FISCAL YEAR 2006 BUDGET

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MARCH 2, 2005

Serial No. 109–3

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
20–904 PDF WASHINGTON : 2005

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

Committee on Homeland Security

Christopher Cox, California, *Chairman*

Don Young, Alaska
Lamar S. Smith, Texas
Curt Weldon, Pennsylvania, *Vice Chairman*
Christopher Shays, Connecticut
Peter T. King, New York
John Linder, Georgia
Mark E. Souder, Indiana
Tom Davis, Virginia
Daniel E. Lungren, California
Jim Gibbons, Nevada
Rob Simmons, Connecticut
Mike Rogers, Alabama
Stevan Pearce, New Mexico
Katherine Harris, Florida
Bobby Jindal, Louisiana
Dave G. Reichert, Washington
Michael McCaul, Texas
Charlie Dent, Pennsylvania

Bennie G. Thompson, Mississippi
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
Bill Pascrell, Jr., New Jersey
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida

Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Daniel E. Lungren, California, *Chairman*

Don Young, Alaska
Lamar S. Smith, Texas
John Linder, Georgia
Mark E. Souder, Indiana
Tom Davis, Virginia
Mike Rogers, Alabama
Stevan Pearce, New Mexico
Katherine Harris, Florida
Bobby Jindal, Louisiana
Christopher Cox, California *Ex Officio*

Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Peter A. DeFazio, Oregon
Zoe Lofgren, California
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., New Jersey
James R. Langevin, Rhode Island
Bennie G. Thompson, Mississippi *Ex Officio*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

Material Submitted for the Record

INTEGRATING HOMELAND SECURITY SCREENING OPERATIONS

WEDNESDAY, MARCH 2, 2005

House of Representatives,
Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity,
Committee on Homeland Security,
Washington, DC.

The subcommittee met, pursuant to call, at 2:05 p.m., in room 2318, Rayburn House Office Building, Hon. Daniel Lungren [chairman of the subcommittee] presiding.

Present: Representatives Linder, Davis, Rogers, Pearce, Cox, Sanchez, Dicks, DeFazio, Lofgren, Pascrell, and Thompson.

Mr. Lungren. [Presiding.] The Committee on Homeland Security's Subcommittee on Economic Security Infrastructure Protection and Cybersecurity will come to order.

The Subcommittee is meeting today to hear testimony on the DHS proposed fiscal year 2006 budget relating to the integration of homeland security screening operations.

As we begin the first ever hearing of this Subcommittee, I would like to start by thanking Chairman Cox and Ranking Member Thompson for their leadership in helping to establish this committee as a permanent standing committee.

I would like to also thank Chairman Cox for giving me the honor of chairing this critically important Subcommittee.

I look forward to working with Chairman Cox and Ranking Members Thompson and Sanchez and all members of the Committee on both sides of the aisle in the coming years.

I am also excited personally to be back serving in the Congress. I came back because of my genuine desire to help this country tackle its greatest challenge since the fall of communism: The specter of international terrorism, particularly terrorists armed with weapons of mass destruction. It is my sincere hope we can work together to accomplish this important work, the important work of this Subcommittee, in a non-partisan manner driven by rational risk assessments and always putting the good of the Nation above partisan politics.

This Subcommittee has a vital role to ensure that our homeland security policies strengthen our nation and protect our economic as well as physical security. As we know, our terrorist enemies seek not only to kill Americans but also to weaken our economy and destroy our way of life.

In the broader sense, this Subcommittee will lead the Committee's efforts in answering several fundamental homeland security questions: Which critical assets and infrastructure require protection, and how do we prioritize our investments in a world of finite resources? What are the appropriate homeland security roles and responsibilities of Federal, State and local governments?

And as a former Attorney General of California, I am very, very concerned about that and also the responsibilities of the private sector. How do we ensure that our investments in securing the homeland do not subtract from but actually contribute to promoting our national economic security? Answering these questions correctly will ensure that our collective work makes a real difference for our nation, for the citizens we serve and for the critical new department that we oversee.

With that background, we now turn to the focus of our hearing today. Since the tragic events of September 11, 2001, the Congress and the Administration have created numerous new programs or enhanced old ones aimed at screening individuals and cargo entering the United States or accessing critical parts of our infrastructure. However, these actions were taken in a piecemeal fashion serendipitously, usually in reaction to some event rather than as part of a strategic effort to build a comprehensive, integrated screening system.

The 9/11 Commission in its final report last summer faulted this patchwork system of screening as leaving the Nation vulnerable to terrorist attacks, and that Commission called for a new system that fully integrates our border, transportation and critical infrastructure screening activities. The proposed Office of Screening Coordination and Operation, or SCO, as we will come to know it, appears to be a step forward in the right direction towards meeting the 9/11 Commission recommendations.

This new office seeks to consolidate and coordinate the US–VISIT Border Security Program, certain registered or trusted traveler programs, the FAST NEXUS and SENTRI cargo security and expedited border crossing programs, background checks and credentialing for persons working in high security areas of our transportation system and for those seeking to transport hazardous materials within the U.S. and background checks for foreign nationals seeking flight training in the U.S.

The President's budget seeks approximately $847 million for this operation in fiscal years 2006 and based on some data we got that is a significant increase over those expenditures for those programs in the current year.

We as a nation need to establish our homeland security priorities, and that does not simply mean increasing the budget. The Homeland Security Committee is charged with the most important mission of our government today, I believe, protecting our citizens from the threat of global terrorism. I assert that we must continue to adapt to the changing tactics of our enemy and directly fight the transnational Islamic fascism of those who elect terrorism as their weapon of choice.

This Committee and the Congress must seek to spend the taxpayer money wisely and efficiently to demonstrate the most effective way to protect as many Americans as possible. We must create a homeland security strategy based on rational risk assessment rather than pork barrel politics. And when taxpayer money is allocated for the defense of our homeland, we must ask one simple question: Is spending on this specific program the most productive means to safeguard our citizens?

I believe this new office has the potential to enhance our homeland security by improving the efficiency and effectiveness of our terrorist-related screenings. It also has the potential to expedite cross-border movement of low-risk persons and goods and reduce bureaucracy and administrative burdens on the traveling public and enhancing our economic growth.

However, many of the details behind this proposal remain somewhat understandably unclear at this time. For instance, why were some DHS screening programs proposed for consolidation while others were not? What will happen to the programs that will be placed within the new office? Will they be merged into one single program or continue to exist as distinct programs with their own unique database queries, requirements and privacy controls?

And as we attempt to do this, we should always remember that privacy controls are something that is necessary in this engagement as well.

What efficiencies and cost savings can we expect to see from this consolidation, if any? And if you can't suggest some, why not? And more importantly, how do we use this reorganization to make America more secure? I hope the witness's testimony today will allow us to begin, and I stress begin, to address some of these questions.

I would like to welcome and thank Deputy Administrator DiBattiste from TSA, Deputy Commissioner Spero from CBP, and Director Williams of the US–VISIT Program Office for appearing before the subcommittee today, and I certainly look forward to your testimony.

And it is now my pleasure to recognize the Ranking Member, Ms. Sanchez, from my home state of California for an opening statement.

PREPARED OPENING STATEMENT FROM THE HONORABLE DANIEL E. LUNGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

As we begin the first-ever hearing of this Subcommittee, I would like to start by thanking Chairman Cox and Ranking Member Thompson for their leadership in helping to establish this Committee as a permanent standing committee. And I want to thank Chairman Cox for giving me the honor of chairing this critically important Subcommittee. I look forward to working with Chairman Cox, Ranking Members Thompson and Sanchez, and all the Members of the Committee, on both sides of the aisle, in the coming years.

I also am excited to be back serving in the Congress. I came back because of my genuine desire to help this country tackle its greatest challenge since the fall of Communism—the specter of international terrorism, particularly terrorists armed with weapons of mass destruction. It is my sincere hope that we can work together to accomplish the important work of this Subcommittee in a non-partisan manner, driven by rational risk assessments and always putting the good of the Nation above partisan politics.

This Subcommittee has a vital role to ensure that our homeland security policies strengthen our Nation and protect our economic as well as our physical security. As we know, our terrorist enemies seek not only to kill Americans, but also to weaken our economy and destroy our way of life.

In the broadest sense, this Subcommittee will lead the Committee's effort in answering several fundamental homeland security questions. Which critical assets and infrastructure require protection and how do we prioritize our investments in a world of finite resources? What are the appropriate homeland security roles and responsibilities of Federal, state, and local governments, and of the private sector? And how do we ensure that our investments in securing the homeland do not subtract from, but actually contribute to promoting, our national economic security. Answering these questions correctly will ensure that our collective work makes a real difference for our Nation, for the citizens we serve, and for the critical new Department that we oversee.

With that background, we now turn to the focus of our hearing today. Since the tragic events of September 11, 2001, the Congress and the Administration have created numerous new programs, or enhanced old ones, aimed at screening individuals and cargo entering the United States or accessing critical parts of our infrastructure. However, these actions were taken in a piecemeal fashion, usually in reaction to some event rather than as part of a strategic effort to build a comprehensive, integrated screening system. The 9/11 Commission, in its final report last summer, faulted this patchwork system of screening as leaving the Nation vulnerable to terrorist attack, and called for a new system that fully integrates our border, transportation, and critical infrastructure screening activities.

The proposed Office of Screening Coordination and Operations, or SCO, as we will come to know it, appears to be a step forward in the right direction towards meeting the 9/11 Commission recommendation. This new office seeks to consolidate and coordinate the US–VISIT border security program, certain registered or "trusted" traveler programs, the FAST, NEXUS and SENTRI cargo security and expedited border crossing programs, background checks and credentialing for persons working in high security areas of our transportation systems and for those seeking to transport hazardous materials within the United States, and background checks for foreign nationals seeking flight training in the United States. The President's budget seeks approximately $847 million dollars for the SCO in Fiscal Year 2006.

We as a nation need to establish our homeland security priorities, and that does not mean simply increasing the budget. The Homeland Security Committee is charged with the most important mission of our government today, protecting our citizens from the threat of global terrorism. I assert that we must continue to adapt to the changing tactics of our enemies and directly fight the transnational Islamic fascism of those who elect terrorism as their weapon of choice.

This committee and the Congress must seek to spend the taxpayer money wisely and efficiently to determine the most cost effective way to protect as many Americans as possible. We must create a homeland security strategy based on rational risk assessment rather than pork barrel politics. When taxpayer money is allocated for the defense of our homeland, we must ask one simple question, "Is spending money on this program the most productive means to safeguard our citizens?"

I believe that this new office has the potential to enhance our homeland security by improving the efficiency and effectiveness of our terrorist-related screening. It also has the potential to expedite cross-border movement of low-risk persons and goods, reducing bureaucracy and administrative burdens on the traveling public and enhancing our economic growth. However, many of the details behind this proposal remain, somewhat understandably, unclear at this time. For instance, why were some DHS screening programs proposed for consolidation, while others were not? What will happen to the programs that will be placed within the new office? Will they be merged into one single program or will they continue to exist as distinct programs, with their own unique database queries, requirements and privacy controls? What kinds of efficiencies and cost savings can we expect to see from this consolidation? And most importantly, how will this re-organization make America more secure?

I hope the witnesses' testimony today will allow us to begin to address some of these questions. I would like to welcome and thank Deputy Administrator DiBattiste from TSA, Deputy Commissioner Spero from CBP, and Director Williams of the US–VISIT program office for appearing before the Subcommittee today. I look forward to hearing your testimony.

I now recognize the Ranking Member, Ms. Sanchez, from my home State of California, for an opening statement.

Ms. SANCHEZ. Thank you, Mr. Chairman, and I would like to congratulate you on your chairmanship. And I know that we have many of the same goals, and I look forward to working with you in this Congress.

I would also like to welcome all of my colleagues on this side and on the other side to the Subcommittee, because this Subcommittee has significant jurisdiction. We have a lot of ground to cover, and it is going to take all of us working together to get all of this done. Nothing short of the security of the American people is at stake.

And, finally, I would like to welcome the witnesses that we have before us today. I am looking forward to hearing from you. And I don't really want to harp very much on this, but our Committee rules call for our witnesses to give us their written testimony no less than 48 hours before a hearing. And I say that because we didn't receive your testimony until last night at 6 p.m. And in the last couple of years that we have had this Committee, what we have seen out of this department is that we don't get the testimony in time.

And it is important for us because that way we don't waste our time on questions that are already answered in your testimony. And if we can really get to some real meat on some of these questions. So if maybe you can go back with that in mind and let your colleagues back there know also that this is a very important issue to us. I like to read it way ahead of time so I can think about what you are trying to tell me.

The hearing today is a budget hearing. What we are trying to do is to carry out our oversight responsibilities, and the beginning of each year when the President's budget comes forward we all look at the different departments and we ask the questions that we think we need to do, because we want to know whether you have enough resources to get all of those priorities and tasks that you are assigned to do or that you think you must do in order to perform your job. And ideally, we start at the macro level and then delve down into the finer details at a later hearing.

But the problem with that is that the Border and Transportation Security Directorate within DHS finds itself without a director. And I think that fact itself is a little troubling to some of us, and I would just state for the record that an organization with a mission as important as DHS cannot afford to go too long with key positions such as this one unfilled. And I hope that the new director will endeavor to correct this problem quickly so we can all get to work.

Instead of talking today about the macro look, we are really looking more focused looking at the consolidation of several of the screening programs within DHS under the one roof, Office of Screening Coordination and Operation. And this proposed consolidation is part of the President's budget, and so we want to find out today what this means, what is the scheme, what are you guys thinking about? Because it is new and none of us have seen it really before or spoken towards them.

The screening programs are very important. Many of them work well, and they can, I think, be a very powerful took to help our TSA and our CBP officers do their job catching the bad guys and protecting the public. If they don't work well, then we burden with our officers with repeatedly doing unnecessary screening of innocent people, wasting both our own resources, those officers' time, and of course the travelers' time, the legitimate travelers' time.

We also run the problem of if the innocent traveler's time is used, then our tourists and our business people will not want to travel and do the business of America, which is business. So I am very interested in particular in the database, in the coordination, if you are going to keep separate databases, if you are going to put them together, and more importantly one of the real issues of why are innocent people always repeatedly coming up and why haven't we figured out a way in which to help these people in a very fast way get them off of these lists so that they can continue to travel. And one of the indications is, for example, our own colleague, Senator Ted Kennedy, who continued to be stopped because his name was the same as somebody else on the list. And I think that is a very legitimate problem, and we need to take a look at it, and I would like some answers to that.

So I am looking forward to your testimony. I know you have a hard job. We all realize that. But now we have got a couple years of experience and we need to take these lessons learned and we need to get this better, these practices better. So I look forward to discussing this today. Thank you.

Mr. LUNGREN. Thank you, Congresswoman Sanchez.

And I would just say for the record that in the future we will expect to have testimony 48 hours ahead of time. I am not sure I will invoke the actions of the chairman of the Judiciary Committee who refuses to allow people to talk if they don't give it within 48 hours. And I know you have to work with OMB but maybe you can tell OMB that for our work we need to have this in plenty of time.

It is now my pleasure and honor to recognize the Chairman of the full Committee, the gentleman from California, Mr. Cox, for any statement he may have.

Mr. COX. Thank you, Chairman Lungren, and I want to begin by commending you on your chairmanship and Ranking Member Sanchez for the leadership that I know that you will provide to this committee, which, as has been stated, has substantial and important jurisdiction over the nation's homeland security. I want to thank you for holding this hearing today and thank our witnesses for being here to discuss these important issues with us.

In his fiscal year 2006 budget request, President Bush proposes to create a new office within DHS to integrate the multiple terrorist-related screening activities currently conducted by the Department of Homeland Security. This was a 9/11 Commission recommendation and even before that a recommendation of the Select Committee on Homeland Security in the 108th Congress. The effective management of these programs is critical to our nation's security. Coordinating them will help us identify, track and interdict terrorists and dangerous cargo that pose a threat to our homeland security.

What is proposed is a new Screening Coordination and Operations Office, as my colleagues have outlined. It would consolidate nine different screening programs from TSA and CBP into a single office, although I note not necessarily into a single screening program. The goal is to enhance terrorist-related screening and facilitate efficiency in trade and travel through risk-based assessments, while safeguarding individual privacy and civil liberties. This would be good news, and I look forward to hearing in more detail how this will happen.

I support this effort to improve integration and coordination of these screening systems which, as Chairman of the Select Committee on Homeland Security in the last Congress, I strongly encouraged the Department to undertake. In implementing this effort, it will be important for the Department to define the interrelationships and commonalities among these programs and to explicitly define the limitations and unique requirements of these separate programs.

Along these lines, I hope to hear from our witnesses today the process by which it was determined which programs were to be included in the SCO and which ones were to be excluded. For example, TSA's Secure Flight Program, which once operational will be the principal mode of screening domestic air travelers against terrorist watch lists, is recommended for inclusion within the SCO. But CBP's Advanced Passenger Information System, which is used for the screening of international passengers flying into the United States, is not proposed for inclusion within the SCO at this time. This is an issue that needs to be explored, among many others in this hearing.

Each day, our nation's transportation system moves over 30 million tons of freight and supports approximately 1.1 billion passenger trips. The Department of Homeland Security is now primarily responsible for managing the security risks to this system and the risks from this system. Quick, safe and secure access to this system by passengers and cargo must always remain a top priority, for our livelihood and our way of life depend on our ability to travel and engage in interstate commerce.

Our challenges are many and our resources are not limitless. We need to assess and prioritize the risks we face and apply our energies and resources accordingly. That is the daunting task assigned to this subcommittee. The President has asked for nearly $847 million for the new SCO office. We need to ensure we are spending our resources wisely, where they are most needed and, therefore, I look forward to hearing from our witnesses on how the SCO will move us in this direction.

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

Mr. LUNGREN. Thank you, Chairman Cox. Other members of the Subcommittee are reminded that opening statements may be submitted for the record.

PREPARED STATEMENT FOR THE RECORD FROM THE HONORABLE TOM DAVIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

I would like to thank Chairman Lungren and Ranking Member Sanchez for holding this important hearing on integrating the Department of Homeland Security's (DHS) screening operations and programs. I am pleased to be serving on the Subcommittee for Economic Security, Infrastructure Protection, and Cyber Security and look forward to participating, as this Subcommittee has jurisdiction over issues that are of personal importance to me and to the oversight work of the Committee on Government Reform, which I chair.

As Chairman, I have oversight of the federal government, including its information systems, and my staff has conducted extensive oversight on most of the programs that will become part of the Office of Screening Coordination and Operations (SCO). I applaud efforts to consolidate duplicate activities within the federal government and, in turn, reduce government waste.

I am pleased that Jim Williams, the Director of the US–VISIT program, will be testifying today. US–VISIT has shown significant progress. Our oversight of the program has shown that DHS has an excellent US–VISIT team and is moving at an appropriate pace to meet technical and organizational challenges. Currently, the wait times are down and demonstrations are being conducted on the exit end. It would be hugely disappointing to have this forward movement be interrupted. I am anxious to hear Mr. Williams' take on how consolidating US–VISIT into SCO will affect the overall strategic plan of the program.

FAST, NEXUS and SENTRI are very successful programs on our Northern and Southern borders. Not only are these programs well run by Customs and Border Protection (CBP), cargo carriers and personal travelers have shown great enthusiasm to join and participate within the boundaries of United States law. As with my concerns regarding the functioning of US–VISIT, I hope Deputy Commissioner Spero will assure the Members of the Subcommittee that the operational aspects, particularly the numbers of processed applicants, of FAST, NEXUS and SENTRI will not suffer during the transition to SCO.

My Committee monitored the Transportation Security Administration's (TSA) work on the Computer Assisted Passenger Pre-screening System II (CAPPS II). My former Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census was a requester of the Government Accountability Office's (GAO) report on CAPPS II and GAO's follow up report on Security Flight. I have concerns about moving Secure Flight to SCO, as there are outstanding issues to be resolved regarding the program. TSA will not know the results of its commercial data concept testing until April 2005. Even after receiving these commercial data test results, TSA will need to access these results and work on how to integrate commercial data into the Secure Flight program. I look forward to Deputy Administrator Dibatiste addressing these issues regarding Secure Flight and how DHS and TSA will assure Members that the mission and operability of the program will not be hampered due to the move to SCO.

I believe this will be a productive hearing and look forward to the witness testimony.

We are now pleased to have an expert panel of witnesses before us on this important topic. Let me just remind all three of you that each of your entire written statements will be entered into the record. We would ask you strive to limit your oral testimony to the 5-minute time period allotted. And that is particularly true because we are scheduled to have a vote, I believe, at 2:45 p.m. I would like to get all of your testimony in first before we are interrupted and hopefully can begin questions.

The Chair now recognizes Mr. Jim Williams, Director of US–VISIT Program, Border and Transportation Security Directorate, U.S. Department of Homeland Security, to testify.

STATEMENT OF JIM WILLIAMS, DIRECTOR, US–VISIT PROGRAM, BORDER AND TRANSPORTATION DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WILLIAMS. Thank you, Chairman Lungren.

Good afternoon, Chairman Cox, Chairman Lungren, Ranking Member Sanchez and distinguished members. It is a pleasure to be here before you today.

I would like to congratulate you on your appointment, the creation of this new subcommittee and the permanent creation of the Homeland Security Committee. I look forward to working with you to enhance our national and economic security with the transformation of our borders and the modernization of our immigration and transportation security systems.

