, the impact remains untested, as most carriers are not yet live with AQQ—passengers will need to wait at check-in for a real-time response from the AQQ system. CBP has set a service standard of sub-four seconds response time. For transit passengers, many carriers will no longer be able to through-check international passengers to their connecting flight into the United States, as the initiating carrier will not be able to receive an AQQ response.

For international carriers, a positive step is that responsibility for watch list vetting will be undertaken by CBP when AQQ becomes live.

ESTA—Electronic System for Travel Authorization

Data will be collected via a web portal up to 2 years in advance of travel. This will be mandatory by January 2009. All visitors to the United States under the Visa Waiver program will need an ESTA in order to board an aircraft to the United States.

The ESTA rule fails to address the issue of how to respond to passengers who have not established an ESTA prior to initiating travel to the United States or whose ESTA might have been canceled or have expired. Absent an effective mechanism that addresses the need for Government-supported day-of-departure applications at airports outside of the United States, including smaller regional airports feeding into the primary transfer hub locations, IATA anticipates that full implementation of this proposal will result in thousands of visitors being prevented from traveling each month.

Infrastructure (public internet access, etc.) at most, if not all, international airports is insufficient (if not non-existent) to respond to a significant number of individuals at any single airport who are attempting to travel without having previously filed for and obtained an ESTA.

Detailed technical information relating to ESTA and its requirements was published in the revised U.S. Consolidated Users Guide only in late July. The industry has insufficient time to develop and implement changes in the specified time frames. ESTA will require all carriers serving the U.S. market to develop an automated capability within Departure Control Systems necessary to receive and understand the ESTA status indicator relating to each passenger, at a time when programming resources are fully allocated to responding to additional U.S. and other governments' mandates. ESTA seriously disrupts carriers' efforts to develop systems necessary to implement CBP's Pre-Departure Passenger Manifest (AQQ) functionality.

The majority of ESTA data requirements are duplicative in nature, such as the collection of an address in the United States provided as part of the initial ESTA

application. Since an ESTA is valid for 2 years, it makes no sense to collect an address for the initial visit as that address would likely not be known or would be subject to change. It also duplicates entirely the purpose of API, the address collection being a major enhancement made only 2 years ago. In addition, inclusion of the security questions as part of the data collection process (such as passenger's involvement in criminal or political activity and presence of communicable disease) precludes any opportunity for carriers to collect data on behalf of passengers due to privacy issues. IATA questions the relevance of the collection of these data items in relation to today's international travel environment.

PNR

Data collected by airlines during the reservation process is supplied to CBP for prescreening of passengers. There are numerous legal implications regarding the supply of PNR data—carriers are only just developing a "push" mechanism to provide data to CBP in accordance with EU data protection rules. However, CBP requires four individual timed pushes of the same data per flight, plus the ability to acquire ad-hoc data. Since reservation data rarely changes, this requirement seems duplicative and disproportionate and incurs high transmission costs for carriers.

In addition, international carriers are required to perform their own screening of PNR data to meet TSA's domestic selection criteria for passengers departing the United States. This requirement has restricted the use of on-line check-in and issuance of home printed boarding passes for many passengers, as international (non-U.S. flag) carriers are not permitted to use TSA's CAPPS screening systems.

Secure Flight

The Secure Flight program will enable TSA screening of all domestic and international passengers against the watch lists and no-fly lists. PNR and APIS information is used to select passengers for additional screening measures (secondary) and, in some cases, even denial of boarding. Secure Flight, AQQ and ESTA requirements have been published in a "consolidated" user guide. However, in reality this document reflects three different sets of requirements.

Secure Flight proposes transmission of select API data elements, using an entirely new message format and differing data submission timelines in contrast to those that will continue to be required under the AQQ program. Secure Flight will also include additional transmissions of PNR data supplemental to those already provided to CBP. For international carriers (both U.S. and foreign-flagged), this will mean another round of programming effort, duplicative data transmissions, and zero coherence between programs.

Question 3b. How can the different requirements of these programs be better integrated to prevent unnecessary or duplicative efforts?

Answer. We strongly recommend that the only option available to avoid the needless duplication, increased costs, and inefficiencies associated with different passenger information programs is to work together across all the relevant agencies to develop a single harmonized program. The program should draw together components from Secure Flight, API/AQQ, CAPPS and US–VISIT Exit to utilize a combination of all data sources to verify the passenger's identity and that he/she is genuinely allowed to travel. In addition, ESTA should use API data to determine entry eligibility rather than duplicating data collection.