We are here before you today to discuss the administration's proposal to create the Screening Coordination and Operations Office; a bold initiative that will enhance DHS' capabilities to secure the homeland by integrating multiple programs that support multiple Federal departments' and agencies' screening needs. We are creating a more cohesive, streamlined approach that will enhance the security of our citizens and visitors, protect personal privacy and provide better customer service for lower risk travelers.

As the Director of the US–VISIT Program, I can say firsthand that an integrated program provides tangible benefits. As we have implemented the beginning phases of US–VISIT, we have seen that collaboration works, that technology and better information management makes us more effective and that we can enhance national security without compromising economic security.

US–VISIT is a major component of border reform and modernization. It is bringing integrity back to our immigration system and demonstrating the value of incorporating biometrics into the international travel process.

To date, US–VISIT has processed over 20 million visitors. As a direct result of the use of biometrics, thousands of individuals have been denied visas by Department of State consular offices, and more than 450 criminals and immigration violators have been denied admission to the United States by Customs and Border Protection officers.

Also, through the delivery of timely and accurate information to the Immigration and Customs Enforcement officers, visas overstayers have been identified and removed from the United States. US–VISIT and U.S. Citizenship and Immigration Services are also working together to link biometric screening systems which will aid their adjudicators in making more informed decisions.

The use of biometrics and biographic data together provides Department of State consular officers, Customs and Border Protection officers and other law enforcement officials the information they need to verify identity, authenticate travel documents and identify criminals, immigration violators and others who pose a threat to our nation's security. For legitimate visitors to our country, this same access to data means that they can be processed more quickly and more efficiently while protecting their privacy.

These same benefits can be realized across our screening and credentialing programs by establishing the Office of Screening Coordination and Operations (SCO). DHS' vision of an integrated program is echoed and clarified by the 9/11 Commission and the President's Homeland Security Presidential Directive 11. Both recognize the need for a coordinated approach to managing our nation's security screening system.

Secretary Chertoff has been briefed on the SCO and has endorsed its concept. However, he is currently undertaking a major policy and operational review of initiatives facing the Department. Following this review, and subject to congressional approval of the President's budget, he will determine how the SCO and other departmental initiatives will move forward. He looks forward to sharing his thoughts on this once this review is complete. Until then I am prepared to share some high-level thinking about the need for the SCO.

Initially, DHS proposes to integrate the management and coordination of many of the Department's voluntary and compulsory people screening programs. This integration will move us closer to achieving our overall vision of secure, transparent and convenient travel, both within and across our borders. We want to build a future state whereby decision makers have complete access to the information they need, when and where they need it to make the best and most informed decision in time, every time.

The President has proposed to establish the SCO within the Directorate of Border and Transportation Security. In fiscal year 2005, DHS will develop a migration plan following the Secretary's review to ensure a seamless path for standup of the SCO.

In closing, I would like to share with you our vision. Simply put, we are creating a screening system that responds to the security and economic needs of a dynamic 21st century world. That means securing our borders from threats wherever they come from and expediting the millions of people and trillions of dollars in trade and tourism that keep our country strong.

Thank you again for inviting me to address this committee, and I look forward to working with you to make this new office successful in achieving its goals. I look forward to your questions.

[The statement of witnesses follows:]

PREPARED STATEMENT FROM JIM WILLIAMS, DIRECTOR, US–VISIT, CAROL DIBATTISTE, DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, AND DEBORAH SPERO, DEPUTY COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION

Introduction

Chairman Lungren, Ranking Member Sanchez, and distinguished Members of the Subcommittee. Thank you for this opportunity to share with you information about how the Department of Homeland Security (DHS) will enhance immigration and border management, transportation security, critical infrastructure protection and the delivery of other benefits through the establishment of an Office of Screening Coordination and Operations (SCO).

As you all well know, the Department was created to integrate security activities across the Federal government more effectively, thereby enhancing security for the American people in a manner that preserves our freedoms. Consistent with the purpose of DHS, the Administration is creating the SCO to focus on coordination of screening processes and procedures for people, cargo, conveyances, and other entities and objects that pose a threat to homeland security.

Secretary Chertoff, who was confirmed recently, has been briefed and has endorsed the concept of the SCO. As the Committee may know, he is currently undertaking a review of the major policy and operational issues facing the Department; therefore, following this review, he will determine how the SCO and other Department initiatives will move forward.

Background

As a result of the attacks of September 11, various statutory requirements and assessed security needs, the Department has instituted a number of layered security measures, including screening processes. Many of these screening processes require interoperability among systems within DHS and across the Federal government.

One example of this type of security measure using screening is the United States Visitor and Immigrant Status Indicator Technology (US–VISIT) program. This program adds biometrics to the screening process and allows the Department of State visa issuance officials to check foreign visa applicants against terrorist and criminal databases as well as other relevant data resources before a visa may be issued. Once the approved applicant arrives at the U.S. border, his or her passport and biometrics and biographic data are matched by a Customs and Border Protection (CBP) Officer, using the US–VISIT system, to ensure that the person presenting the document is the same applicant who received a visa and rechecked against the watchlists. The CBP Officer determines whether the person should be admitted into the United States or not. In addition, visitors traveling under the Visa Waiver Program are also enrolled in US–VISIT. Through US–VISIT, DHS is apprehending criminals and denying admission to other persons who have attempted to enter the United States illegally.

One of the significant achievements of US–VISIT is that privacy protections have been embedded into the operational architecture of the program. US–VISIT is staffed with a dedicated Privacy Officer who is directly involved in the development and review of all US–VISIT functions. The Privacy Officer reports both to US–VISIT management and to the DHS Chief Privacy Officer. Through this management approach, US–VISIT has been successful in identifying the potential privacy impact of new program functions, resolving issues as they arise, and making US–VISIT operations transparent to the public.

Since the tragic attacks of 9/11, the U.S. has taken many significant actions to enhance our homeland security (the enactment of the USA PATRIOT Act, the creation of the Transportation Security Administration, the Department of Homeland Security, and the implementation of US–VISIT). The 9/11 Commission report reaffirmed the importance of screening processes such as US–VISIT and called for better integration and improvement of terrorist-related processes. In addition, Homeland Security Presidential Directive-11 (HSPD 11), issued on August 27, 2004, directed DHS, in coordination with other Federal agencies, to "enhance terrorist-related screening through comprehensive, coordinated procedures. . .in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law."

The establishment of the SCO within DHS is key step to build upon the broad range of existing government and private sector security initiatives that will result in a comprehensive, coordinated and integrated screening environment.

Mission

SCO will enhance the interdiction of terrorists and the instruments of terrorism by streamlining and strengthening terrorist-related screening through comprehensive coordination of procedures that detect, identify, track, and interdict people, cargo and conveyances, and other entities and objects that pose a threat to homeland security. The mission, of course, must safeguard legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law.

By establishing the SCO, DHS will work to obtain a seamless set of systems, data, processes, and procedures coordinated with other federal agencies that would achieve many benefits: deny access to the United States, our transportation systems, critical infrastructure, and other benefits to people, cargo, and conveyances, and other entities and objects that pose a threat to homeland security; facilitate the expedited and efficient movement of people, cargo, and conveyances, leading ultimately to a better experience for travelers, shippers and anyone else who engages with our screening programs; promote better public awareness of and compliance with screening programs; create more operational efficiency through integration and the elimination of duplicative efforts across the government; ensure the integrity of the screening systems, and; protect personal and institutional privacy and other rights and freedoms that are essential to our way of life.

The streamlining and integration of these programs by the SCO will result in greater accuracy in screening and provide for consistent policies and training on the protection of civil liberties and privacy.

Another critical element of effective screening is effective information sharing and collaboration. The SCO will work closely with DHS' Information Sharing and Collaboration Office (ISCO) to coordinate intra-agency information sharing and collaboration requirements related to screening efforts as these are identified. The ISCO is located within DHS' Information Analysis and Infrastructure Protection Directorate.

SCO Organization

As proposed in the President's fiscal year 2006 budget request, the SCO would integrate program management of the following DHS screening activities:

- US–VISIT (United States Visitor and Immigrant Status Indicator Technology (US–VISIT)
- Secure Flight domestic passenger prescreening (TSA)
- International Flight Crew Vetting (TSA)
- Free and Secure Trade (FAST—driver registration only) (CBP)
- Nexus/SENTRI (CBP)
- Transportation Worker Identification Credential (TWIC) (TSA)
- Registered Traveler (TSA)
- Hazardous Materials Commercial Driver Background Checks (TSA)
- Alien Flight Student Background Checks (TSA)

The first phase of the SCO will integrate screening processes that focus on people.

While the Secretary has endorsed the SCO concept, there are many critical details still to be determined. For that reason, the Secretary is currently undertaking a full review of this proposal, including such issues as: the appropriate structure for the SCO; its relationship to operational entities; and the migration plan to smoothly transition for fiscal year 2006. The Department recognizes the Congressional interest and oversight responsibility in this area, and, once the review is completed, will share and discuss further how the SCO is implemented. While work is ongoing, progress on the screening programs that have already been initiated will, of course, move forward.

A key element of the success of the SCO is contained in the fiscal year 2006 request for Screening Administration and Operations. The fiscal year 2006 request includes $526 million and 192 FTEs in direct appropriations, and $322 million and 63 FTEs in fee funded authority. Specifically, in the direct appropriations, the request includes an increase of $50.2 million for the US–VISIT program, $49.4 million for the Secure Flight and crew vetting programs, and $20 million for Screening Administration and Operations. Included in this $20 million dollar line item is $6 million for 32 full-time equivalents (FTEs) who would be responsible for the delivery of this $847 million enterprise, because within the SCO, a cadre of experts will be needed to provide leadership and management for the effective and efficient integration of screening activities. In the fee funded accounts, the request includes authority to collect and expend $244.7 million for the TWIC, $22.5 million for Registered Traveler, $44.2 million for Hazardous Materials Truck Driver checks, and $10 million for Alien Flight School background checks.

And now, we would like to provide the Committee with an update on some of the key programs proposed in the President's budget for inclusion in the SCO.

US–VISIT

In January of 2004, US–VISIT was successfully implemented at all 115 U.S. international airports and 14 seaports. In December of 2004, US–VISIT technology was expanded to the nation's 50 busiest land border crossings. Since its been in operation, more than 450 people with records of criminal or immigration violations have been prevented from entering the United States.

US–VISIT intends to institute additional functional capabilities at the land borders, in particular radio frequency technology. In fiscal year 2005, US–VISIT will pilot this enhanced technology at various land border sites. This will provide US–VISIT with the information necessary to develop detailed plans and technical and infrastructure costs to determine the number of locations where entry/exit lanes and accompanying procedures can be implemented in fiscal year 2006.

US–VISIT is also working on the vision for the 21st century immigration and border management system. Through this initiative, US–VISIT will provide a new information module to field offices and agents—enabling them to see relevant and timely data from all partnering agencies about a person, not just about a single transaction. This investment will ensure that DHS and Department of State officers have comprehensive, accurate, relevant, and timely information in a single electronic view of a traveler (e.g., dates of previous entries and exits, watchlist, current immigration status, and immigration benefit status). This module will assist in identification of potential terrorists offshore, before they board an airplane, bus, cruise ship, car, or cargo vessel to travel the United States or when they change their status. It will provide a comprehensive mechanism for name vetting of visa applicants to DOS and DHS that provides the basis for the human element involved in the visa issuance process.

The SCO should leverage the strong foundation of screening processes developed and fielded by US–VISIT, such as its work with biometric standards, and multi-agency application processes, by applying those fundamentals to other screening activities.

Secure Flight

On August 26, 2004, the Secretary announced that DHS would pursue a new domestic pre-screening program called *Secure Flight.* This program will be piloted with two carriers in August 2005. Like US–VISIT, TSA's Secure Flight program would also transfer to the proposed SCO. The Secure Flight program would address the 9/11 Commission recommendations regarding use of watch lists, and would reflect recommendations received from Congress, the privacy and civil liberties communities, the aviation community, airline travelers and DHS's international partners.

Secure Flight will shift the responsibility for checking passengers against terrorist watchlists from domestic and foreign air carriers to the Federal Government. This will improve the consistency of and response to watch list comparisons. Domestic flight passenger name record (PNR) information will be compared against records contained in the Terrorist Screening Center Database (TSDB). *Secure Flight* will significantly improve the Federal government's ability to prevent terrorists from boarding aircraft, help move passengers through airport screening more quickly, and reduce the number of individuals selected for secondary screening, while fully protecting passengers' privacy and civil liberties.

Consolidating these checks within the Federal government will allow the automation of most watchlist comparisons; apply more consistent internal analytical procedures where automated resolution of initial "hits" is not possible. It will allow for more consistent response procedures at airports for those passengers identified as potential matches. Consistent procedures will also help to enhance privacy and civil liberties protections. Significant progress has already been made by the U.S. government by providing greatly expanded No-Fly and Selectee lists to airlines to conduct checks on their own systems.

As proposed in the President's budget, international passenger pre-screening would continue to be conducted by U.S. Customs and Border Protection (CBP) through its Advanced Passenger Information System (APIS) and Passenger Name Record (PNR) authority. The *Secure Flight* program would be coordinated with APIS to the extent that integrated systems would be shared. This would ensure that both domestic and international prescreening is consistent and equally effective.

Secure Flight will support the Department's goals of improving the security and safety of travelers on domestic flights, reducing passenger airport screening time, and protecting privacy and civil liberties. Secure Flight will protect the civil liberties and privacy of passengers and will include mechanisms to assist passengers with resolving instances in which they believe they have been unfairly or incorrectly selected for additional screening.

Crew Vetting

Crew vetting is a TSA program that uses computerized vetting, to assess potential threats presented by terrorists posing as cleared cockpit and cabin crew on inbound and outbound international flights. Crew vetting is the evaluation and analysis of airline crew lists against watch list and lost/stolen passport lists. This analysis allows intelligence analysts to evaluate the collected data to determine whether or not any crewmember is a potential threat to the aviation system.

Aviation crew manifests are received 24 hours in advance of take-off, or two hours in the event of a crew change. This information is provided directly from the airlines. The program is building a continuous "Opt In" database known as the Master Crew List, which will serve as a first database check as each airline submits Flight Crew manifests.

The Crew Vetting Program allows DHS to mitigate risk by vetting airline crewmembers against the same terrorism-related information used for passengers.

The SCO should leverage the strong foundation of screening processes developed within Secure Flight and Crew Vetting, such as establishing watchlist checks on airline passengers and personnel, and apply those sound practices to other screening activities.

The Importance of Privacy Protection

Screening by its very nature requires the gathering and analyzing of large amounts of information, a significant portion of which is personally identifying. It is therefore important that consistent rules be put in place for the respectful handling of this information. The individual programs that will be coordinated through the SCO either have been or will be examined for their impact on privacy to the extent required by law. Completed privacy impact assessments are available for review on the DHS Privacy Office website at www.dhs.gov/privacy. Through improved management of the screening process and alignment of these programs under the SCO umbrella, DHS can deliver enhanced security with improved privacy protections.

In coordination with an appointed Privacy Officer and the DHS Chief Privacy Officer, the SCO would be able to ensure that appropriate and consistent privacy protections are instituted for these consolidated screening activities, that DHS personnel are adequately trained in the need to handle personally identifiable information in a sensitive manner, that compliance with statutory privacy requirements is enforced, and that consistent redress is developed to handle complaints about the use of screening information. The Office of Screening Coordination, in fact, offers DHS the opportunity to further its strategic plan to "defend America while protecting the freedoms that define America."

Conclusion

The Office of Screening Coordination and Operations is an expression of the longer-term vision we have outlined. It is a significant step along the way to achieving, as our vision statement says:

> "a future state in which cross-border travel and in-country immigration activities are simple and convenient for eligible, low-risk persons, and virtually impossible for those who seek to do harm or violate U.S. laws.
>
> ". . .a state in which decision-makers have complete access to the information they need, when and where they need it, to make the best, most informed decision every time.
>
> "[and]. . .an environment where technology is used to address the challenges posed by volume, speed, and distance and where best practices from across the Government and private sector are shared and leveraged."

Thank you for the opportunity to share information on the establishment of the Office of Screening Coordination and Operations.

Mr. LUNGREN. Thank you, Mr. Williams. I might tell you you were within 10 seconds of the 5-minute rule, so I appreciate that very much.

The Chair now recognizes Ms. Carol DiBattiste, the Deputy Administrator, Transportation Security Administration, U.S. Department of Homeland Security, to testify.

STATEMENT CAROL DIBATTISTE, DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. DIBATTISTE. Good afternoon, Chairman Cox, Chairman Lungren, Ranking Member Sanchez and distinguished members of the subcommittee.

Thank you very much for the opportunity to join my colleagues, Director Williams and Deputy Commissioner Spero, in telling you about the proposed creation of the DHS Office of Screening Coordination, better known as the SCO, in fiscal year 2006.

As you will hear from all of us representing DHS this afternoon, the new SCO has been proposed to enhance immigration and border management and transportation security by managing screening and credentialing programs in one central office. It is important that DHS coordinate security activities across the Federal Government to make our mission of securing the American people more effective and more efficient.

Over the next several weeks, the Transportation Security Administration will assist Secretary Chertoff as he conducts a full review of the concept of consolidating the screening and credentialing programs in the SCO to make sure that it is organized the best way to successfully manage these critical programs.

As proposed, the SCO would be comprised of many important programs that TSA conceived and continues to develop. Secure flight, under the Secure Flight Program, the responsibility for checking air passengers against terrorist watch lists will shift to the Federal Government and away from the air carriers. That is a change that will improve consistency and responses in watch list comparisons.

TSA is currently testing its capabilities in this area using passenger data from June of 2004 and the watch list maintained by the Terrorist Screening Center. We soon will undertake limited testing to determine whether comparing passenger information to commercially available data can more accurately verify the identity of individuals. Results from this test as well as tests of comparison to the Terrorist Screening Center database will be made a publicly transparent as possible without compromising national security.

The current year budget for Secure Flight is $34.9 million. The President's request for next year is $81 million. We plan to begin implementing the program with two airlines this August, and we will steadily increase the number of carriers online through fiscal year 2006.

Crew Vetting, another program that will be going into the SCO, Crew Vetting Program checks all cockpit and cabin crew on every inbound and outbound international flight against available terrorism information prior to takeoff. We began this operation during the elevated threat period in December of 2003. Today, we screen more than 30,000 crew members daily. We have identified known or suspect terrorists working for air carriers, and we have taken the necessary steps to prevent them from boarding flights or otherwise entering the United States.

The current-year budget for Crew Vetting is $10 million. The President's request for next year is $13.3 million.

TWIC, the Transportation Worker Identification Credential Program, will improve security by establishing an integrated credential based identify management program for transportation workers who require unescorted access to secure areas of our nation's transportation system. When fully implemented the program will ensure that the identity of each TWIC holder has been verified, that a robust background check has been completed on that identity and that each credential issued is positively linked to the rightful holder through the use of biometric technology.

This program will enable TSA to implement the credentialing provisions of the Maritime Transportation Security Act. We are now working with the U.S. Coast Guard to implement regulations.

The TWIC Program began initial operation on November 17, 2004 and currently the TWIC prototype is in phase III of the pilot at Los Angeles–Long Beach, Wilmington–Philadelphia and at Florida's sea border ports. The prototype is scheduled to end in May and shortly thereafter we will report on its results. During fiscal year 2005, we will continue to test the TWIC prototype with a goal of issuing approximately 100,000 prototype credentials.

The current-year budget for TWIC is $5 million, and beginning next year we expect to fund the TWIC Program through fee collections as we continue to develop the program.

Registered Traveler, TSA's Registered Traveler Pilot Program is testing the use of biometric technology to enhance identity verification at passenger screening checkpoints. It includes a name-based security assessment utilizing intelligence and law enforcement databases and a check of outstanding wants and warrants for each applicant to the program. The goal of the program is to see that if a registered traveler program would speed up screening at airports with shorter lines at security checkpoints and reduce secondary screening, at the same time maintaining a high level of security.

The current budget for Registered Traveler is $15 million. Beginning next year we would expect to fund the program with fee collections.

HAZMAT, hazardous material commercial drivers background checks. The U.S. Patriot Act requires TSA to conduct a security threat assessment on every driver who applies for, renews or transfers a hazardous material endorsement on his or her state-issued commercial driver's license. Under TSA rules, certain individuals will not be allowed to hold a HAZMAT endorsements. TSA has completed name-based security threat assessments on all 2.7 million HAZMAT drivers, generating more than 100 referrals to law enforcement agencies and revocations of HAZMAT endorsements.

Fingerprint-based criminal history record checks began in all 50 states and in the District of Columbia on January 31, 2005 for new applicants, and they will begin by May 31 of 2005 for drivers transferring or renewing their endorsement.

The HAZMAT Program is currently entirely fee-funded. TSA uses discretionary funding this year to cover contingencies associated with standing up the program. Next year, we expect to conduct background checks on 400,000 drivers.

And, finally, the Alien Flight Student Program, also going to be merged into the SCO. In December of 2003, the FAA Reauthorization Act, Vision 100, transferred responsibility for the alien flight student vetting from the FBI to TSA. This program reviews and assesses personal biographic and biometric information in order to help identify individuals who pose a security threat to aviation or national security.

Prior to 9/11 attacks, there were no systematic security checks performed on alien pilots who receive training in the United States. And in fact, seven of the 9/11 hijackers took flight training here in the United States. This program began in late September 2004. We currently conduct a security threat assessment through name-based terrorist and fingerprint-based criminal background checks on all alien flight students, including those trained in aircraft less than 12,500 pounds.

This program is entirely fee-funded. We have utilized some discretionary funding this year to cover contingencies associated with standing up the program, and we expect to conduct background checks on 14,000 flight students this year and 15,000 flight students next year.

Chairman thank you for granting me this opportunity to discuss with you TSA's efforts to secure our nation's transportation system through vetting and credentialing. We are committed to working with our partners at DHS in the coming months to complete the review of the plans to consolidate these critical programs, and I would be happy, of course, to answer any questions you may have on this subject.

[The statement of Ms. DiBattiste follows:]

See page 10.

Mr. LUNGREN. Thank you, Ms. DiBattiste.

The Chair now recognizes Ms. Deborah Spero, the Deputy Commissioner, U.S. Customs and Border Protection, U.S. Department of Homeland Security, to testify.

STATEMENT DEBORAH J. SPERO, DEPUTY COMMISSIONER, BUREAU OF U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. SPERO. Thank you, Chairman Lungren, for holding this hearing, and good afternoon, Chairman Cox, Chairman Lungren and Ranking Member Sanchez and other distinguished subcommittee members. It is a pleasure to appear before you today.

My colleagues have spoken extensively about the merits of the administration's proposal to create an Office of Screening Coordination and Operations, or SCO. I certainly concur with their statement, and I will now add a bit about how Customs and Border Protection, CBP, will support the SCO by describing some of the successful CBP strategies and screening efforts and include some historical perspective of those initiatives. I will close with some observations regarding the value of the SCO.

U.S. Customs and Border Protection includes more than 41,000 employees to manage, control and protect the nation's borders at and between the official ports of entry. As the principal agency responsible for protecting our borders, CBP's mission is vitally important to the protection of America and the American people.

CBP's priority mission embraces two goals: To prevent terrorist and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel. We call these our twin goals.

Working at over 300 ports of entry, CBP faces the challenge of an enormous volume of trade and travel. On an average day, more than 1.1 million passengers, nearly 65,000 trucks and commercial cargo containers and over 365,000 vehicles seek to enter the United States. The use of screening and effective targeting and analysis are critical to our ability to meet this challenge. In fact, every day CBP officers refuse entry to an average of 1,200 non–U.S. citizens who are ineligible for admission to the United States. We also seize over 2,300 pounds of narcotics every day.

Since the late 1980's, CBP, previously Legacy Customs and Legacy Immigration and Naturalization Service, has used data from the Advanced Passenger Information System, APIS, and Passenger Name Records, PNR, or reservation data to support screening of arriving international passengers.

Before 9/11, this data was provided on a voluntary basis, but in 2001 the Aviation and Transportation Security Act mandated the collection of APIS and PNR from carriers. CBP screens this data through the automated targeting system and makes that data available to CBP officers at the National Targeting Center and at analytical units located at the ports of entry. The results of this targeting process are used by CBP officers on the frontline to make decisions regarding potential terrorists and other law enforcement threats.

Similarly, I might add, CBP receives electronic manifests for sea, air and rail cargo which are matched with entry and other data through the automated targeting system, with the results fed back into the automated commercial system to support release or examine decisions by CBP officers at the ports of entry. And the new Automated Commercial System, or ACS, adds an electronic manifests for truck cargo to this process.

The National Targeting Center was created in November 2001 as a centralized organization for research, targeting and analysis, analyzing data from many sources along with current intelligence to serve as a focal point for CBP's field locations and to support CBP officers on the front lines.

As I mentioned earlier, the NTC, working with analytical units located in the ports, provides targeting information to CBP officers. The NTC also responds to requests from frontline officers on a real-time basis to research potential risks presented by passengers and cargo seeking to enter the country. The NTC, which is staffed with experience CBP officers, plays a vital role in ensuring that those officers stationed at the ports of entry and overseas have the best possible targeting and analysis support to effectively address the vast flow of passengers and cargo coming to the United States every day.

US–VISIT adds a valuable tool to the screening strategies deployed to the front line to meet the challenges of processing the millions of arriving international passengers. CBP has worked closely with the US–VISIT Program Office to develop and deploy technology to collect biometrics from arriving international passengers and screen against law enforcement databases. The US–VISIT has been rolled out to 115 airports, 14 seaports and the top 50 land border crossings. This technology has been extremely useful in assisting CBP officers with identifying individuals with outstanding arrest warrants or questionable admissibility issues.

It is important to note that this biometric technology works in conjunction with biographic data obtained through the APIS initiative and further analysis by the NTC and field analytical units.

The massive number of passengers seeking entry into our country requires extensive use of the principles of risk management. In simple terms, risk management is essential in order to distinguish between the vast majority of legitimate travelers from those who would seek to do harm to our country. Registered traveler programs provide CBP with the ability not only to make this important distinction but also to facilitate legitimate travel and direct our own resources to those who present a potential risk. In fact, since the terrorist attacks of September 11, CBP has placed great emphasis on expanding registered traveler programs for passenger vehicles and individuals on our land borders with Canada and Mexico.

I would like to explain how these programs are working today. Three of these programs are Nexus, for northern border vehicle drivers and their passengers, Century, for southern border vehicle drivers and their passengers, and FAST, for commercial truck drivers on both the northern and southern borders. All three of these programs offer expedited and where possible dedicated entry lanes for registered, vetted and low-risk individuals.

CBP has expanded Nexus from a small pilot that was suspended in the aftermath of the terrorist attacks to a robust registered traveler initiative with over 75,000 enrollees at 11 northern border locations. Century has 77,000 enrolled members at 3 southwest border locations, and expansion is being planned to 4 additional locations this year.

A registered and vetted program for commercial truck drivers, FAST, or Free and Secured Trade, was also developed in the last few years. FAST is currently operational at 20 locations at the northern and southern borders, with over 37,000 drivers enrolled. All three of these programs enroll new members every day.

Nexus, Century and FAST all identify low-risk registered travelers through an application, vetting and fingerprint name check process, thereby allowing resources to be focused on more high-risk unknown travelers. To support these programs. CBP has developed enrollment processes for applications vetting, biometric captures and face-to-face interview of participants with CBP officers. CBP also has databases, hardware policy and procedures in place to run day-to-day operations in all registered traveler environments.

Furthermore, Nexus and FAST Programs have been developed as bi-national programs in conjunction with Canada under the auspices of the Shared Border Accord. CBP is also currently piloting an Air Nexus Program with Canada for expedited pre-clearance from the Vancouver International Airport using biometric technology and an automated kiosk.

Most recently, CBP has been fully engaged with the US–VISIT Office and TSA in developing an International Registered Traveler Pilot Program. This program would encompass the best practices of existing CBP and TSA programs and would fully utilize US–VISIT technology to ensure that vetted and low-risk travelers are offered expedited service through CBP and TSA processing. This project is also envisioned to become global in scope, and preliminary discussions have already been held with the Dutch government to develop a bilateral registered traveler initiative.

Clearly, some coordination has taken place among DHS agencies. However, the SCO would provide an even greater opportunity to engage in systematic and comprehensive coordination of screening programs. Although the operational agencies within DHS have been chartered with different missions, rely on different statutory authorities and operate in different environments, there are, nevertheless, numerous opportunities through the SCO to optimize the standardization of systems, equipment and databases in a way that will take these differences into account.

Thank you again for the opportunity to share information on the establishment of the Office of Screening Coordination and Operations. This concludes my testimony and I look forward to responding to any questions you may have.

[The statement of Ms. Spero follows:]

See page 10.

Mr. LUNGREN. Thank you all for your testimony. I am going to ask a few questions at this point in time.

You have a number of different systems here, number of different databases. I recall as Attorney General of California I was the head of the WSIN, the Western States Information Network, which originally started as an information sharing among a number of different law enforcement agencies with respect to fighting drugs. When we expanded it to go into gangs, we realized that there was a different set of criteria. We had to make sure that people who shouldn't have access to gang information didn't get that, even though they had information to the other parts of WSIN. As we developed pointer systems and so forth, we had to make sure that there were safeguards.

The thing that would defeat something like this the fastest is if we didn't make sure that we had appropriate privacy standards and privacy guards here. I presume that with the various different databases you have different standards of privacy depending on the particular program involved.

First of all, is that true, and, second, how do you seek to coordinate these various databases without running into the problem of some people having access for an appropriate manner for a particular database but not for another under privacy concerns?

Mr. WILLIAMS. Chairman, let me first talk about this in terms of the US–VISIT Program. This is a program where privacy is one of our top four goals, and we take it very, very seriously because we want people to feel comfortable when we collect that information that it will be shared only with those people on an appropriate basis.

All of the programs that we are talking about that have databases like the databases that US–VISIT uses, have to comply with having systems of records notices, the Privacy Act of 1974 and the E-Government Act. In fact, with US–VISIT those acts do not apply, strictly speaking, because we are talking about information today on foreign visitors. But in fact, DHS made a policy decision to apply those Acts to the US–VISIT databases. All of the systems today however have to build in security and privacy controls so that we know the general answers to privacy questions, which are "what information are you collecting?" "how long are you keeping it?" "who are you sharing it with and what are they doing with it?" And all of these questions have been answered with regard to all of these systems.

As we look to the future of the SCO, whether databases are combined or whether they are just simply linked, we need to continue to answer all of those privacy and security questions.

Mr. LUNGREN. Before you answer, I would just say I would hope that when you make those decisions—I would expect before you make those decisions you would consult with Congress on those matters.

Ms. SPERO. Yes, we would, indeed. And I would just add to Jim's statement that we also take privacy very seriously. There are probably three ways to look—three elements of making sure that the data is secure. One of them is user IDs and password controls, another one is access controls, and the third is training. I am speaking of our employees. And that we are able to through these three elements ensure that employees understand what the restrictions on the data they are seeing and also that they only see what they are entitled to see based on need. So we can in fact take data and make it only available to certain groups and make a broader data available to larger groups. So it is possible, and we do in fact practice that.

Ms. DIBATTISTE. Chairman, if I may add, on all of the programs that I discussed in my opening testimony, TSA has taken extreme measures to protect the privacy of the data and the individuals that are in the databases. And I would like to talk to you specifically Secure Flight, which I know has a lot of interest from this committee. We have developed a very comprehensive privacy package to support the Secure Flight testing, which is being done as we speak. And we already issued the privacy impact assessment which explains how the PNR data would be used and protected by TSA; A system of records notice that explains our statutory authority to collect the passenger information and conduct the testing; and what is called PRA, Paperwork Reduction Act Notice, was included in the order to obtain the data from the air carriers which they provided to TSA from which we did the testing. And after we did that, we got 500 comments back from the public on those three documents alone.

We incorporated their comments and as much as we could and where appropriate and before we implement Secure Flight. I even have a little more to tell you about Secure Flight; we are going to be redrafting the Privacy Impact Assessment (PIA). It will be reissued to the public again, and the agency will then publish an interim final rule and seek comment from the public on these documents as well. So we are implementing every possible protection.

As Deputy Commissioner Spero mentioned, we treat the data within the Secure Flight Program similar to those of you who have criminal backgrounds as an evidentiary chain of custody. It is treated as if it were evidence in a case. And we have a very controlled chain of custody on any data that we receive. We also train all of our people. Everybody at TSA has been required to go through privacy training, but on the Secure Flight Program they have all specifically received privacy and security training. Any medium that is used to transfer the data is locked in a high security safe when it is not in use. And this is regarding Secure Flight. We have daily inspections to ensure that the data is protected. And anybody that has access to the data facility is through key card and pin access to make sure that our data center is protected.

So I can't say enough about how much we value the privacy protection in all of the programs, and we have done similar things with Registered Traveler, the HAZMAT Program. I could go through it, Alien Flight and TWIC in issuing all the proper notices and protecting the data.

In this SCO consolidation, at this moment in time, we are not intending to commingle the databases. Now, I know Mr. Williams mentioned that at some future time if there is ever any intent to do that, we will be coming back to you.

Mr. LUNGREN. Thank you very much.

I now recognize the Ranking Member for questions.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I have several questions. The first is why wasn't Student and Exchange-Visit or Information System included in the SCO consolidation? I am interested because I still think there is some problems with it, and I also would like to see some improvements made there if it is in consolidation, because at least five of the 9/11 hijackers had student visas.

So I just wanted to know where that was rolling, why you had decided to keep it out. Is it because it has problems that you didn't put it in this office, new office?

Mr. WILLIAMS. SEVIS, the Student Exchange Visitor Information System, was at one time considered to be included in SCO. But the logic behind not including it was looking at those programs where they thought they were in discussions with OMB and DHS where there was more commonality around people screening.

SEVIS is something that is particular to immigration and customs enforcement. In talking about student visas, that is something where those people holding student visas are screened by various methods that Deputy Commissioner Spero mentioned, including the US–VISIT's biometric screening as well as the biographic screening.

And any of the programs that are out there that are not included today, I would say we will be looking across the department to determine at if it is a system or program that contains elements of what we should coordinate-whether it is a biographic, biometric database, an enrollment process, or analysis tools. We would look for commonality to be able to make sure we are coordinating all those things.

But as I said in my oral statement, Secretary Chertoff will be looking at the SCO and will be doing this as part of his major operational and policy review of the departmental initiatives. So I am sure that all of these things will be looked at as part of the Secretary's review.

But the logic behind leaving a program like SEVIS out of SCO was looking at, the critical people screening programs, whether it is clear commonality, and if it is a program that is particular to one operational entity. And, frankly, it was also part of looking at what is the right thing to bite off initially, how much could you take in and try and consolidate and integrate, at the same time looking eventually outside those boundaries to make sure you harmonize and synchronize all the other common elements that are particular to screening programs.

Ms. SANCHEZ. I am also interested in the travel, and it happens either way. It has happened to me several times, either when you are at the airport or where you are crossing across the border. I am just trying to figure out who is setting the standards, what kind of—how are you going to end up on a list? What if you have the same name as somebody else who is on a list? How are we going to work with these people to make sure that they don't continually get stopped?

Mr. WILLIAMS. Let me first answer. I know Deputy Administrator DiBattiste would like to answer too.

One of the things that helps in this regard where somebody has the same name as someone on a watch list is biometrics, because biometrics are unique to the individual. And we believe biometrics help verify identity. And in fact, as our Chief Privacy Officer Nuala O'Connor Kelly often says, biometric programs help protect your privacy from somebody taking your identity.

Ms. SANCHEZ. But how long is it going to take to have that in place? I mean, I have got people right now who?I represent a large Arab and Muslim community, and I have people who four or five hours sit at LAX every time they have to travel.

Ms. SPERO. Ms. Sanchez, first, I will answer your first question, how do people get on the no-fly list, and then I will attempt to answer how we try to help the traveling public when their name is similar to someone that appears on the list—it is not an exact match but it is similar to someone that appears on the list—and what we have instituted at TSA to try to help alleviate their concerns and their problems when they come to the screening checkpoints.

First, how does someone get on the list, the no-fly list, a nomination is made by either the law enforcement community or the intelligence community. It could be the FBI, the State Department, CBP, the CIA. To the FBI for domestic persons and to the NCTC, the National Counterterrorism Center for International Persons. Then the FBI or the NCTC does a review and they then provide a nomination of that based on the information they have gotten from law enforcement to the Terrorist Screening Center.

The Terrorist Screening Center then will review what the nominating agency has given to them, and they do an assessment. We have TSA people detailed there to do that assessment, to make that determination whether they are going to go on the no-fly list, along with law enforcement people. And they make a decision whether to reject the person, nominate the person or accept the nomination, the Terrorist Screening Center does with TSA people detailed there.

After that assessment is done, there is a constant review of that every six months. There is a review of the people on the no-fly list to ensure that they still should remain on the list.

Now, your second question really goes to what happens when someone has a name that is similar to someone that is placed on the list, because it is really not someone that is erroneously placed on the list. The list is finite and we know who is on it and who isn't on it. But it is very rare that individuals are erroneously on the list. For instance, you mentioned the Senator, Senator Kennedy. His name was similar to someone that was on the list, and what we do then is we have a redress program that we are going to even make more robust when Secure Flight is initiated.

But the redirect mechanism that is in place today is if someone has a name that is similar and the carriers implement the list right now. So the air carrier tells them, "You can't fly, your name is similar to someone that is on this list." They can contact on our TSA web site, www.tsa.gov, and go in and contact our contact center, which is a call center. They give them what is called a PIVF, a Personal Identify Verification Form. They fill out that form, notarize that form and then we run them through our intel community and they verify whether they are really on the list or their name is just similar to someone on the list, and then we issue them a cleared letter. And that cleared letter they use from there on our to be able to get on the airplane.

Ms. SANCHEZ. My constituents tell me that even when they carry this letter that they are still being pulled aside and that it takes—that they still get searched, et cetera, even when they are carrying this letter and that it could sometimes be up to an hour for them before they get let through.

Ms. SPERO. We are still working through expediting the process and that leads me to my third point, and that is the new Secure Flight Program that we are working and it is in testing right now. That will help solve a lot of this problem because it will be—the watch list will be in the hands of the Federal Government. Right now the carriers are executing and comparing the names on the list. Once Secure Flight is up and running, we will be comparing them. The name matches, we believe we will have less problems, what you call false-positives, with the name matches, and we will be able to fine tune and people will not be delayed at the security checkpoint.

But we are working through that, Ms. Sanchez, and we are improving it. Some are still delayed. It is based on individual carriers, and that is why we are working with the carriers on helping them move through the cleared letter and process the cleared letter a little bit faster. But with Secure Flight we are going to solve a lot of these problems that you mentioned.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. LUNGREN. I might just tell members of the Committee the information we have received is that we have recessed subject to the call of the Chair on the floor, and at approximately 3:15 we expect our first votes of the day.

One of the lights is burned out. The Committee can't afford to pay for that right now.

So now I recognize the Chairman of the full Committee, Mr. Cox, for his questions.

Mr. COX. Thank you very much, Mr. Chairman.

Ms. DiBattiste, Ms. Spero, in the first case, TSA saw its Secure Flight Program contributed to the new office. On the other hand, the Advanced Passenger Information System was not contributed. If you could describe why in one case and not the other, starting with Ms. Spero.

Ms. SPERO. Yes, sir. I think the best way to look at it might be to think about APIS as a system, and Secure Flight perhaps is more of a program. APIS is in fact integrated with US–VISIT, which is part of the SCO. So APIS plays a major role. The fact that it is connected to CBP in terms of the way it works data-wise doesn't mean that it isn't fully integrated with US–VISIT. So I think it is more of a conceptual difference.

And also we use APIS, as you know, in our National Targeting Center, which has a different function than the Secure Flight Program. So APIS feeds into the National Targeting Center analysis work.

Mr. COX. Ms. DiBattiste, do you want to add to that? Do you want to draw any distinctions between the two programs?

Ms. DIBATTISTE. I think Ms. Spero addressed the major distinctions.

Mr. COX. All right.

Ms. DIBATTISTE. We are domestic and APIS is international. I mean, that is another major distinction. And we do use APIS when we do the crew vetting. Now, that is another program that I briefly mentioned in my opening statement. So the TSA Crew Vetting Program where we are vetting the flight crews and the cabin crews, uses from APIS, because it is all international.

Mr. COX. Well, first, let me reiterate what I said at the outset, that I applaud the movement of the Department toward coordination and integration of these disparate screening systems. I also recognize that your plan of deployment is people first and cargo second. So that explains some of the decisions that have been made at the first pass to put things in and keep other things out.

And I am now trying to understand the more fine distinctions that have been made between passenger screening programs or individual person screening programs so I can take a step back and not be too concerned that I think some of these distinctions are being made rather finely if I can be made to understand that this is a work in progress, that you expect that these programs will in fact all be ultimately coordinated and integrated but that this is a proper first pass. Or, alternatively, are you considering that because something is international and not domestic that it will be forever separate?

Mr. WILLIAMS. Chairman, I would just say you used the correct words, "coordination" and "integration." There will be other examples of systems that may not be under the SCO, such as the State Department's Consolidated Consolar Database (CCD) system, which is used by CBP as part of a US–VISIT system, so that when a traveler comes into the United States and the machine-readable zone of a passport or a visa is swiped, the CCD is accessed as part of that to put up on the screen of the CBP officer that photograph that was taken by the State Department visa issuing officer. And that photo that appears on the screen of the Customs and Border Protection officer then becomes part of the screening process, because they look to see if the photo on the screen—the photo that the State Department took—is the same as the person standing in front of them. That CCD then is part of the screening process. So there will be other systems and processes that have to be coordinated and integrated to make sure we have a harmonized system.

Mr. COX. Ms. DiBattiste?

Ms. DIBATTISTE. Yes. Chairman Cox, if I may add, I think you stated it exactly correct. This is the beginning, and Secretary Chertoff has said in his few short days as being our new Secretary that he wants to do a review, a thorough review of everything that is going into the Screening Coordination Office. Then we are going to go from there and take what he calls a second stage review and look at all of the programs and then move to possibly cargo and conveyances.

So I think this is the beginning of a process, and we are subject to review at the highest levels of the Department with consultation, with members of this committee, and I think you are going to see us doing whatever we can to integrate and consolidate while still protecting people's privacy and safeguarding their civil liberties.

Mr. COX. Thank you very much. My time is expired.