We suggest that biometric data for US–VISIT Exit should be collected by DHS using a dedicated, secure, Government-run system inserted directly into the existing passenger flow (for example, at a kiosk during wait time for the security check point).

Using Secure Flight and/or API data, TSA would be able to validate that a passenger should be traveling, therefore removing any concerns regarding falsified boarding passes. The same validation process could also determine whether a passenger needed to have their biometric collected (according to their destination and nationality) and, at the same time, perform immigration and watch list checks.

Question 4a. DHS and the air industry worked very closely to implement US–VISIT entry at airports, but the partnership apparently deteriorated when DHS began developing its biometric exit system and ESTA.

Please describe the dialog IATA had with DHS as it was developing its plans to implement US–VISIT Exit and ESTA.

Answer. There has been little to no two-way dialog regarding US–VISIT Exit between IATA and DHS since the inception of the program. IATA hosted a meeting in July 2007 between DHS and carriers to discuss concerns with the US–VISIT Exit program and to make proposals on how biometric capture could best be approached, but DHS was not willing (or able) to openly discuss these issues. It should be noted that a full year passed between when US–VISIT made its initial declaration that

carriers would be forced to implement biometric data capture under US–VISIT Exit and when the agency published its NPRM. Carriers were categorically told, as recently as June 19, 2008, that it would be their obligation to meet US–VISIT Exit requirements and that DHS did not have the funding or the ability to fulfill that role.

To reiterate, during the past 16 months, IATA has repeatedly made representations to DHS but has been unable to set up a meaningful dialog.

In terms of ESTA, the CBP program team has been very open in discussing options, issues and listening to proposals from carriers. However, it has been clear that in moving to an interim final rule with no opportunity to comment on the proposed rule, CBP is under pressure to implement the program regardless of carriers' concerns about lack of systems and public preparedness.

Question 4b. Your cost estimate for US–VISIT Exit ($12 billion) is significantly higher than the number DHS provided ($3.5 billion). Why is there such a disparity between the two cost estimates? Did DHS reach out to IATA to better understand the costs involved with US–VISIT Exit?

Answer. The NPRM makes several critical erroneous assumptions that dramatically drive up the cost of an airline-operated US–VISIT Exit system.

First, DHS assumes that airport networks are designed to transmit large image files and work like the Internet connections many of us have in our homes. Nothing could be further from reality. Airport networks are low-bandwidth, highly optimized networks designed for transmitting small text files. It is highly likely that major upgrades or replacement of airport networks would be necessary. The NPRM also assumes that airline check-in systems can simply be changed to include a further data item (the fingerprint image) in the API transmission. However, airlines' systems are not designed to capture, store or transmit image data; a major upgrade or even replacement of many airlines' systems would be required to accommodate this requirement. This upgrade would include hardware acquisition, installation, testing, and certification at every check-in, transfer and gate facility in the United States serving the international market.

The US–VISIT Exit data requirement would also overwhelm existing networks by increasing message volume 350–800 times and would dramatically increase transmission costs paid to providers. We estimate that the average size of an API passenger manifest requirement under US–VISIT Exit would increase from today's 100KB (for 400 passengers) to approximately 31.35 MB for the same flight. API transmission costs are based on the size of the transmitted block of data; if data transmission costs increased proportionately, this would lead to costs in the region of millions of additional dollars per month for most airlines.

It is IATA's conclusion, based on consultation with airlines and service providers, that a wholesale rework of carriers' legacy departure control systems and data networks would be required to capture, store and transmit image data. As there is a wide variety of network systems and airline Departure Control Systems in use, this would involve many different integrators and many IT suppliers across the globe.

Secondly, DHS has added additional encryption requirements for collection, storage, and retention of fingerprint images. We do not believe that DHS's calculations factored in costs associated with this requirement. As indicated in our comments submitted in response to the NPRM, airlines today do not operate with systems or data transmission lines that would meet the requirements of a "secure" system as envisaged in the DHS Regulatory Impact Analysis. Such systems, if ultimately required under a final rule, would need to be designed and put into service—with first-year costs likely exceeding $1 billion across the industry.

There was little detailed discussion of the proposals that US–VISIT was developing, including any frank and open discussions of costs that might be incurred by the industry under the US–VISIT Exit program. Certainly, IATA was not party to any discussions concerning existing airline system capabilities, or costs that might be incurred to expand those capabilities to respond to US–VISIT Exit's operational requirements.

Our first indication of US–VISIT's projections for costs to industry came only with the publication of the NPRM. We immediately questioned the validity of the financial projections contained in the NPRM due, in large part, to the conspicuous absence of methodologies used to establish the figures presented in the filing. We found the same absence of explanatory justification in the associated Regulatory and Privacy Impact Analysis supplements.