Mr. LUNGREN. Mr. Pascrell?

Mr. PASCRELL. Thank you, Mr. Chairman.

The question I have is two things. Is it true that in every major airport in this country that the workers who go to work every day are screened before they are allowed to go into the airport proper? Deputy Administrator?

Ms. DIBATTISTE. Yes. Yes. All the workers that go into the sterile area are screened, and the workers that have access to the SIDA are not. We have a plan and we are still working on moving forward. That is one of our number one issues for this year. One of our number one goals is thorough SIDA access, access control and working on what we can do to screen all workers.

Mr. PASCRELL. Well, I think that is critical. It has been asked both on the Transportation Committee and in Homeland Security, both Select Committee and now I am asking it. Because that was not the case before, and we brought this up many times. And what you are telling me is that every worker who is not screened we intend to screen before that worker can go to work every day.

Ms. DIBATTISTE. What I am saying is if they are going into the sterile area, they have to be screened, physically screened.

Mr. PASCRELL. So, in other words, they are going to be treated like a passenger.

Ms. DiBattiste. But the SIDA people going into the SIDA area still can get into the SIDA with their badge, and that is our next phase of the process.

Mr. Pascrell. And we intend to inspect those as well, eventually.

Ms. DiBattiste. Yes, sir.

Mr. Pascrell. When this program is up and ready; is that correct?

Ms. DiBattiste. Yes, sir.

Mr. Pascrell. OK. Mr. Williams, what progress has DHS made to date to ensure that passengers on international flights are checked against a watch list?

Mr. Williams. Today when somebody is coming into the United States, through the APIS system the airlines send the arrival manifest 15 minutes after wheels up. That arrival manifest is checked while those people are in the air against the terrorism screening database. And when that person arrives, the passport or visa that is swiped then tells the officer whether that person has been a hit against those biographic watch lists.

In addition, when those people arrive at a Customs and Border Protection port of entry and are included in US–VISIT, they put down their biometrics using the digital finger scans and digital photograph, they are checked against a watch list biometrically. So they are checked two different ways.

Ms. Spero. If I may add to that, in addition to the APIS information that comes in on passengers, we also have passenger name record information, which is the airline reservation system, and that is also taken into account, along with other databases, including the terrorist watch list targeting rules are applied, and that information is provided through the National Targeting Center, through the CBP passenger analytical units so that by the time the flight arrives the frontline officer has the information he needs to know who is a potential risk.

Mr. Pascrell. So this is a far cry for what we are learning after the 9/11 Committee report came out, and the FAA showed a very severe lack of coordination and communication abilities and telling folks who were on those flights. I mean, a lot of it is redacted, of course, I mean, we don't know what the heck happened when you look at the redacted report. Something went on between April and August of 2001, and that is not just a lack of communication. There was a total breakdown of the ability of Federal agencies to protect this country and its residents.

Do you think what you have seen so far, Madam Deputy Commissioner, what you have seen so far have we improved the position, the operations of communications to the extent that we could avoid or should be able to avoid all of them, most of the breakdowns that occurred during that six-month period? That is a tough question, but you are up for it.

Ms. Spero. I am not sure I can answer definitively because there is more to what happened in 9/11 than what the functions of Customs and Border Protection and so forth as far as the intelligence aspects of it. But you do see now all of the government coming together with the establishment as Deputy Administrator DiBattiste mentioned, of how the terrorist screening database is constructed.

Many different agencies play into that determination. The fact that we work with the carriers and that we have a partnership also with US–VISIT so that all international passengers are truly screened, analyzed and targeted before they get to the frontline officer. So I would say that we have made vast improvements.

Mr. PASCRELL. Mr. Chairman, just in conclusion, I am not that concerned about the inconvenience which all of us, many of us seem to be complaining about. If folks are doing their job and if the agencies are doing their job, we are going to have to be inconvenienced. This is called shared responsibility, and we should try to facilitate folks going through airports, but we should not be doing the bidding of the carriers.

And if you look at the history of this problem, many of these problems—I am not just talking about airlines here—but if you look through the history of this, we have done their bidding for many, many years, even long before 9/11. So the inconvenience is one thing, but we want to make sure we protect America. That is most important.

Thank you, Mr. Chair.

Mr. LUNGREN. Thank you, Mr. Pascrell.

And now Mr. Pearce.

Mr. PEARCE. Thank you, Mr. Chairman.

I appreciate your testimony today.

As I listened to Ms. Spero, can you give me a list of all the numbers of people who are affected? You read through a list that 65,000 people are checked in the air, 14,000 foreign pilots. It would be nice to have that measuring stick. Can I get a copy of your testimony? I did not have that in my packet.

Ms. SPERO. Sure.

Mr. PEARCE. OK. I would appreciate that.

I would like to offer a different perspective than my friend who just testified, that one of the concerns that we have to reach in the security business is also making sure that commerce is represented. We can shut down all industry and we can shut down every single trucking, cargo, shipping business that exists, and we can get a very secure nation, we just won't have much of an economy left. What feet at the table, as you have discussions about the procedures, do businesses have?

Ms. SPERO. Well, if I might start, that is a subject near and dear to our hearts. As I mentioned, CBP views its mission as having twin goals, which is in fact preventing terrorists and terrorist weapons from entering the United States while facilitating the flow of legitimate trade and travel. And getting that balance is something that we have been striving for with all of our strategies. We have a number of partnerships that we are extremely proud of. One of them is the Customs Trade Partnership Against Terrorism, CTPAT, which we started immediately after 9/11 when there was legacy Customs working with all members of the trade community to establish greater security in our supply chain.

Mr. PEARCE. If I might interrupt, what seat does business have—do they actually have a representative that sits in on your discussions?

Ms. SPERO. CTPAT members are actively part of forming—consulting with us on all of our policies.

Mr. PEARCE. But they are actual businesses.

Ms. SPERO. Yes. CTPAT members are household names. They are importers, they are carriers.

Mr. PEARCE. OK. Thank you. Yes, that is fine. Just want to check.

Mr. WILLIAMS. Can I add to that? You asked how does business have a seat at the table. I think DHS may be unique by having the position of a Special Assistant to the Secretary for the private sector, Al Martinez-Fonts. In addition, we also meet with stakeholders, U.S. Chamber of Commerce—.

Mr. PEARCE. OK. That is fine. We are kind of running out of time here. The one function that you are bringing in that was handled by that airlines before and you are now bringing it over into your function, is it possible to get a cost that the airlines assessed for that service and compare it to the cost that you all are going to use on the service?

Ms. DIBATTISTE. We will get that for you.

Mr. PEARCE. The administrative section that is going to take—I forget the figures—$6 million for 32 people, can I get a copy of the budget request all the way down? If it is just salaries, that is sort of high. And is it possible also for you all to get us some examples of actually the improved coordination that you are hoping to achieve with this springing together of departments and security functions.

What I am looking for there is some of the stumbling blocks that have been provided in the past that you see are going to be improved by this because it is easy to just say we are going to get improved coordination and sometimes we aren't going to get improved coordination at all.

Why is the free and secure trade the smallest piece of your budget? Out of an $847 million budget, $7 million is dedicated to the free and secure trade and that was maybe at the heart of my question on what are we doing to make sure business still occurs?

Ms. SPERO. The FAST Program is actually up and running. It is an operational program, and it will be expanded. It has been developed in concert with the private sector, notably many of the major auto companies. And the costs are relatively low to that program because it relies on very little in the way of new technology other than transponders.

Mr. PEARCE. Thank you, Mr. Chairman.

Mr. LUNGREN. We have gotten notice that there are two votes on the floor, one a 15, one a 5-minute. And after Mr. DeFazio has his opportunity to ask questions, we will break for approximately 20 minutes.

Mr. DEFAZIO. Thank you, Mr. Chairman. Ms. DiBattiste, I would like to go to secure flight and registered traveler. I note on the registered traveler that you are assuming some fairly substantial revenues in 2006. Does that mean we are past the pilot and into an expansion of the program?

Ms. DIBATTISTE. No, it does not, Mr. DeFazio. We are still in the pilot. We have the five pilots, and they are—.

Mr. DEFAZIO. But may I ask what—?

Ms. DIBATTISTE. Yes, sir.

Mr. DEFAZIO. —sense the current pilot program makes. You have to fly a certain airline out of a certain airport in order to be in the pilot program. It isn't that you fly out of that airport all the time or it isn't that you fly—I stood in a very long line with many other frequent travelers and looked at the unutilized machine there at National with no one using it because we are all in the line for all the other airlines in that terminal, I don't understand.

I mean, since we are moving toward the government controlling things, why doesn't the government issue the frequent traveler IDs to people who apply to the government and pay a fee as opposed to having to use a certain airline out of a certain airport to do a certain thing?

Ms. DIBATTISTE. Well, one of the things we are looking at is testing the biometrics as a pilot and looking at interoperability. That is our issue right now on whether we are going to expand the pilot. Because, you are right, you have to be at a certain airport and only a certain carrier. So we are looking at solving the interoperability issue, and that is one of the purposes of the pilot.

Mr. DEFAZIO. I appreciate that, but I don't understand the interoperability issue. The government sets the standard, you issue a card, you use the standard machines that are linked to a database. But, in any case?

Ms. DIBATTISTE. But you know we have a commercial pilot that is being tested in Orlando, the Public–Private Sector Pilot, that will also give us a lot of interesting area to improve and expand and do some of the things that you are suggesting, because it is a public-private partnership. We would set the standard, we would do the background checks, but the private sector will actually do the enrollment. And that might be the answer to your concerns.

Mr. DEFAZIO. Well, I am sorry to hear the government is that inefficient that you can't do this. I mean, I have got my concealed carry permit with me. I had an FBI background check to get it. Other people in all the states do this. I mean, it is not biometrics yet. I mean, it doesn't seem like rocket science.

Let's go to Secure Flight and CAPPS II. We are still utilizing CAPPS II whose criteria are well known, correct? That is, you buy a one-way ticket, oh, you are going to come up. You are a threat. You buy cash, whoops, you are going to come up. You are in the Frequent Flyer Program. Well, you are not going to come up. We are still using that, right?

Ms. DIBATTISTE. No, we are not still using CAPPS II.

Mr. DEFAZIO. OK. Then how are we charging—.

Ms. DIBATTISTE. That is CAPPS I that you are describing.

Mr. DEFAZIO. Well, CAPPS II isn't much more sophisticated. How are we then selecting people. We are using CAPPS II to select people.

Ms. DIBATTISTE. No. CAPPS II is no longer—.

Mr. DEFAZIO. When you get the black X's on your ticket.

Ms. DIBATTISTE. That is CAPPS I, sir.

Mr. DEFAZIO. Well, and that doesn't happen anymore?

Ms. DIBATTISTE. We still use CAPPS I that generates a random number of selectees, and it does also—.

Mr. DEFAZIO. Do you know what terrorism experts say about random selection and how likely it is that you are going to deter and/or find a threat?

Ms. DIBATTISTE. But that is why we are going to Secure Flight.

Mr. DEFAZIO. Right. Now, that is the problem. I don't think Secure Flight is ever going to work, but maybe it will. But back to the trusted traveler, what percent of the people take what percent of the flights? Are you aware of those statistics? That is a very small number of people take a very large number of the flight. Are you aware of that?

Ms. DIBATTISTE. Yes.

Mr. DEFAZIO. OK. Now, wouldn't it make sense to expedite those people through and then focus on the other three quarters of the passengers who are unknown until such a time as you have Secure Flight, which I am not sure you ever will beyond some sort of test phase. And by getting those people through your system, you then have all the others who are occasional travelers over here.

It would also help the airlines; they are all going broke, because they are losing all their business execs because they are all going to corporate jets who you don't screen, by the way. I mean, in any of these ways, yes, we do some very cursory sort of checks on people getting on a corporate jet but not much, and they don't stand in the line.

So you are hurting the airlines, you are jamming up the airports, you are focusing on the wrong people, and we have been doing this for 3 years now. You would think at this point we could begin to evolve beyond the original primitive CAPPS system and we could also expedite what is a known technology and in our military, in all our nuclear plants and everywhere else with the so-called Secure Traveler card and biometrics. It is off-the-shelf technology.

Ms. DIBATTISTE. Mr. DeFazio, that is exactly where we are headed. The biggest complaint from the air carriers is that they have to compare the watch list every day. We are taking that away from them. It will reduce the number of selectees once we get Secure Flight up and running. It will reduce it in half.

Mr. DEFAZIO. If you do. OK. Then how do we know that the person whose name came up as not a threat name is that person? That is the other problem with Secure Flight. You don't know that is the person. You are not using biometrics. That person is using an ID card, which Mr. Mica famously had his staff download from the Internet and create driver's licenses from a number of states with IDs on them in an hour's time and that will be the basis for how you determine whether that person who you just ran through the system that you took 3 years to construct, maybe it is really not that person.

Ms. DIBATTISTE. Well, that is one of the reasons why we are doing the testing now, the original testing and now the commercial database testing, so we can reduce the number of what is called false-positives. And we believe that—.

Mr. DEFAZIO. No, no. I am getting to the—you know, someone steals your name, your good name, they manufacture a fake ID, they are flying as Carol DiBattiste, and they have a driver's license that shows them to be Carol DiBattiste, and they are not going to pop up under that system.

I mean, the basic flaw in Secure Flight is you don't know whether that name and that person are that person. Whereas under Registered Traveler you are using biometrics. By not focusing on Registered Traveler and getting to a small number of people who take a very large number of flights, diverting them out of system and then focusing the remaining security on those other people, we are creating vulnerability.

Ms. DIBATTISTE. But, sir, that is exactly what we are doing. Secure Flight keeps bad people off airplanes. Registered Traveler let's the good people—.

Mr. DEFAZIO. You just explained my point. It keeps bad names off airplanes. It doesn't keep bad people off airplanes. There is a difference. Someone who manufacturers an ID of a good name isn't going to come up with a bad name. I am a terrorist, I am whatever, X Smith, well-known terrorist. Tell you what, I am not going to use my name when I get on the plane. I am going to use someone else's name and ID, which I have stolen, and I am going to get on the plane and Secure Flight isn't going to find them because that other good citizen whose name they have temporarily stolen is not in your database. So that is the flaw with that system.

Mr. LUNGREN. The gentleman's time has expired, although the gentleman has not expired.

[Laughter.]

We will stand in recess subject to the call of the Chair for now 10 minutes.

[Recess.]

Mr. LUNGREN. [Presiding.] The subcommittee will reconvene and recognize Congressman Dicks.

Mr. DICKS. Thank you, Mr. Chairman. I want to congratulate you on coming back to Congress and also being Chairman. I think it is terrific.

Mr. Williams, going on 3 years now, you and I have been discussing the importance of making sure that US–VISIT is interoperable with other existing databases to ensure that we are getting the system that the Nation needs and that Congress mandated. Indeed, as early as 2003, Congress is on the record stating that it is essential for US–VISIT and the IDENT system DHS uses to be interoperable in real time with IAFIS, the FBI's criminal database.

In August of 2004, metrics study, a report done by the Department of Justice, shows exactly why this interoperability is so important. Almost three-quarters of the criminal aliens encountered at Border patrol stations and ports of entry were identified only by checking the FBI's system and would not have been identified by checking IDENT alone.

As we both know, checking incoming aliens against the FBI's database during the US–VISIT process is not feasible because of the administration's decision to use two flat fingerprints instead of 6, 8 or 10, 10 being preferable, which likely would improve the accuracy rate enough to make this work.

I am sure you have seen the review of the status of that IDENT, IAFIS integration issued by the Justice Department Inspector General in December. Justice argues that this effort has stalled primarily because of the inability of DHS and the State Department to adopt a uniform method of collecting fingerprint information that conforms to the NIST standard put forward in 2003. DOJ concludes that the Federal Government may face significant costs to reengineer its fingerprint identification system in the future to implement a uniform fingerprint technology standard to make all the systems fully interoperable.

Mr. Williams, Congress brought the issue of interoperability up 2 years ago to ensure that we wouldn't have to create this system and spend the money to do so twice. I am deeply concerned that the congressional directive to make U.S.–VISIT fully interoperable with IAFIS is not happening and that the long-term vision to implement US–VISIT you are in the process of developing will require billions of additional dollars to be spent in order to interact with the IAFIS database, as Congress directed you to do years ago.

What is being done in the current increments and in the development of a long-term strategy to make sure we don't have to do this? In other words, why didn't you guys do what Congress directed you to do and that is to use 10 fingerprints and have a system that would be compatible with the FBI's system instead of going with this two fingerprint system? We have had the best experts before this committee, from Stanford and other places. The best you can get with two fingerprints is 53 percent accuracy, and you saw what happened in this metric study.

Why was this done? I brought this up to Asa Hutchinson, brought it up to the Secretary, the Senate raised this issue repeatedly, and yet you guys just stiffed us and said, "No, we know better. We are going to do it our way. We are going to go with a two-finger system," even though every expert that we have had before the Congress has said that the two-finger system is not the way to go. Why was this done? I mean, it bothers me that somehow maybe this is contractor oriented. I mean, why wouldn't we do the right thing when it was so obvious that it was the right thing?

Mr. WILLIAMS. Congressman Dicks, I believe there are several questions in your comments that I would like to respond to. First of all, the fingerprint system that we check against when people come into the country at a customs and border port of entry requires that the check needs to be done within a matter of seconds. Checking against the FBI system cannot be done today. It takes at a minimum—.

Mr. DICKS. That is not what I am told, sir. I am told you can do the 10 fingerprints within a fraction of the second of the time you can do two fingerprints. And it is because the 10-fingerprint system is so much more accurate. That is what we are giving up here. We went with a system that doesn't work, and all the experts told us it doesn't work. And you guys are—it is the same old argument, and it is going to cost us now. We are going to have to go back and fix this system because it doesn't work.

Mr. WILLIAMS. Sir, the system that we use, IDENT, is a subset of the FBI's fingerprint system IAFIS, and that used to be where we got extracts every 2 weeks. In June of 2004, we changed that so that it is daily extract that updates our database. Our database is about 1 million fingerprints plus. To check against the FBI's 47 million, 48 million fingerprints, 80 percent of which are U.S. citizens which I am not even sure that we need to check takes at least 15 minutes, if not hours. The State Department will tell you, as they are pilot testing with using the IAFIS system, it is taking in some cases hours, hours to get a response.

Mr. DICKS. Now, why does NIST say that new scanners can do fast checks with eight or 10 prints?

Mr. WILLIAMS. Well, it is a question of taking the print is one aspect of it. Getting a response back from the system you are checking against is the other half of that equation. Getting a response back from the FBI's system, which was not designed to be a large-scale transactional system, to meet that few seconds response time, it just simply cannot be done today.

Mr. DICKS. But what do you do with the fact that the people, the top experts in the world that have looked at your system, say it is only accurate 53 percent of the time?

Mr. WILLIAMS. That is simply—it is not accurate when you take a poor quality fingerprint, which we take—.

Mr. DICKS. When you only take two, the chances of poor quality fingerprint are very high.

Mr. WILLIAMS. When you take the fingerprint and you get a poor quality fingerprint and it looks like a false-positive, that person is sent to secondary where the fingerprint is retaken and verified. It is verified whether it is a match or not. We have a 96 percent accuracy rate. It is not 53 percent. It is 53 percent only when there is a poor quality fingerprint. And in fact we work closely with—.

Mr. DICKS. And a lot of the people who are trying to disguise their identity have fixed their fingerprint. That is a known fact, and that is why the people, the experts who came in and testified before our committee from Stanford University said there is a much higher chance that your numbers are inaccurate and that the number is around 53 percent.

Mr. WILLIAMS. Again, that 53 percent happens in only a small percentage of the time, and it is when those people put down a poor quality fingerprint. Those people are then sent to secondary where they are subject to a further check. We do have a 96 percent accuracy rate and looking at—.

Mr. DICKS. Well, then how do you explain what the metric study showed? The 2004 metric study showed that when they were using this system they were unable to identify the people who were the criminal aliens, and they had to use the FBI system in order to find out that they were criminals, that your system wouldn't have detected them. How do you explain that?

Mr. WILLIAMS. Well, again, what we get from the FBI, which we update daily, is all of their major wants and warrants and their sexual predators that are foreign born, unknown country of origin. That system that is being used by the Department of State today at all of their 207 visa issuing posts, used by Customs and Border Protection, that is identifying criminals, and in fact we have denied entry to over 450 criminals and immigration violators through the use of that system.

Mr. DICKS. Well, let me just tell you what the study showed, the metric study. Three-quarters of the criminal aliens encountered at border patrol stations and ports of entry were identified only by checking the FBI system and would not have been identified by checking IDENT alone. And I am also told that in US–VISIT it uses only a small segment of the IAFIS system.

Mr. WILLIAMS. That is true. We use that percentage of the system in order to get the response time that the Customs and Border Protection officers need. If somebody's coming into Dulles Airport, they need to be able to get a response time very quickly in order to not have the lines go out on to the tarmac. And if they had to wait 15 minutes—.

Mr. DICKS. Explain to me again why you instead of getting a system that was interoperable with the FBI system that you decided to go and do your own system?

Mr. WILLIAMS. This is the decision made when INS was part of the Department of Justice, as FBI is part of the Department of Justice. Many years ago when they looked to need a system to serve the transactional needs of the border, a decision was made within the Department of Justice to develop the IDENT system. So the system evolved as something that had a different business need, a need to be able to have sub-second response time.

Mr. DICKS. The IG, the Inspector General's report says that DHS has not been willing to have the same metric study done like the Department of Justice; is that correct?

Mr. WILLIAMS. I am not sure what that is referring to, but you referred to the NIST standards. The NIST standards that were set, as I read it, recommended the use of two fingerprints and digital photographs. It also said that you may need to go to more, and that is when you do enrollments. When you are comparing it in a one to many—when you start to get too many fingerprints in your database, you can get into what they said unchartered territory, where you get an unacceptable level of false-positives. That is not happening today.

Mr. DICKS. Let me just make one statement and then I will quit, Mr. Chairman.

The results clearly show that not checking aliens against IAFIS increases the risk that the United States will unknowingly admit criminal aliens. The Department has proposed conducting a similar study on visitors enrolled in US–VISIT but as of October 22, 2004, the Department of Homeland Security has not yet agreed to do so. I would like you to answer for the record why you have not been willing to do so.

Thank you, Mr. Chairman.

Mr. LUNGREN. Ms. Lofgren?

Ms. LOFGREN. Just quickly because Congressman Dicks actually covered the issues that I wanted to raise, but it does segue into another issue, which is the goal of SCO to integrate the various databases and that is really part of this question. And given that the databases in some cases are Legacy systems that are a mess in flow and in some cases need to be replaced, my question goes to the budget.

Is your budget going to allow for the legacy systems to be upgraded so that the kind of query that has just been discussed could be done promptly instead of clumsily as might currently be the case?

Mr. WILLIAMS. I am not sure we know the answer to that yet. The Department, as Deputy Commissioner Spero just recently said, was just created about 2 years ago yesterday, and programs were built upon legacy systems to meet specific business needs. And we have to look at the SCO not only from a database standpoint but meeting a business need standpoint.

I always believe you have to look at integration starting with the mission.

How much we have to then change the underlying infrastructure in order to meet the now harmonized business need, I don't think we know yet.

Ms. LOFGREN. Well, could I ask this, because some of it is your department and some of it isn't, but until we upgrade the legacy systems we are not going to be in a position to do the kind of search that I think we would all want to do.

And one other point I would like to make, and I won't use the full 5 minutes because we are after our time, I know, but I really think the biometrics serves two functions. One is is the person standing before you who he or she says she is, I mean, an identifier? And then, two, the ability to search what we know about various people with that same biometric to see is this the person who pops up.

And there is nothing that prevents us—I mean, this is something I have been talking about for the last 3 years—there is nothing that prevents us from having more than one biometric to do that. And I, for the life of me, don't understand why we don't have a biometric with a very small data load in a very high reliability component for the ID function. And in addition to, not instead of, a biometric that also can serve as a template for searching other databases.

When INS went to this two-finger system, I don't know if you recall, I complained about it because it was not compatible with the FBI database, which was also a mess anyhow. And so what I would like to get from you in writing is the budget question: What would it take for your agency to upgrade the legacy systems that you are dealing with now so that databases could be searchable with the proper privacy protections built in in a timeframe that is suitable for business purposes?

Number two, what biometric indicator could be used as an addition, not instead of, that would have a small data load and a high reliability? I have been told that might be an iris scan, but I am not pushing that technology. Whatever it is that would do the ID function as compared to the search function that could get things moving rather quickly.

And, finally, if you don't know the answer I wouldn't expect you to, if you could at least estimate the FBI's function—I am going to ask the same thing over in the Judiciary Committee—on what kind of budget would be required for the Department. They just had their whole system crash and burn. What kind of budget are we looking at for them to upgrade their Legacy systems.

And then the third question is if you could identify those databases that either you maintain or you interface with that are currently incompatible so that we have an idea of the scope of what we are talking about, that would be very, very helpful to me and I am sure the entire committee. Can you do that?

Mr. WILLIAMS. We would be glad to do that.

Ms. LOFGREN. Thank you very much.

Thank you, Mr. Chairman.

Mr. LUNGREN. I know we are over time but I would just like to ask two questions: one in the area of effectiveness and one in the area of efficiency.

You have given us a lot of data about what you are doing, how you are doing it and so forth. Can you very succinctly tell me what the specific goals are to be achieved by the consolidation of these screening initiatives? How is it that it will make us safer, simply put?

Mr. WILLIAMS. I think it will lead to, as the President of the 9/11 Commission and I believe the Select Committee pointed out, the need for consistency in screening which leads to enhanced security. It also leads to increased efficiency that leads to getting more mission for the same amount of dollars, as well as making information sharing a lot easier where you can align the systems and processes.

Mr. LUNGREN. In terms of efficiency, I look at the budget request, I see the amount of money you have got in there, and I know the largest amount is self-generated, that is it is fee-based. But I fail to see any savings in here. The request envisions the need for 32 additional FTEs to manage the office. The first question people would ask is "if it is more efficient, why do you need 32 more people and another level of bureaucracy?"

Mr. WILLIAMS. I would be glad to answer that question. The 32 additional people are to help achieve the benefits of integration. The programs coming together have their own staffs that have to operate their programs. To achieve integration, you cannot do it without somebody who looks at this from a corporate level and starts to knit together these programs in terms of how the business processes, the data, the systems, the system interfaces, the data sources, how do those get harmonized?

That doesn't just happen by putting all of these programs together. You need some overhead of people who would help achieve that integration vision and help manage that integration vision. That comes from having an operational business vision and an information technology business vision. All of those things have to happen.

The 32 people where there is $6 million set aside in the budget I believe that is a small price to pay for the integration benefits that come through putting together these different programs under the SCO.

And in terms of the savings, as I mentioned before, what I think you really get is cost avoidance. If you don't do the SCO and you don't coordinate and integrate, then you have systems and programs that are building separate infrastructures potentially, buying the same tools instead of sharing the same tools. And that way you have duplicative costs that can be avoided by achieving the benefits of integration. If you then have the same budget, then you get more mission for the same amount of money by building upon that common set of services or that common infrastructure.

Mr. LUNGREN. I appreciate that, but that presumes that everybody in the separate systems is absolutely necessary and no efficiencies can be wrung out of the systems that exist now. We are throwing a lot of money at your department, and we keep being asked by people back home whether it is all being spent as efficiently as possible, and I would at least have liked to have seen some identified potential savings, and I don't see that here. But I appreciate what you had to say.

I want to thank all three of you for appearing. I appreciate the time. I appreciate your indulgence as we went over to vote and had to come back. And I would like to thank the other members of the Committee for being here, but they are all gone except one, and I thank Ms. Lofgren for being here.

For those of you who don't know, on the board we are listed as voters as Zoe Lofgren and Daniel E. Lungren to make sure that no one mistakes the two of us.

Ms. LOFGREN. Two fine Swedish Americans from the same state.

Mr. LUNGREN. That is right. That is right. Although as my mother and father would say, I am Swedish Irish but I take the Swedish side as well.

Ms. LOFGREN. And so am I.

Mr. LUNGREN. I thank the witnesses for your valuable testimony and the members for their questions.

The members of the committee may have some additional questions for the witnesses, and we will ask you to respond to them in writing and the hearing record will be held open for 10 days.

This committee stands adjourned.

[Whereupon, at 4:17 p.m., the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Record

Prepared Statement for the Record from Marc Rotenberg, EPIC Executive Director and Melissa Ngo EPIC Staff Councel

March 1, 2005

Chairman Dan Lungren
Ranking Member Loretta Sanchez
House Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity
Washington, DC 20515

Dear *Chairman* Lungren and *Congresswoman* Sanchez,

We are writing on behalf of the Electronic Privacy Information Center ("EPIC") to bring to your attention the significant increase in surveillance funding in the proposed Transportation Security Administration ("TSA") budget for Fiscal Year 2006. This includes increases in funding for programs that would move from TSA to the Department of Homeland Security's proposed Office of Screening Coordination and Operations ("SCO") if it were created. We ask that this statement be included in the March 2,2005, hearing record of the House Subcommittee.

EPIC strongly opposes this increase in federal funding for TSA's surveillance programs and urges the federal government to openly and transparently explain how it intends to safeguard American citizens' privacy rights under the SCO. In its development and implementation of these surveillance programs, TSA has failed to meet its legal obligations for openness and transparency under the Freedom of Information Act, and the agency has violated the spirit if not the letter of the Privacy Act. TSA also has shown a proclivity to using personal information for reasons other than the ones for which the information was gathered or volunteered. TSA also has shown poor management of its financial resources.

We urge you to ask the witnesses at the March 2 hearing what steps the agency will take to protect privacy and ensure transparency in data collection and use. The Subcommittee should particularly scrutinize how the agency will safeguard citizens' civil liberties and guarantee accountability of the actions of the proposed Office of Screening Coordination and Operations.

President Bush's proposed budget would increase TSA spending by $156 million to $5.6 billion for fiscal year 2006, but this increase is contingent upon $1.5 billion that will be generated by a 120 percent jump in security fees assessed to airline passengers.[1] Assistant Secretary David M. Stone defended the increase at the Feb. 15, 2005, hearing before the Senate Committee on Commerce, Science and Transportation saying air passengers, not the general public, should pay for air travel security. However, this money will not go toward new security measures, but will replace funds now provided by the government for current air traveler security programs.

Assistant Secretary Stone also testified that this increased fee would mean "resources from the general taxpayer could be used for more broadly applicable homeland security needs," but he did not define what these needs would be.[2] Other programs under TSA that are receiving an increase in funding in the proposed fiscal year 2006 budget include surveillance programs that have significant privacy implications for tens of millions of American citizens and lawful foreign visitors.

When it enacted the Privacy Act, S V.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and re-

[1] Transportation Security Administration Statement of Assistant Secretary David M. Stone Before the Committee on Commerce, Science & Transportation (Feb. 15, 2005) (hereinafter "Stone Statement")

[2] *Id*

quired agencies to be transparent in their information practices.[3] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[4]

The Supreme Court as recently as last year underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that: .

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, § 2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[5]

It is critical for TSA's programs to adhere to these requirements, as they have a profound effect on the privacy rights of a large number of American citizens and lawful foreign visitors every year. However, TSA has failed to follow the spirit of the Privacy Act during development of these surveillance programs.

Office of Screening Coordination and Operations Raises New Privacy Problems

The Department of Homeland Security ("DHS") has proposed the creation and funding of the Office of Screening Coordination and Operations, which would oversee vast databases of digital fingerprints and photographs, eye scans and personal information from millions of Americans and foreigners. This office would be responsible for United States-Visitor and Immigrant Status Indicator Technology (US–VISIT), Free and Secure Trade, NEXUS/Secure Electronic Network for Travelers Rapid Inspection, Transportation Worker Identity Credential ("TWIC"), Registered Traveler, Hazardous Materials Trucker Background Checks, and Alien Flight School Checks. This mass compilation of personal information has inherent dangers to citizens' privacy rights and it is imperative that SCO fulfill its legal obligations for openness and transparency under the FOIA and Privacy Act.

According to the president's proposed fiscal year 2006 budget, the mission of the proposed SCO is "to enhance the interdiction of terrorists and the instruments of terrorism by streamlining terrorist-related screening by comprehensive coordination of procedures that detect, identify, track, and interdict people, cargo and conveyances, and other entities and objects that pose a threat to homeland security."[6] The budget goes on to say that "the SCO would produce processes that will be effected in a manner that safeguards legal rights, including fteedoms, civil liberties, and information privacy guaranteed by Federallaw."[7] It is unclear, however, what steps the office intends to take to protect these rights.

There is a significant risk that the creation and funding of the SCO would allow for mission creep—a risk that the data collected and volunteered by airline passengers, transportation workers and foreign visitors will be used for reasons not related to their original aviation security purposes. Though TSA has stated that it will not use the sensitive personal data of tens of millions of Americans for non-aviation security purposes, TSA documents about the CAPPS II program collected by EPIC under the FOIA clearly showed that TSA had considered using personal information gathered for the CAPPS II program for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local, international or foreign agencies for their investigations of statute, rule, regulation or order violations.[8] TSA exhibited a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered.

TSA Has Failed to ComplY With Open Government Laws

The Freedom of Information Act ("FOIA"). 5 D.S.C. § 552. establishes a legal right for individuals to obtain records in the possession of government agencies. The FOIA helps ensure that the public is fully informed about matters of public concern. Government agencies are obligated to meet the requirements of open government

[3] S. Rep. No. 93–1183, at 1 (1974).

[4] *Id.*

[5] Doe v. Chao, 540 U.S. 614 (2004).

[6] Homeland Security, *Budget-in-Brief Fiscal Year 2006,* (Feb. 7,2005) at 19 *available at* http://www.dhs.gov/dhspublic/interweb/assetlibrary'Budget—BI–BFY2006. pdf.

[7] *Id.*

[8] Department of Homeland Security TSA, *Draft Privacy Impact Statements (CAPPS II),T1 April 17, 2003, July 29, 2003, and July 30,2003, obtained by EPIC through FOIA litigation, available at* http://www.epic.org/privacy/airtravel/profiling.html.

and transparency under the FOIA, but TSA has failed to meet its FOINs obligations during the creation of these surveillance programs.

TSA is requesting an increase of $49.3 million for its Secure Flight program to bring its fiscal year 2006 budget to $94 million. The Secure Flight passenger prescreening program could affect the tens of millions of citizens who fly every year, but in the creation of the program. TSA has failed to meet its obligations under FOIA. and its actions concerning openness and transparency have violated the spirit of the Privacy Act.

In September 2004, TSA announced plans to test Secure Flight. Secure Flight is intended to replace the now-defunct CAPPS II. but it includes many elements of the CAPPS II program, which was abandoned largely due to privacy concerns.[9] TSA said that "Secure Flight will involve the comparison of information for domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), to include the expanded TSA No-Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity."[10]

On Sept. 28. 2004, EPIC submitted a FOIA request to TSA asking for information about Secure Flight.[11] EPIC asked that the request be processed expeditiously, noting the intense media interest surrounding the program. Specifically. EPIC demonstrated that 485 articles had been published about the program since TSA announced its plans for Secure Flight. EPIC also mentioned the Oct. 25. 2004, deadline for public comments on the test phase of the system, explaining the urgency for the public to be as well informed as possible about Secure Flight in order to meaningfully respond to the agency's proposal for the program. TSA determined these circumstances did not justify the information's immediate release, and refused EPIC's request that the information be made public prior to the Oct. 25 deadline for these comments. TSA also denied EPIC a fee waiver. which the agency has never done before in its three-year existence. This maneuver imposed a significant procedural barrier to EPIC's ability to obtain the information. EPIC appealed TSA's decision noting that TSA' s actions were unlawful. Rather than defend its position in court, TSA has released a minimal amount of the information that EPIC requested. EPIC continues to seek from TSA information about the program that will affect tens of millions of airline passengers each year.

The recently enacted Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA to create a system for travelers to correct inaccurate information that has caused their names to be added to the no-fly list.[12] TSA maintains that it has an adequate redress process to clear individuals improperly flagged by watch lists; however, it is well known that individuals encounter great difficulty in resolving such problems. Senators Ted Kennedy (D–MA) and Don Young (R–AK) are among the individuals who have been improperly flagged by watch lists.[13] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge; unfortunately, most people do not have that option.

Also, in June 2004 then-TSA Acting Administrator Admiral David Stone admitted to the Senate Governmental Affairs Committee that in 2002 TSA facilitated the transfer of passenger data from American Airlines, Continental Airlines, Delta Airlines, America West Airlines, Frontier Airlines, and JetBlue Airways to TSA "cooperative agreement recipients" for purposes of CAPPS II testing, as well as to the Secret Service and IBM for other purposes.[14] Stone also stated that Galileo International and "possibly" Apollo, two central airline reservation companies, had provided passenger data to recipients working on behillf of TSA.[15] Further, TSA directly obtained passenger data from JetBlue and Sabre, another central airline res-

[9] *See* Sara Kehaulani Goo and Robert O'Harrow Jr., *New Screening System Postponed,* Washington Post. July 16,2004, at A02.

[10] System of Records Notice, Secure Flight Test Records, 69 Fed. Reg. 57345 (Sept.24, 2004).

[11] Letter from Marcia Hofmann. Staff Counsel, EPIC. to Patricia Reip-Dice, Associate Director. FOIA Headquarters Office. TSA. Sept. 28.2004 (on file with EPIC).

[12] P.L. No. 108–458 (2004).

[13] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem,* Washington Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List,* Associated Press, Sept. 29, 2004; Richard Simon, *Iconic Senator Is Suspicious to Zealous Airport Screeners,* Los Angeles Times, Aug. 20, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems,* United Press International, Aug. 20, 2004.

[14] *See* U.S. Senate Committee on Governmental Affairs Pre-hearing Questionnaire for the Nomination of Admiral David Stone to be Assistant Secretary of Homeland Security, Transportation Security Administration 17, 19, *available at* http://www.epic.org/privacy/airtravellstone—answers. pdf.

[15] *Id.*

ervation company, for CAPPS II development.[16] TSA did not observe Privacy Act requirements with regard to any of these collections of personal information.[17] Stone's admission followed repeated denials to the public, Congress, Government Accountability Office ("GAO"), and Department of Homeland Security Privacy Office that TSA had acquired or used real passenger data to test CAPPS II.[18] TSA exhibited a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered.

Another example of TSA's failure to operate its programs with the openness and transparency necessary under the federal open government laws is its recent creation of an Aviation Security Advisory Committee Secure Flight Privacy/IT Working Group. It appears to EPIC that, based upon the little public information that is currently available, the working group is subject to the Federal Advisory Committee Act ("FACA"), 5 US.C. App. 1, which includes the requirement that the working group publish notices of their meetings in the Federal Register. However, the formation of this working group was not announced in the Federal Register, and neither TSA nor DHS has publicly acknowledged its existence or defined its mission. EPIC recently sent a letter to TSA's privacy officer, Lisa Dean, to ask for an explanation as to why this working group is not operating with the transparency and openness required under FACA.[19] More than four weeks have passed since we sought clarification ofTSA's position concerning the status of the working group, but to date we have received no response.

TSA Has Failed to Comply With Privacy Laws

The proposed fiscal year 2006 budget accords TSA's Registered Traveler program $22 million. This is a pilot program TSA began conducting in July 2004 and is now operating at five airports.[20] The preliminary results are now being examined by TSA to determine whether the program should be expanded to other airports. Registered Traveler allows frequent travelers to submit digital fingerprints, iris scans and undergo a background check in exchange for receiving a fast pass through the airport checkpoint. (TSA recently announced the International Registered Traveler program.)

TSA first published a Federal Register notice about the program in June 2004.[21] In July 2004, EPIC submitted comments to address the substantial privacy issues raised by the Registered Traveler program and the new system of records established to facilitate the program.[22] EPIC requested that TSA substantially revise its Privacy Act notice prior to implementation of the fmal phase of Registered Traveler. TSA's subsequent Federal Register notice of the implementations of Privacy Act exemptions in the Registered Traveler program did not solve any the privacy right threats that EPIC highlighted in its comments.

TSA's notice for the Registered Traveler system of records, exempted the system from many protections the Privacy Act is intended to provide—in fact Registered Traveler was exempted from all specific exemptions under the Privacy ACt.[23] TSA's notice leaves it under no legal obligation to inform the public of the categories of

[16] *Id.* at 19.

[17] *Id.* at 18.

[18] *See, e.g.,* Ryan Singel, *More False Information From TSA,* Wired News, June 23, 2004 ("After the JetBlue transfer was brought to public attention in September 2003, TSA spokesman Brian Turmail told Wired News that the TSA had never used passenger records for testing CAPPS II, nor had it provided records to its contractors. In September 2003, Wired News asked TSA spokesman Nico Melendez whether the TSA's four contractors had used real passenger records to test and develop their systems. Melendez denied it, saying, 'We have only used dummy data to this point.' "); *U.S. Representative John Mica (R–FL) Holds Hearing on Airline Passenger Profiling Proposal: Hearing Before the Aviation Subcomm. of the House Transportation and Infrastructure Comm.,* 105th Congo (March 2004) (Admiral Stone testifying that CAPPS II testing was likely to begin in June 2004); GAO Report at 17 ("TSA has only used 32 simulated passenger records—created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data to conduct [CAPPS II] testing"); Department of Homeland Security Privacy Office, *Report to the Public on Events Surrounding jetBlue Data Transfer* (Feb. 2004) 8 ("At this time, there is no evidence that CAPPS II testing has taken place using passenger data").

[19] Letter from David Sobel, General Counsel, EPIC, and Marcia Hofmann, Staff Counsel and Director, Open Government Project, EPIC, to Lisa Dean, Privacy Officer, Office of Transportation Security Policy, TSA, Jan. 31,2005 (on file with EPIC).

[20] Press Release, U.S. Department of Homeland Security TSA, Secretary Ridge Unveils Registered Traveler Pilot Program At Reagan National Airport (Sept. 3, 2004).

[21] Privacy Act Notice, 69 Fed. Reg. 30948 (June 1,2004).

[22] Comments of the Electronic Privacy Information Center on Registered Traveler Operations Files Privacy Act Notice, June 1,2004, *available at* http://www .epic.org/privacy /airtravel/rt—comments. pdf.

[23] Privacy Act Notice, 69 Fed. Reg. 54256 (Sept. 8, 2004).

information contained in the system or provide the ability to access and correct records that are irrelevant, untimely or incomplete. The program contains information that is unnecessary and wholly irrelevant to the determination of whether an individual poses a threat to aviation security. TSA asks for the public's voluntary disclosure of personal information, yet operates the Registered Traveler program with very of the little transparency and openness obligations that the Privacy Act demands.