IATA provided a cost analysis in its submission to the NPRM. Without necessary information detailing what DHS used to establish its estimates for both immediate and longer-term costs over 10 years, it would be speculation on our part to try to establish the cause of differences in our projections.

Question 5a. It is my understanding that the air travel industry is regulated by a number of international agreements.

What types of international agreements must DHS consider when implementing programs like US–VISIT and ESTA?

Answer. DHS must consider ICAO's Annex 9 to the Chicago Convention, which prescribes standards for the provision of passenger data. Annex 9 also refers to the WCO/ICAO/IATA Guidelines for passenger data, and to the UN/EDIFACT PAXLST message standard (adopted as an Annex to the WCO/IATA/IACO Guidelines) which describes the method and form of transmission allowable.

Since its original adoption in 1993, the United States has repeatedly ignored the agreed international standard for API message construction, and has made unilateral changes to that format. The result has been that in addition to airlines, the WCO and the other governments that have adopted the WCO's API messaging standard have been forced to retroactively modify the standard (and in many cases, their own API systems).

This unilateral approach has led to a series of modifications to existing API systems at significant costs to parties (both public and private) other than the U.S. Government and, ultimately, to a non-standard U.S.-centric API and AQQ application.

However, it should be noted that CBP has actively engaged with IATA in terms of PNR data standards and is working cooperatively on a new standard for a push mechanism. It will be imperative that TSA takes the same approach for Secure Flight.

Question 5b. Will the implementation of US–VISIT or ESTA, as currently proposed by DHS, contradict any of the industry's international agreements and require subsequent modifications?

Answer. ICAO's Annex 9 does not envisage collection of a biometric as a requirement for departing passengers and, therefore, sets forth no guidance in this matter. If, however, biometric data were considered part of API (as suggested by the NPRM), then the US–VISIT Exit requirement would be in contravention of the industry standards in place for passenger data as described in Annex 9 section 3.47.1. Amendments to the WCO/ICAO/IATA guidelines and the UN/EDIFACT messaging standards would be required to accommodate the additional data, if it were even possible to include image data in the standard message.

International agreements and standards do not preclude electronic application for visa applicants (as in the ESTA program), and indeed this is a positive step forward in terms of facilitation, if implemented correctly. However, the program is duplicative in nature and is likely to cause severe disruption and denied boarding for many passengers at many airports, as adequate preparation has not been made for the introduction of the program.

The Annex makes specific references to Contracting States being required to use applicable technology and multi-channel inspections systems to expedite clearance inspections, to secure the highest practical degree of uniformity in regulations, and to ensure that facilities are provided on terms no less favourable than those which apply to the operators of other modes of transport. The Annex also lays down a goal time of 60 minutes for processing of passengers, including check-in, aviation security and outbound border controls. Introducing both US–VISIT Exit and ESTA is likely to significantly add to current passenger processing time, taking it well beyond this recommendation. Although it is subjective whether US–VISIT Exit proposal is in direct contravention of these Annex 9 standards and recommended practices, is does appear to fly in the face of the principles laid down.

Within the airline industry itself, we would anticipate that implementation of new requirements under the US–VISIT Exit and ESTA initiatives would drive a need for sweeping changes to existing industry standards (Passenger Conferences Resolutions) and interline policies and practices bearing on the relationship between two or more carriers involved in single itineraries. As much of what both new programs would require of airlines is entirely new—it is hard to say that any specific provisions would conflict with existing industry-agreed standards. On the other hand, the proposals would require significant modification to industry standards relating to:

- Interline Message Construction;
- Origin Carrier Responsibilities in Interline Itineraries;
- Ground Handling Agreements;
- Denied Boarding and Compensation;
- Involuntary Rerouting—Processes and Handling.

QUESTIONS FROM CHAIRWOMAN LORETTA SANCHEZ FOR GREG PRINCIPATO, PRESIDENT, AIRPORTS COUNCIL INTERNATIONAL—NORTH AMERICA

Question 1a. With respect to the previous US–VISIT air exit pilots, DHS has indicated that it encountered numerous problems with airport authorities regarding space and signage. For example, in certain airports DHS was unable to place as many exit kiosks as it would have liked or in the locations it would have liked. According to the Notice for Proposed Rule Making (NPRM) for US–VISIT air and sea exit, compliance with biometric exit collection "depended on the convenience of the process."

Can you describe the space and signage challenges that DHS refers to in the NPRM?