TSA is requesting $244 million for its pilot program TWIC for fiscal year 2006. TWIC is an identification card given to transportation workers, authorized visitors and all other persons requiring unescorted access to transportation infrastructure secure areas. Currently, the program is operating at 34 sites in six states, but TSA hopes to eventually extend the program to workers in all modes of transportation, which could encompass as many as 6 million people,[24] Persons required to have the identification card submit sensitive personal and biometric information to a central TSA database used to validate a person's eligibility to access these areas. EPIC submitted comments in November 2004 highlighting the dangers to participants' privacy rights inherent in the program.[25] TSA has not released information clearly explaining to the public how it intends safeguard the sensitive personal information gathered on program participants. The lack of transparency and openness about TWIC is against the spirit of federal open government laws.

TSA Has Mismanaged Its Programs

Another important reason not to increase the funding for TWIC is because TSA has not used its current funding judiciously. The GAO reviewed TWIC in December 2004, and found that because of program delays, some port facilities are forced to proceed "with plans for local or regional identification cards that may require additional investment in order to make them compatible with the TWIC system. Accordingly, delays in the program may affect enhancements to port security and complicate stakeholder's efforts in making wise investment decisions regarding security infrastructure."[26]

The financial problems encountered in TSA's TWIC program are emblematic ofTSA's troubles managing its finances, according to the GAO. Cathleen Berrick, GAO Director of Homeland Security and Justice, told the Senate Committee on Commerce, Science & Transportation on Feb. 15, 2005, that TSA had not always "conducted the systematic analysis needed to inform its decision-making processes and to prioritize its security improvements."[27] Examples include the fact that in fiscal year 2005, TSA was forced to transfer about $61 million from its Research and Development budget of $11 0 million, to support its operations, such as personnel costs for screeners.[28]

A significant issue is that these surveillance programs are receiving substantial funding and TSA manpower while the current aviation program to screen passengers and their luggage for threatening objects is woefully inadequate. Ms. Berrick reported at the Feb. 15, 2005, hearing that there has been only modest progress in how well screeners detect threat objects following a report last year that documented gaps in screener security.[29] The increased funds that TSA has earmarked for surveillance programs can also be used in another important program: Threat Assessment of General Aviation. The GAO reported that "though the Federal Bureau of Investigation has said that terrorists have considered using general aviation to conduct attacks, a systematic assessment of threats has not been conducted."[30] TSA has cited cost as the reason that TSA has conducted vulnerability assessments at only a small number of the 19,000 general aviation airports nationwide.

TSA has failed to meet its legal obligations for openness and transparency under the Freedom ofInformation Act and has violated the spirit of the Privacy Act for the protection of privacy rights in the development of the above programs, some of which DHS proposes to move into the SCO if it is created. TSA also has shown a

[24] TSA's fact sheet on the Registered Traveler program, available at www.tsa.gov/interweb/assetlibrary/RT—Factsheet.pdf.

[25] Comments of the Electronic Privacy Information Center on Transportation Security Threat Assessment System and Transportation Worker Identification Credentialing System Privacy Act Notice, Sept. 24, 2004, available at http://www.epic.org/privacy/airtravel/twic—comments.pdf.

[26] Government Accountability Office, *Transportation Security: Systematic Planning Needed to Optimize Resources, Statement of Cathleen A. Berrick, Director Homeland Security and Justice,* GAO–05–357T (Feb. 15,2005) ("GAO Report").

[27] *Id.* at 2.

[28] *Id.* at 31.

[29] *Id.* at 11.

[30] *Id.* at 17.

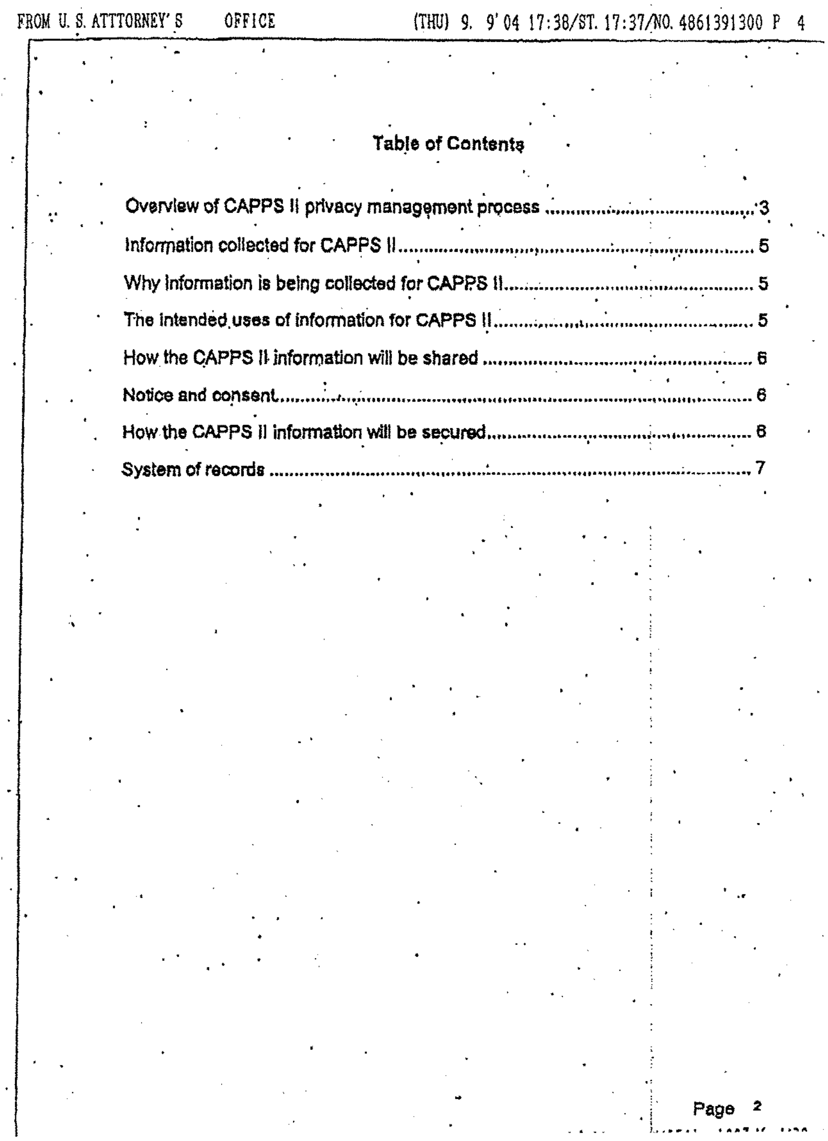
proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered. TSA also has shown poor management of its financial resources. For these reasons, EPIC strongly opposes the sharp increase in funding for TSA's surveillance programs proposed in the president's fiscal year 2006 budget, and urges DHS to openly and transparently explain how it intends to safeguard American citizens' privacy rights and ensure accountability in the proposed Office of Screening Coordination and Operations.

Thank you for your consideration of these issues.

Sincerely,

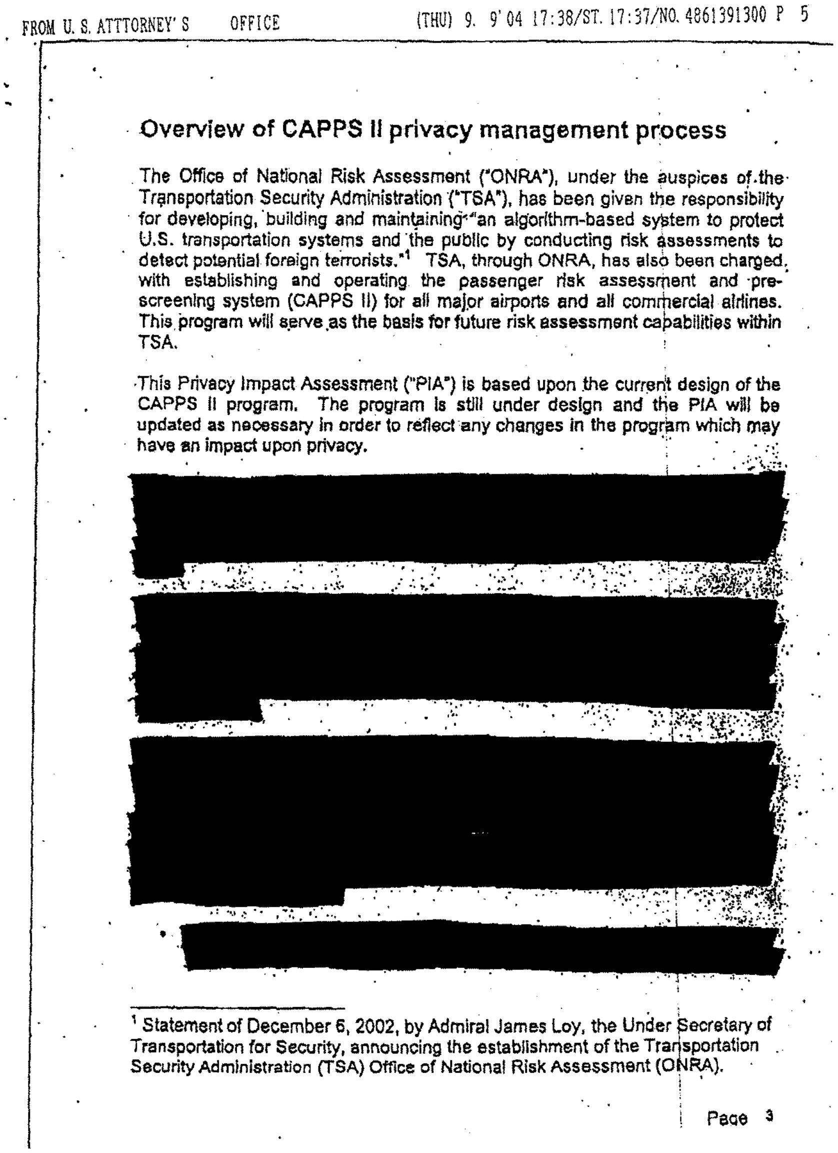
MARC ROTENBERG
EPIC Executive Director

MELISSA NGO
EPIC Staff Counsel



FROM U. S. ATTTORNEY' S OFFICE (THU) 9. 9' 04 17:38/ST. 17:37/NO. 4861391300 P 4

Table of Contents



FROM U. S. ATTTORNEY' S OFFICE (THU) 9. 9'04 17:38/ST. 17:37/NO. 4861391300 P 5

Overview of CAPPS II privacy management process

The Office of National Risk Assessment ("ONRA"), under the auspices of the Transportation Security Administration ("TSA"), has been given the responsibility for developing, building and maintaining "an algorithm-based system to protect U.S. transportation systems and the public by conducting risk assessments to detect potential foreign terrorists."[1] TSA, through ONRA, has also been charged with establishing and operating the passenger risk assessment and pre-screening system (CAPPS II) for all major airports and all commercial airlines. This program will serve as the basis for future risk assessment capabilities within TSA.

This Privacy Impact Assessment ("PIA") is based upon the current design of the CAPPS II program. The program is still under design and the PIA will be updated as necessary in order to reflect any changes in the program which may have an impact upon privacy.

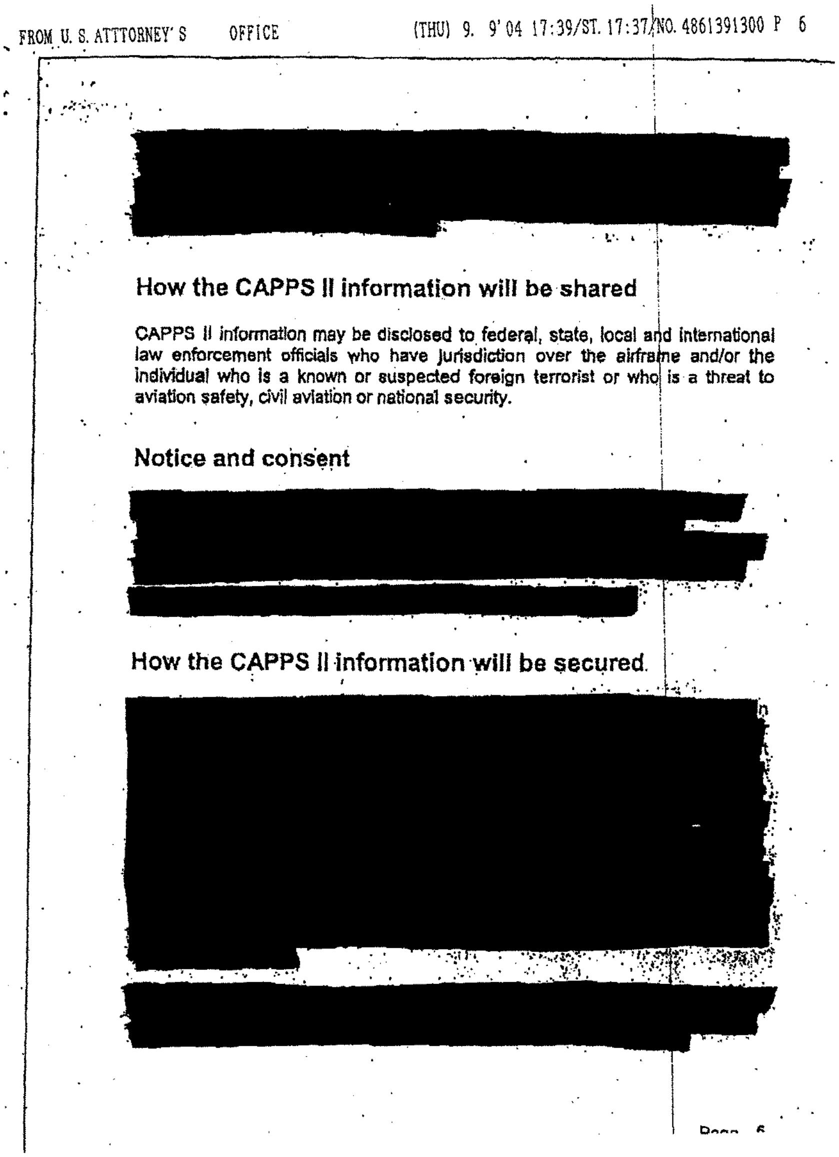
[redacted]

[redacted]

[redacted]

[redacted]

[1] Statement of December 6, 2002, by Admiral James Loy, the Under Secretary of Transportation for Security, announcing the establishment of the Transportation Security Administration (TSA) Office of National Risk Assessment (ONRA).



[redacted]

How the CAPPS II information will be shared

CAPPS II information may be disclosed to federal, state, local and international law enforcement officials who have jurisdiction over the airframe and/or the individual who is a known or suspected foreign terrorist or who is a threat to aviation safety, civil aviation or national security.

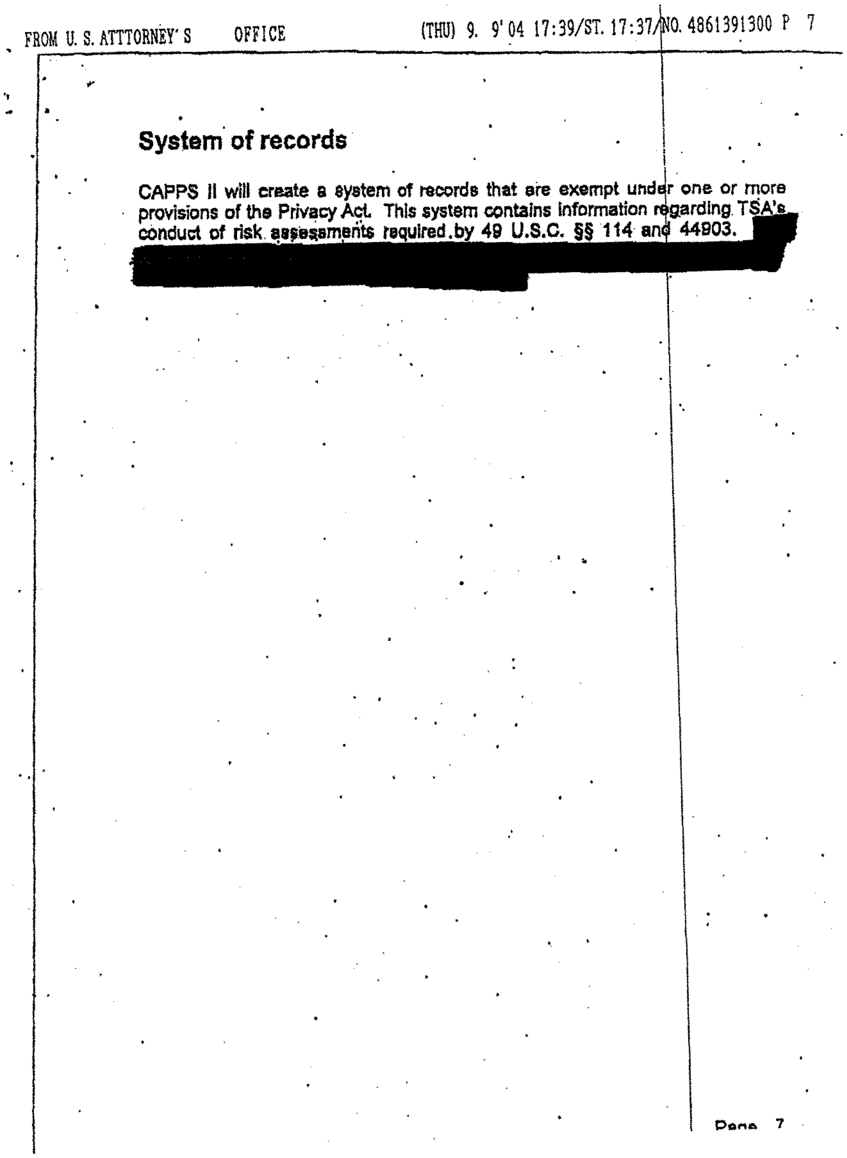
Notice and consent

[redacted]

How the CAPPS II information will be secured.

[redacted]

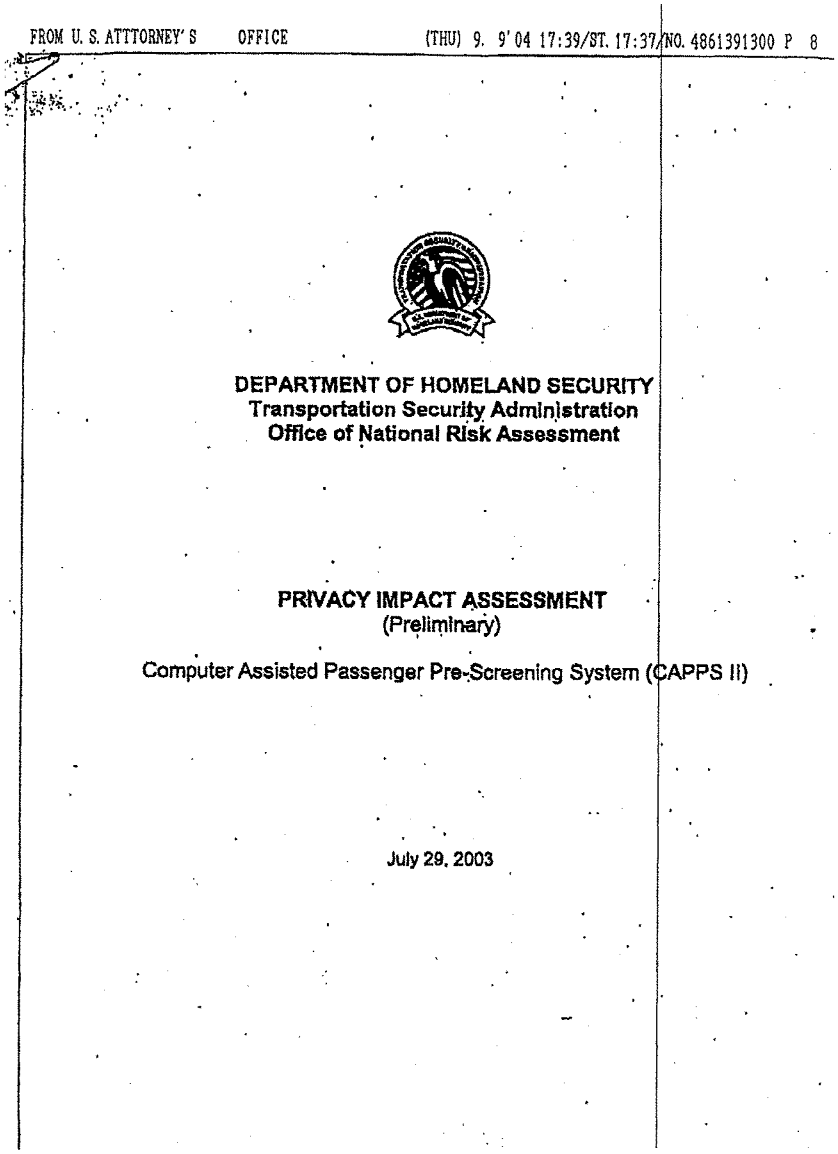
[redacted]



FROM U. S. ATTTORNEY'S OFFICE (THU) 9. 9'04 17:39/ST. 17:37/NO. 4861391300 P 7

System of records

CAPPS II will create a system of records that are exempt under one or more provisions of the Privacy Act. This system contains information regarding TSA's conduct of risk assessments required by 49 U.S.C. §§ 114 and 44903. [redacted]



FROM U. S. ATTTORNEY'S OFFICE (THU) 9. 9'04 17:39/ST. 17:37/NO. 4861391300 P 8

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration
Office of National Risk Assessment

PRIVACY IMPACT ASSESSMENT
(Preliminary)

Computer Assisted Passenger Pre-Screening System (CAPPS II)

July 29, 2003

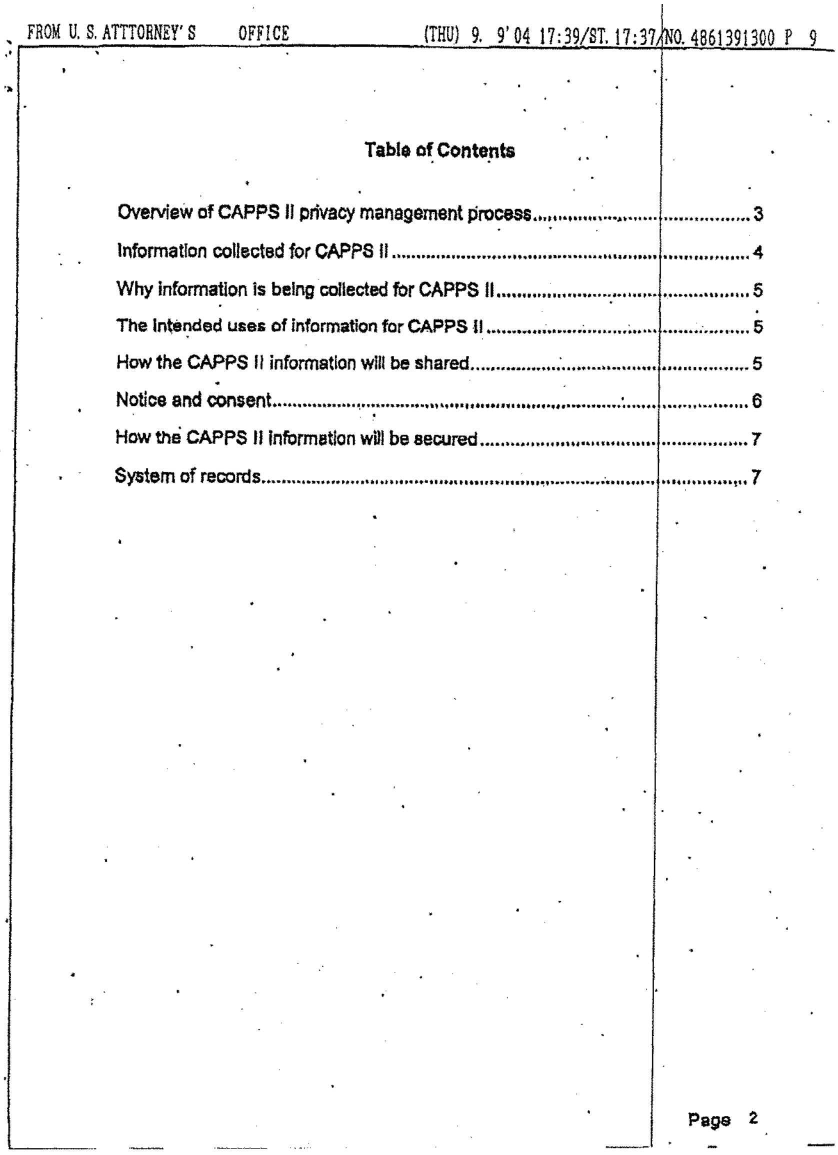
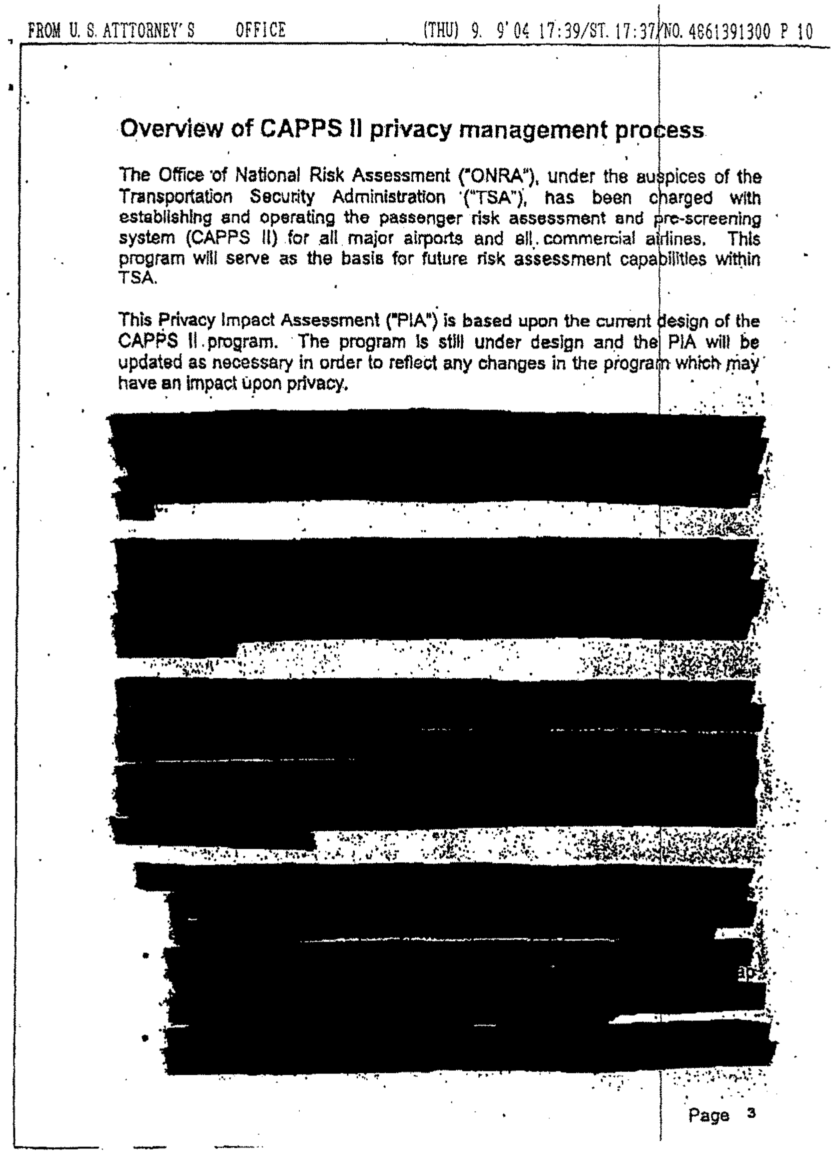


Table of Contents



FROM U. S. ATTTORNEY'S OFFICE (THU) 9. 9'04 17:39/ST. 17:37/NO. 4861391300 P 10

Overview of CAPPS II privacy management process

The Office of National Risk Assessment ("ONRA"), under the auspices of the Transportation Security Administration ("TSA"), has been charged with establishing and operating the passenger risk assessment and pre-screening system (CAPPS II) for all major airports and all commercial airlines. This program will serve as the basis for future risk assessment capabilities within TSA.

This Privacy Impact Assessment ("PIA") is based upon the current design of the CAPPS II program. The program is still under design and the PIA will be updated as necessary in order to reflect any changes in the program which may have an impact upon privacy.

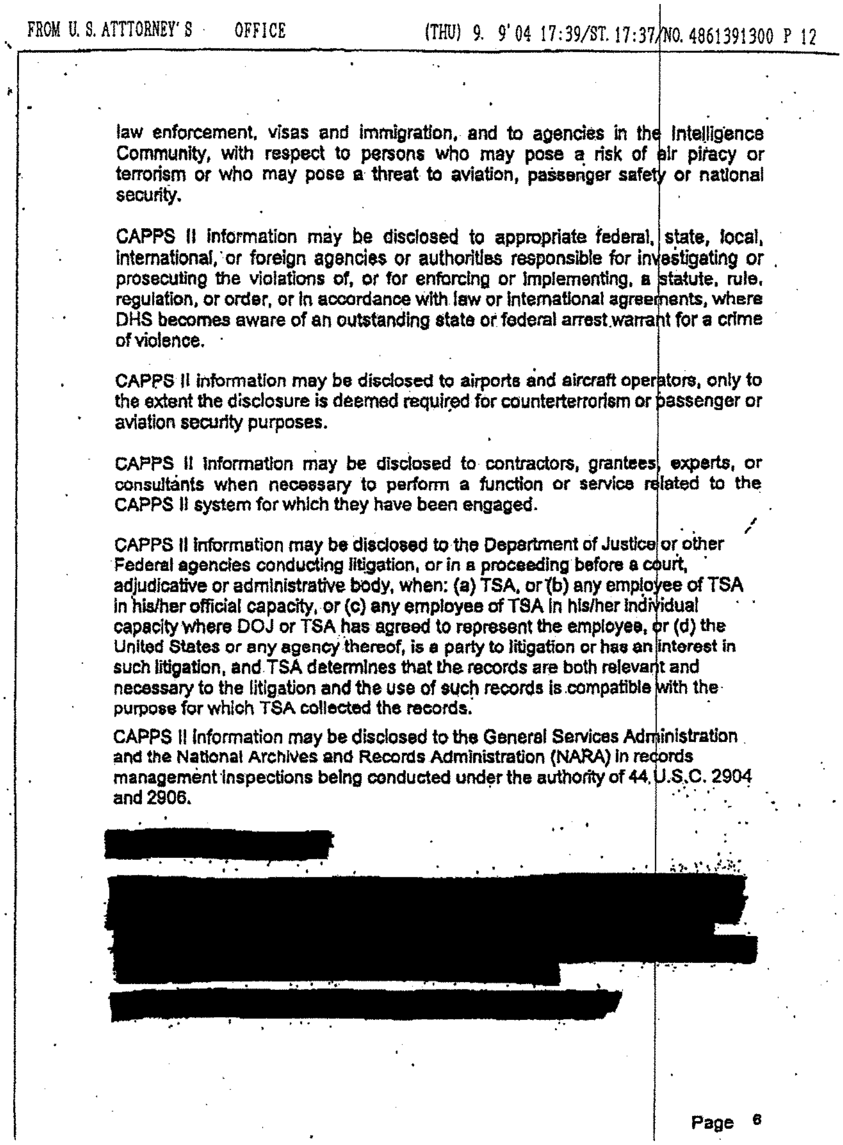
[redacted]

[redacted]

[redacted]

[redacted]

Page 3



law enforcement, visas and immigration, and to agencies in the Intelligence Community, with respect to persons who may pose a risk of air piracy or terrorism or who may pose a threat to aviation, passenger safety or national security.

CAPPS II information may be disclosed to appropriate federal, state, local, international, or foreign agencies or authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, or order, or in accordance with law or international agreements, where DHS becomes aware of an outstanding state or federal arrest warrant for a crime of violence.

CAPPS II information may be disclosed to airports and aircraft operators, only to the extent the disclosure is deemed required for counterterrorism or passenger or aviation security purposes.

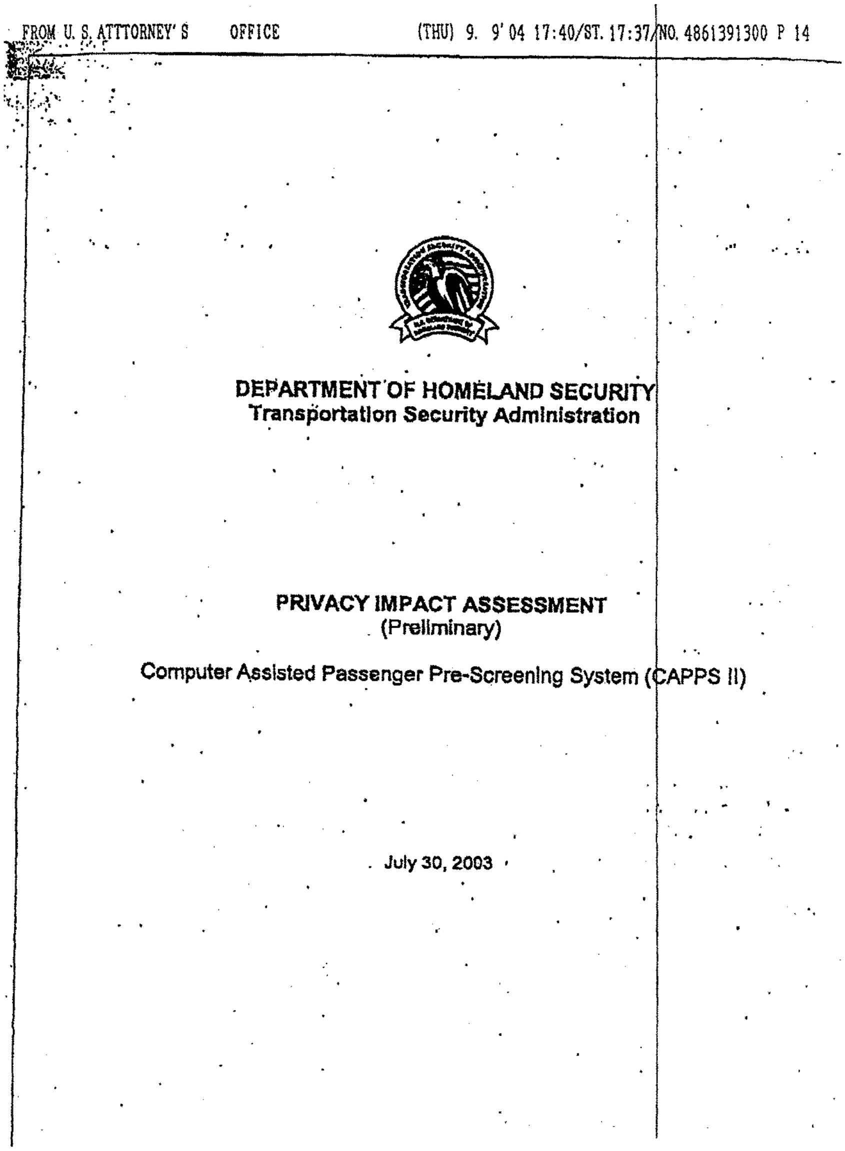
CAPPS II information may be disclosed to contractors, grantees, experts, or consultants when necessary to perform a function or service related to the CAPPS II system for which they have been engaged.

CAPPS II information may be disclosed to the Department of Justice or other Federal agencies conducting litigation, or in a proceeding before a court, adjudicative or administrative body, when: (a) TSA, or (b) any employee of TSA in his/her official capacity, or (c) any employee of TSA in his/her individual capacity where DOJ or TSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to litigation or has an interest in such litigation, and TSA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records.

CAPPS II information may be disclosed to the General Services Administration and the National Archives and Records Administration (NARA) in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

[redacted]

[redacted]



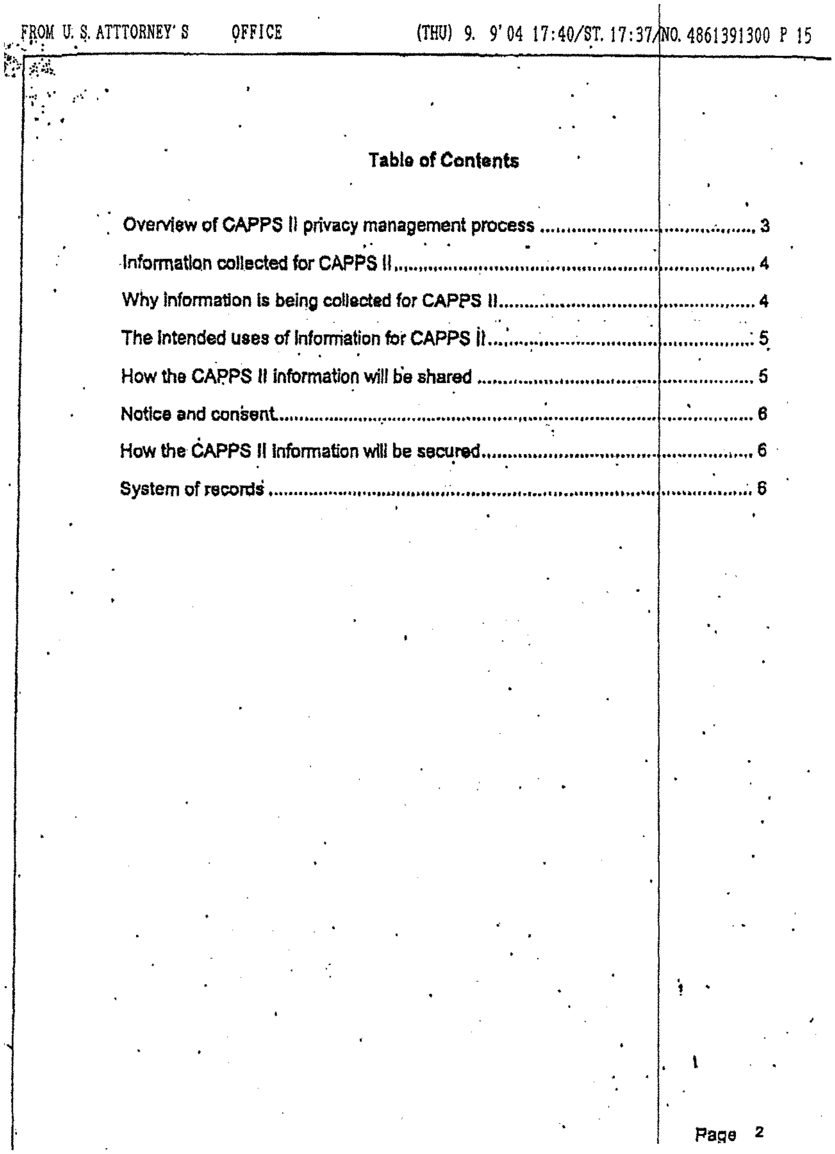
FROM U.S.ATTTORNEY'S OFFICE (THU) 9. 9'04 17:40/ST.17:37/NO.4861391300 P 14

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

PRIVACY IMPACT ASSESSMENT
(Preliminary)

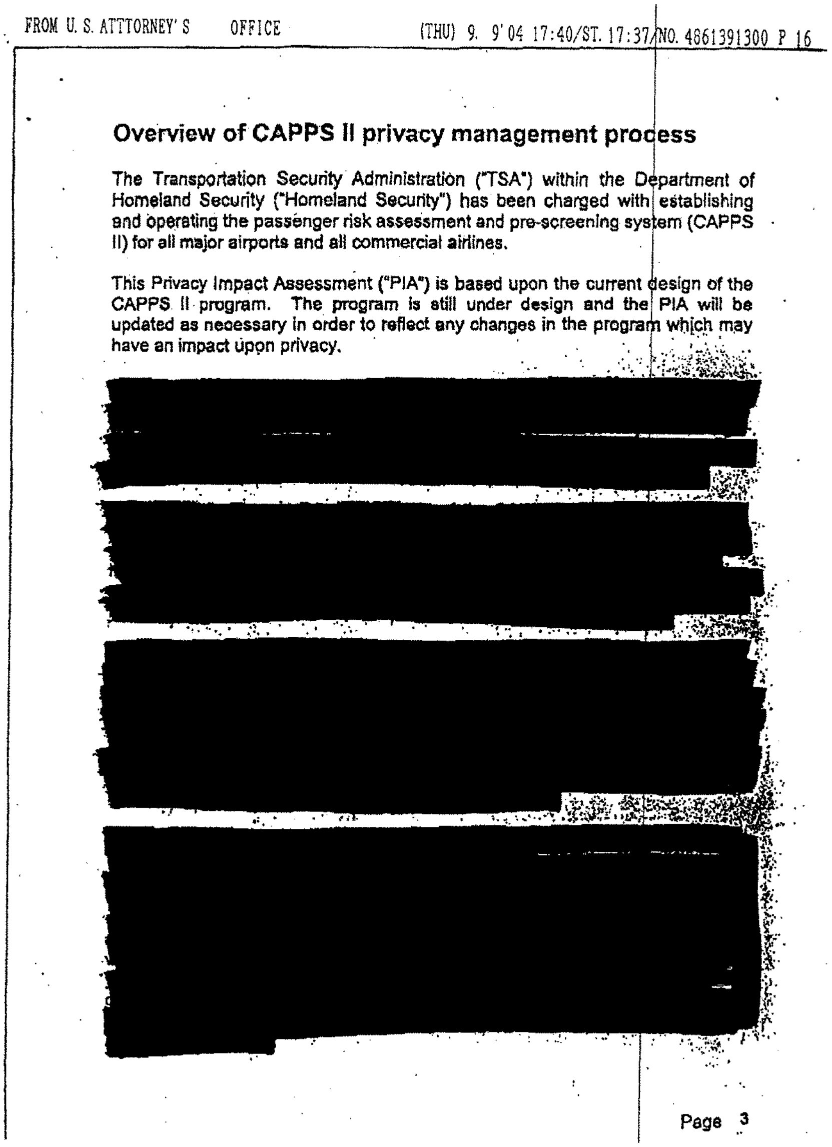
Computer Assisted Passenger Pre-Screening System (CAPPS II)

July 30, 2003



FROM U.S. ATTTORNEY'S OFFICE (THU) 9. 9'04 17:40/ST. 17:37/NO. 4861391300 P 15

Table of Contents



Overview of CAPPS II privacy management process

The Transportation Security Administration ("TSA") within the Department of Homeland Security ("Homeland Security") has been charged with establishing and operating the passenger risk assessment and pre-screening system (CAPPS II) for all major airports and all commercial airlines.