Answer. DHS has not discussed with ACI–NA the problems that it has indicated it encountered at U.S. airports. DHS may be referring to U.S. airport regulations and facility constraints. Numerous parties seek access and signage at airports for a wide variety of governmental, commercial, charitable and other purposes. Each airport has regulations and procedures in place to manage access and signage requests at their facilities. When considering such requests, airports must take into account available space, which is often limited; existing contractual obligations for space with airlines, concessionaires and others; and the financial implications of various uses of its facilities as revenues generated from concessions contribute greatly to the economic viability of airports and, in some cases, reduce costs to the airlines. Airports also need to ensure that signage is clear and uncluttered so that passengers can actually find what they are seeking. The requirements for implementing the US–VISIT Exit pilot program differed on an airport-by-airport basis depending on the layout, space availability, types of traffic, types of equipment used, and existing legal obligations.

Question 1b. How can DHS move beyond these challenges to ensure US–VISIT Exit has the necessary signage and space it needs to be implemented successfully at airports?

Answer. ACI–NA recommends that part of the solution is the use of mobile kiosks and other mobile devices, which are not hard-wired, to perform the collection function. Mobile devices will permit quick and easy redeployment of the collection process should airport or airline operations necessitate a change of gate. Mobile devices would reduce costs and increase efficiency for DHS while minimizing the impact on airports. After the implementation of US–VISIT Exit, changes may be necessary to take account of experience to improve the process. Therefore, DHS should not take an approach that will require structural changes.

ACI–NA believes that a mobile approach will allow airports to be more flexible in their dealings with DHS. However, each airport must take into account differing regulations, contractual obligations and facility constraints. We believe that U.S. airports will want to assist their departing passengers in complying with a mandatory U.S. travel requirement which could affect their ability to catch their flights and to visit the United States again. It is critical that DHS consult with airports and airlines as the program is implemented to ensure that it operates as smoothly and efficiently as possible and does not result in alienating foreign visitors to the United States.

Question 2. DHS and the air industry worked very closely to implement US–VISIT entry at airports, but the partnership apparently deteriorated when DHS began developing its exit system and the Electronic System for Travel Authorization (ESTA).

Please describe the dialog ACI–NA had with DHS as it was developing its plans to implement US–VISIT Exit and ESTA.

Answer. There was good communication between the US–VISIT Program Office and the aviation industry during the rollout of the US–VISIT Exit pilot program. However, DHS did not share its June 14, 2005 evaluation of the US–VISIT Exit pilots, as we had repeatedly urged, until 3 years after it was completed (June 12, 2008). While DHS and US–VISIT Program Office staff have briefed us on their decisions in various venues, there have been no substantive consultations over the last few years about which approaches to US–VISIT Exit would be most appropriate, effective, and efficient.

U.S. Customs and Border Protection (CBP) has provided briefings on ESTA in various settings. ACI–NA would not characterize such briefings as a dialog regarding the implementation of ESTA. We were particularly disappointed that CBP did not issue a Notice of Proposed Rulemaking (NPRM) on ESTA, but rather moved directly to issue an Interim Final Rule (IFR) on June 9, 2008 on which it sought comments. We believe the NPRM process would have allowed for more thorough consid-

eration of and input by the public on critical implementation and operational issues in developing the ESTA program.

Question 3a. DHS outlined a number of alternatives in its proposed rule for US–VISIT Exit at airports and even suggested that it would consider combining a number of alternatives, including the use of a kiosk.

Is there a biometric collection alternative or combination of alternatives that ACI–NA favors?

Answer. ACI–NA maintains that DHS should fund, staff and operate the US–VISIT Program. The collection of the biometrics of departing foreign visitors should take place in the sterile area at the airport where the traveler is ultimately departing the United States (i.e. last airport of departure), using mobile kiosks or other mobile wireless devices, rather than static, hard-wired devices. To ensure the program is as effective as possible, DHS should consult on an airport-by-airport basis with the airport authority and airlines about the deployment of US–VISIT Exit. DHS should not divert CBP and TSA staff performing existing security procedures, but rather should add staff to implement the US–VISIT Exit function.

Question 3b. If DHS publishes a final rule that is closely related to your preferred alternative, do you believe it would be technologically feasible to implement it by June 2009?

Answer. ACI–NA believes that it would be technologically feasible to implement our recommended approach by June 2009 because the technology is available. Mobile devices would minimize the need for structural changes to airports and allow for flexibility to respond to different and changing operating environments. However, we do not know whether a sufficient number of mobile devices would be available to implement the exit procedures. We also do not know whether the DHS budget and procurement process would make it possible to implement the approach by June 2009.

○