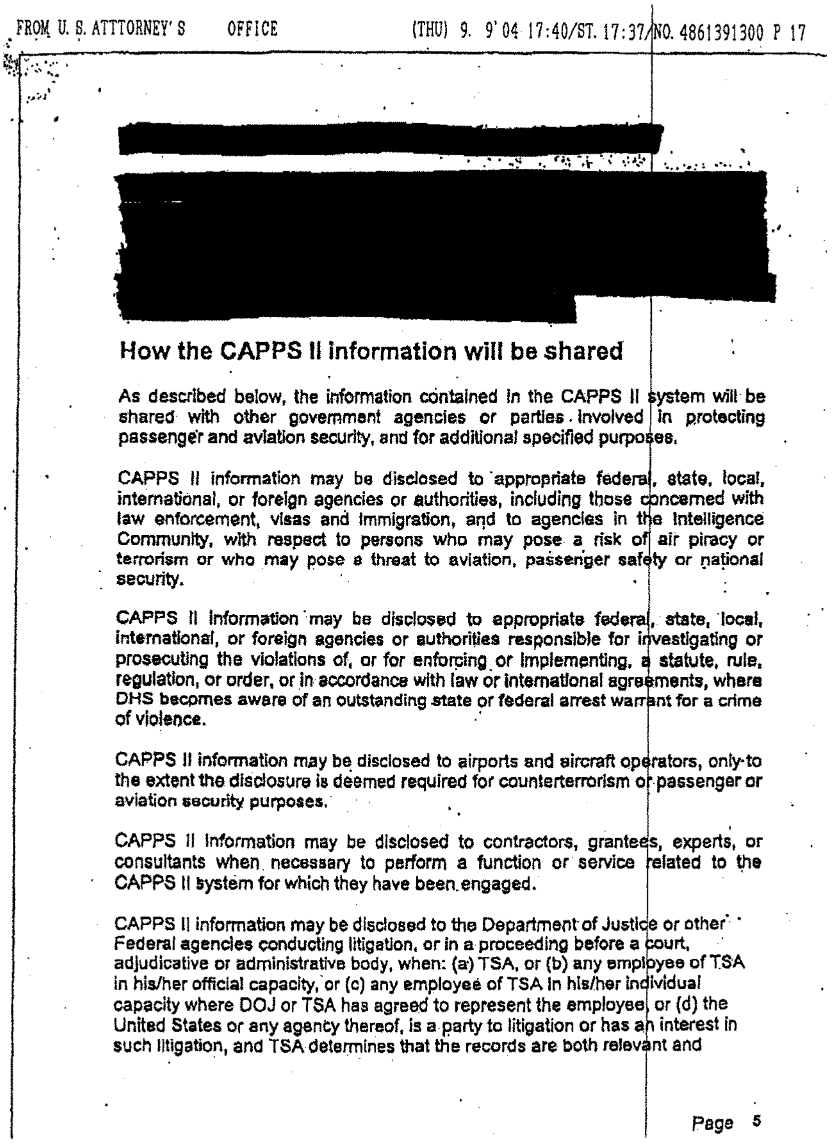
This Privacy Impact Assessment ("PIA") is based upon the current design of the CAPPS II program. The program is still under design and the PIA will be updated as necessary in order to reflect any changes in the program which may have an impact upon privacy.

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

How the CAPPS II information will be shared

As described below, the information contained in the CAPPS II system will be shared with other government agencies or parties involved in protecting passenger and aviation security, and for additional specified purposes.

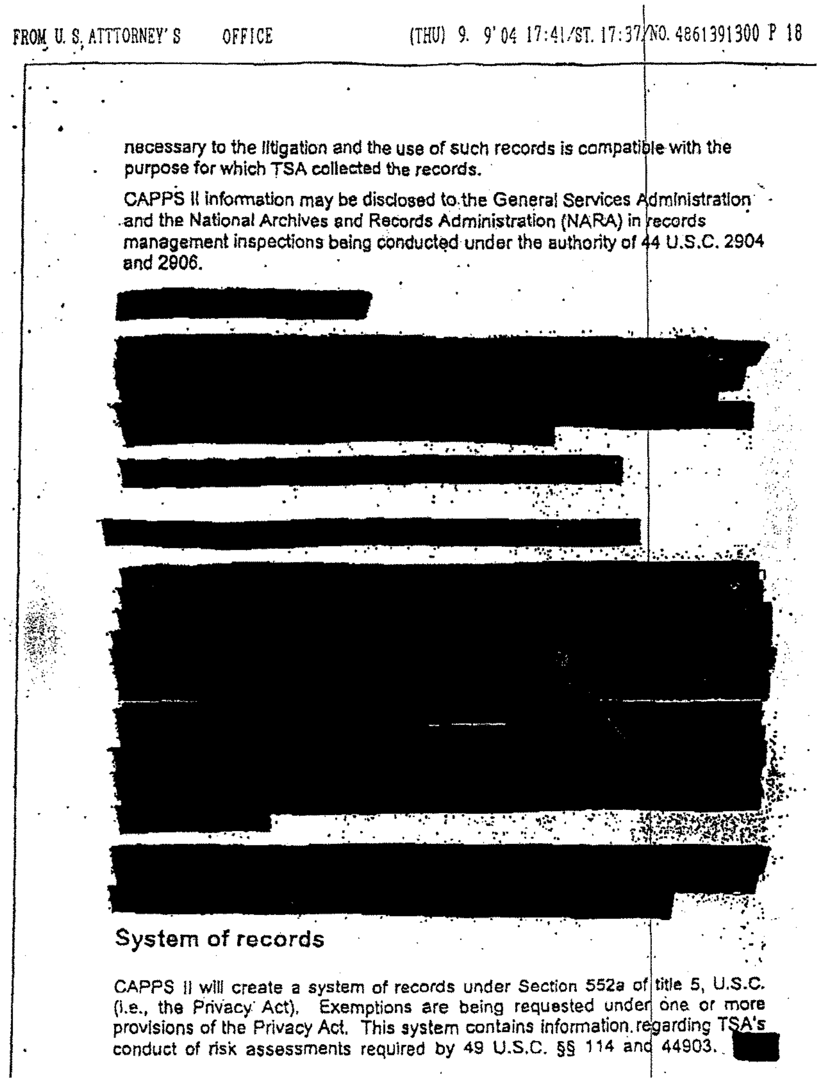
CAPPS II information may be disclosed to appropriate federal, state, local, international, or foreign agencies or authorities, including those concerned with law enforcement, visas and immigration, and to agencies in the Intelligence Community, with respect to persons who may pose a risk of air piracy or terrorism or who may pose a threat to aviation, passenger safety or national security.

CAPPS II information may be disclosed to appropriate federal, state, local, international, or foreign agencies or authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, or order, or in accordance with law or international agreements, where DHS becomes aware of an outstanding state or federal arrest warrant for a crime of violence.

CAPPS II information may be disclosed to airports and aircraft operators, only to the extent the disclosure is deemed required for counterterrorism or passenger or aviation security purposes.

CAPPS II information may be disclosed to contractors, grantees, experts, or consultants when necessary to perform a function or service related to the CAPPS II system for which they have been engaged.

CAPPS II information may be disclosed to the Department of Justice or other Federal agencies conducting litigation, or in a proceeding before a court, adjudicative or administrative body, when: (a) TSA, or (b) any employee of TSA in his/her official capacity, or (c) any employee of TSA in his/her individual capacity where DOJ or TSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to litigation or has an interest in such litigation, and TSA determines that the records are both relevant and



FROM U. S. ATTTORNEY'S OFFICE (THU) 9. 9'04 17:41/ST. 17:37/NO. 4861391300 P 18

necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records.

CAPPS II information may be disclosed to the General Services Administration and the National Archives and Records Administration (NARA) in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

System of records

CAPPS II will create a system of records under Section 552a of title 5, U.S.C. (i.e., the Privacy Act). Exemptions are being requested under one or more provisions of the Privacy Act. This system contains information regarding TSA's conduct of risk assessments required by 49 U.S.C. §§ 114 and 44903. [redacted]

Questions for the Witnesses from the Honorable Dan Lungren

1. Each program proposed to be transferred into the Screening Coordination and Operations Center (SCO) has a slightly different customer base and screening requirement. How will the SCO seek to harmonize those requirements? No response has been received.

2. The SCO emerged from the actions taken per Homeland Security Presidential Directive 11 (HSPD–11). This HSPD mandated a government wide review, led by the Secretary of Homeland Security, of existing screening efforts; however, this office only proposes to consolidate DHS programs. Did the Department consider any programs outside DHS for consolidation into SCO? Which programs were considered? Why were certain DHS screening programs proposed for transfer, while other screening programs were not? What was the guiding rationale for consolidation? No response has been received.

3. Does the Department plan to move forward with the SCO prior to fiscal year 2006? If so, will other programs be considered for consolidation? Will the SCO eventually focus on cargo screening? No response has been received.

4. How will the transition of Secure Flight to the SCO add additional privacy protections? Can you elaborate on how privacy will be enhanced by the creation of the SCO? No response has been received.

5. Please expand on how the united credentialing process under the SCO will facilitate and reduce redundancies in the issuance of credentials for the included programs, such as FAST, NEXUS, Registered Traveler, and HAZMAT licenses? Is it envisioned that there will be one office to coordinate the security checks, liaison with the FBI on fingerprints, and the establishment of joint enrollment centers? No response has been received.

6. The Committee is closely following the deployment of an exit screening capability to US–VISIT. Please provide the Committee with an update on where this technology stands. Further, what are the potential benefits to US–VISIT of being incorporated into the Screening Coordination and Operations Center (SCO)? No response has been received.

7. In your opinion, is it possible to unite or coordinate the US–VISIT Exit component at airports with TSA's plans to use electronic boarding passes during security checks to ensure that visa holders are "checked-out" when leaving the U.S.? Will the inclusion of both of these programs in the SCO provide an opportunity for discussions to move forward on this possibility?

8. What is the status of the strategic plan that US–VISIT has been developing, which will describe the "end vision" of the program? When can Congress expect to see the final version? No response has been received.

9. As US–VISIT deploys at ports of entry, installation of additional infrastructure—such as new computer workstations, printers, fingerprint scanning machines and cameras, modified work stations, and ensuring adequate power availability—will be required. How is this process coordinated with other large systems being developed, such as CBP's Automated Commercial Environment (ACE) program, which will require similar infrastructure needs? No response has been received.

10. The fiscal year 2006 budget request contains a $50 million increase over fiscal year 2005, of which $24 million is proposed to create a ”person-centric" view of border management. Can you expand on what this includes, how you envision it being developed (i.e., development of a new database or linking legacy systems), and what models exist either in the U.S. or internationally that you will be reviewing in the development of this "person-centric" system? No response has been received.

Questions for the Witnesses from the Honorable Bennie G. Thompson

1. Can you please explain the Department's rationale for requesting that certain programs be included as part of the SCO office—such as US–VISIT or Secure Flight–while others, such as CPB's National Targeting Center or its Automated Commercial Environment (ACE) program (which is similar to US–VISIT for goods and cargo), are not included? No response has been received.

2. How will those bureaus responsible for the actual operations of the various screening programs interact with the SCO? What resources and authorities will the SCO need to effectively manage and coordinate these

screening programs? Second, what is the chain of command? Who is responsible for making these screening programs work and work together? Will those agencies responsible for these screening programs now report to the head of the SCO? Who can Congress look to for accountability on these projects given the enormous amount of tax dollars that are being appropriated to these programs? No response has been received.

3. One of the goals of the SCO is to integrate the various databases associated with the screening systems being moved to the office. The biggest problem is that many of the existing systems SCO will attempt to "integrate" are obsolete. The legacy systems cannot be integrated and therefore they need to be replaced by modem, modular, interoperable systems. However, the SCO budget request does not include the funds to do this. No response has been received.

In order to accomplish SCO's mission, won't most of the existing computer screening systems need to be completely replaced since many run in ancient computer languages on obsolete hardware? No response has been received.

When can we expect SCO to achieve appropriate interoperability and data-sharing among screening systems? How much more money will be needed in the years beyond fiscal year 2006? No response has been received.

4. A new report by GAO stated that "DHS has not employed rigorous, disciplined processes typically associated with successful programs, such as tracking progress against commitments." If DHS is struggling to manage just the US–VISIT program, how successful will SCO be at the even more complex task of managing US–VISIT and seven other programs? No response has been received.

US–VISIT

1. The President's Budget Justification requests $390 million for US–VISIT. A new report by GAO raises questions about whether DHS' can deliver "promised capabilities and benefits on time and within budget" for US–VISIT. No response has been received.

Will this level of funding allow you to achieve the goals of building an entry and exit system at the remaining land ports of entry by the end of this year? No response has been received.

2. The law states that the entry exit system has to match "an alien's available arrival data with the aliens' available departure data." Can you better define for us what "available data" means? And what available data is currently available for aliens exiting the U.S. at our land borders? No response has been received.

I understand that this information is required in a report that was supposed to be submitted to Congress on December 31, 2004. When will that report be provided? No response has been received.

3. GAO has identified shifting milestones and uncertainty about the benefits and the cost of what you are building and it appears that from one year to the next, the Department's projections and cost estimates are not reliable. We want to be sure that money spent on US–VISIT results in a more effective and secure entry-exit system. No response has been received.

Are you tracking the cost of each increment of US–VISIT? Can you tell us today what measures of performance we can use to see that you are building such a system? No response has been received.

4. DHS officials claim that they have a "short-term" US–VISIT solution. Can you tell us what it is and whether and how it fits into the long term solution? Would you be proceeding along the lines of the short term solution if you did not have the DMIA deadlines to meet? No response has been received.

5. The Data Management Improvement Act mandated a review of the entry-exit program and required that the program be updated and improved based on the recommendations of a Task Force. The Task Force issued two reports and was disbanded; however, the law stated that the Task Force should be terminated when its work was complete. Many might interpret the disbanding of the task force as the desire of DHS to minimize scrutiny of the program. No response has been received.

Can you please explain why the Task Force was disbanded with so much left to do? Would it be a good idea for Congress to legislate a new Task

Force and that this time Congress mandate that this independent Task Force be in place for a set number of years to report on the program and how it might be improved? No response has been received.

6. The Department of Homeland Security is currently rolling out two major border screening programs—US–VISIT, which is focused on people, and ACE, the Automated Commercial Environment—which is focused on vehicles and cargo. Both programs have ambitions of serving as the primary border security information sharing system. A new report from GAD indicates that little to no work has been done to integrate US–VISIT and ACE. The materials we received from the Administration indicate that US–VISIT will be in the SCO but that ACE will not. Can you please explain why ACE, a major border security program, is not included in the SCO? No response has been received.

7. Will the Screening Coordination Office examine the possibility of utilizing various Border and Transportation Security employees for various screening functions depending on their locations at ports of entry and overseas? Is it possible that TSA screeners might be the most appropriate people to do exit screening? No response has been received.

Secure Flight

1. The 9–11 Commission recommended that TSA improve its use of watchlists in pre-screening passengers. I'm glad that we're finally going to screen passenger manifests against all terrorist watchlist records and not just the no-fly list. but it is my understanding that TSA's new Secure Flight plan as currently designed has no protections against identity fraud. Will DHS develop such protections to prevent identity fraud? No response has been received.

Also, section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (or, the "9/11 bill") mandated that by February 7, 2005, DHS begin to establish a process to compare passenger information on any international flight with the government's terrorist watchlist before a plane takes off for the U.S. What progress has DHS made to date to ensure that passengers on international flights are checked against a watchlist? No response has been received.

Registered Traveler

1. I understand that TSA has begun to test the registered traveler program on a volunteer pool of frequent fliers. As I understand it, TSA and the airports are looking at the possibility of dedicating screener lanes at checkpoints for registered travelers. While I can imagine concerns over a program that lets some people skip screening lines, I'm more concerned about the security implications. We know that most airports are already using fewer screeners than ideal, and this proposal would dedicate screeners and detection machines to a small percentage of the passengers. This is going to mean that non-Registered Travelers will be facing even longer lines, and that the pressure on the screeners to move people and bags through will be even greater. Can you explain how this system will run without compounding the screening problems we already have? No response has been received.

2. I've heard the Registered Traveler program justified on the grounds that fewer screener resources will be used on a low-risk population that has provided TSA with additional information. There are two problems I'd like you to address: No response has been received.

First, isn't it reasonable to think that a terrorist group would want to find someone that can get passed your background check with the goal of having less attention paid to them? No response has been received.

Secondly, is the background check planned under the Registered Traveler program any different than what is intended to be done under the former CAPPS II system? If so, what additional security will be gained by having people sign up as Registered Travelers once the new Secure Flight (the replacement for CAPPS II) system is running? No response has been received.

FAST

1. Ms. Spero, I have talked to many truck drivers who would like to participate in the FAST program, but many cite the difficulty of getting the driver credential due to the time it takes for the background check to be completed. For example FAST applicants on the Southern Border must submit

their application to Mellon Bank in Pittsburgh, PA and then it is sent to the CBP risk assessment center in Vermont. No response has been received.

First why do applications for FAST on the Southern border get sent to Pittsburgh rather than a bank or auditor located in California, Texas, or Arizona?

2. I have also heard that many truck drivers feel that the processing center in some cases forces them to go out of their way when their routes take them across remote border crossings. No response has been received.

Has CBP began to look at ways of leveraging existing DHS resources to expand the processing centers or explored ways to reach out to the trucking community to reach truck companies in remote border locations? No response has been received.

NEXUS

1. In the past I understand that NEXUS/SENTRI applications have been handled by CBP at the local level. I am informed that soon all NEXUS/SENTRI applications will be sent to the Citizenship and Immigration Services' Vermont Service Center (VSC) for processing. 'This change in procedures is expected to result in a higher NEXUS/SENTRI denial rate as the VSC is not expected to take the time to interview an applicant in the event of some kind of hit in the system during the background check process. No response has been received.

Will NEXUS/SENTRI processing be centralized at VSC? When? No response has been received.

What branch of DHS has primary responsibility for NEXUS/SENTRI? Prior to the SCO initiative it appeared that CBP was in charge of enrollment, but now given the central enrollment process, it appears that CIS may be charged with this responsibility? When these programs are part of the SCO what roles will CIS and CBP play? No response has been received.

2. My staff was informed that a U.S. citizen residing in Washington State was recently denied enrollment in the NEXUS Air program through an application made at Vancouver International Airport. The person is enrolled in the land border NEXUS program. No response has been received.

Is there a different standard for enrollment in the NEXUS Air program versus the NEXUX land border program? No response has been received.

Is there an appeals process to address NEXUS denials? No response has been received.

3. It seems that two different NEXUS programs are evolving. The first is the land based NEXUS program which uses photos and index finger prints as its biometric identifiers. The second is NEXUS Air that uses retina scans as its biometric identifiers. A person enrolled in the land border NEXUS program cannot use NEXUS Air and vice versa, although that person has been pre-screened as being a low-risk border crosser. No response has been received.

What step if any will be undertaken to allow persons enrolled in one NEXUS program to use the other program? What is the timeline for implementation of these steps? No response has been received.

4. NEXUS technology at a land border crossings at Blaine Washington (and perhaps other crossings) seems to work at a less than optimal fashion. For example, the remote RF reader :frequently does not work. requiring NEXUS enrollees to physically hand their cards to the CBP officer staffing the booth at the crossing who in turn scans the card on a reader to which he has direct access. In recent weeks a technician has been observed making modifications to the remote NEXUS scanning equipment in place at the crossing. No response has been received.

What RF technology and/or equipment problems exist at present at the various NEXUS crossings? What is the estimated cost for remedying these problems? No response has been received.

QUESTIONS FOR THE WITNESSES FROM THE HONORABLE EDWARD J. MARKEY

1. Could the types of privacy breaches that have occurred at ChoicePoint also occur at the Office of Screening Coordination and Operations? What specific actions will the SCO implement to reduce the risk that the personal information maintained by the Office will not be accessed by unauthorized individuals? No response has been received.

2. Which of the following types of personal information will the SCO be responsible for collecting or maintaining? Social Security numbers; home addresses; telephone numbers; fingerprints; photographs; employment records; birth dates; travel records? Are there any other types of personal information that the SCO will collect or maintain? If yes, what are they? No response has been received.

3. How long will the SCO store each of the types of personal information that it collects or maintains? With which entities outside of the SCO will the Office share the personal information that it collects or maintains? No response has been received.

4. What types of analysis will the SCO perform on the data that it collects or maintains? No response has been received.

5. If the private information managed by this new Office were to be stolen, would the Department be required to notify all of the consumers whose information was released? No response has been received.

6. What role, if any, will the Office of Screening Coordination and Operations (SCO) have in the screening of cargo? No response has been received.

7. If the SCO will have a role in cargo screening, will it be involved in screening of cargo carried on all-cargo planes and/or cargo carried on passenger planes? No response has been received.

8. How will the SCO interact with the cargo industry? No response has been received.

9. What authority will the SCO have to initiate and develop regulations? No response has been received.

10. Will SCO be involved in the issuance of private sector grants for security initiatives? No response has been received.

11. Will sea be responsible for disseminating threat information to industry based on the information the Office is responsible for maintaining? No response has been received.

○