S. HRG. 111–883

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 29, 2010

Serial No. J–111–104

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

64–705 PDF WASHINGTON : 2011

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

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ARLEN SPECTER, Pennsylvania
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
BRIAN A. BENZCOWSKI, *Republican Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

BENJAMIN L. CARDIN, Maryland, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
AL FRANKEN, Minnesota
EDWARD E. KAUFMAN, Delaware

JON KYL, Arizona
ORRIN G. HATCH, Utah
JEFF SESSIONS, Alabama
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BILL VAN HORNE, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	1
prepared statement	52
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	3

WITNESSES

Kutz, Gregory D., Managing Director, Forensic Audits and Special Investigations Unit, U.S. Government Accountability Office, Washington, D.C.	4
Sprague, Brenda S., Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. Department of State, Washington, D.C.	6

QUESTIONS AND ANSWERS

Responses of Gregory D. Kutz to questions submitted by Senator Cardin	22
Responses of Brenda S. Sprague to questions submitted by Senator Cardin	27

SUBMISSIONS FOR THE RECORD

Arnold, Robert, National Vice President, National Federation of Federal Employees (NFFE), Washington, DC, statement	45
Kutz, Gregory D., Managing Director, Forensic Audits and Special Investigations Unit, U.S. Government Accountability Office, Washington, D.C., statement	60
Sprague, Brenda S., Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. Department of State, Washington, D.C., statement	74

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

THURSDAY, JULY 29, 2010

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM,
TECHNOLOGY AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Benjamin Cardin, Chairman of the Subcommittee, presiding.

Present: Senators Hatch and Kyl.

OPENING STATEMENT OF HON. BENJAMIN CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Senator CARDIN. The Subcommittee on Terrorism and Homeland Security will come to order. I want to thank our witnesses for being here today. I want to first thank Senator Kyl and Senator Feinstein for their strong interest and continuing interest in this issue of the integrity and security of the passport issuance process.

On May 5, 2009, over 14 months ago, I chaired the Terrorism Subcommittee hearing entitled The Passport Issuance Process: Closing the Door to Fraud. Today we are holding part two of that hearing. And quite frankly, I didn't anticipate that we were going to need a second hearing on this subject when I convened the first hearing 14 months ago.

During that hearing last year, we learned about the Government Accountability Office's undercover investigation that had been requested by Senator Kyl and Senator Feinstein to test the effectiveness of the passport issuance process, and to determine whether malicious individuals such as terrorists, spies and other criminals could use counterfeit documents to obtain a genuine U.S. passport.

What we learned at that time concerned me a great deal. GAO reported to the Subcommittee, and I'm going to quote from its 2009 report, "Terrorists or criminals could steal an American citizen's identity, use basic counterfeiting skills to create fraudulent documents for the identity, and obtain a genuine U.S. passport."

"GAO conducted four tests simulating this approach and was successful in obtaining a genuine U.S. passport in each case. In all four tests, GAO used counterfeit and/or fraudulently obtained documents."

The May 2009 GAO report went on to note that the State Department and U.S. postal employees did not identify GAO documents as counterfeit. And further noted, and I'm quoting, "GAO investigators later purchased an airline ticket under the name used

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

of the four fraudulently obtained U.S. passports and then used that passport as proof of identity to check into his flight, get a boarding pass and pass through security checkpoints at a major metropolitan area airport." That was the 2009 report.

But it was not the first report to identify problems with the passport issuance process. In 2005 and 2007, GAO brought these issues to light. As a result, the GAO's 2009 report stated, and again I'm quoting from the GAO report, that "State Department officials have known about the vulnerabilities in the passport issuance process for many years but have failed to effectively address these vulnerabilities."

Those were very serious findings back in May of 2009 because the U.S. passport is the gold standard for identification. A U.S. passport can be used for many purposes in this country and it gives an individual the ability to travel internationally which is an important tool for someone who wants to do us harm, including terrorists, spies and other criminals.

So the integrity and security of the passport issuance process is extremely important because it can have a profound impact on the national security of the United States.

More than 14 months have lapsed since the first GAO report, and today we will be learning about a new GAO undercover investigation that I requested along with Senators Kyl, Feinstein, Lieberman and Collins.

In this new investigation, a GAO undercover, used fraudulent identity documents including fake drivers licenses and birth certificates to see if they could obtain genuine U.S. passports. So what happened this time?

Well, once again U.S. postal and State Department employees failed to detect the use of fraudulent identity documents. GAO undercover investigators sought seven passports. Most of them were approved by the State Department. Moreover, four of the passport applications that were submitted used a photograph of the same GAO undercover agent, and two passport applications that were initially approved used Social Security numbers of deceased persons.

There is some news that is a credit to the State Department because the State Department detected two fraudulent passport applications before they were approved. However, what happened, happened before, and we were all under notice that this needed to be changed.

As the Subcommittee attempts to get to the bottom of this, we must not forget that dedicated people are working very hard to correct these problems and they take their responsibilities seriously. But we must do better, much better.

Congress can help by giving the State Department all the tools it needs. In that regard, I am introducing, along with Senators Feinstein and Lieberman, legislation that will help to close the door to passport fraud. Today I'm introducing the Passport Identity Verification Act. This legislation is a common sense solution that will give the State Department the legal authority that it needs to access information contained in Federal, state and other data banks that can be used to verify the identity of every passport ap-

plicant and to detect passport fraud without extending the time that the State Department takes to approve passports.

I also will be submitting for the record a letter from the National Federation of Federal Employees which has previously made a number of recommendations to the State Department as to how to improve the passport issuance process.

And from my perspective, management in the State Department needs to partner with its employees to ensure that their helpful, constructive ideas are implemented. I understand that there is pressure on passport examiners to act quickly. I'm sure some of that pressure comes from Members of Congress on behalf of our constituents and I understand that the American people can become concerned when their travel plans, whether for leisure or business are linked to their ability to obtain a passport in a timely fashion.

But we've got to get this right. It is not simply a question of process, techniques and training. We need to make sure that the agencies that are responsible for processing passport application documents are concerned about national security as well as customer service and we need to make sure that they have the legal authority, the resources and the technology to verify the identity of passport applicants and to detect passport fraud. We simply cannot issue U.S. passports in this country on the basis of fraudulent documents. There is too much at stake. We have the technology, and we have the information to prevent such abuses.

We have with us today two witnesses, one from the GAO and one from the State Department. Before I introduce our two witnesses, let me turn to the Ranking Member, Senator Kyl, and once again before recognizing Senator Kyl, I want to thank him for his interest in this issue, not only his interest but his leadership and the fact that he brought this issue to the Senate's attention.

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

Senator KYL. Thank you, Mr. Chairman. Again, I appreciate your holding this hearing and the work you've done on the legislation that you discussed. I also want to thank Senator Feinstein who can't be here because of a scheduling conflict. But as the Chairman noted, she too has a continuing commitment to continue to pursue this issue surrounding fraudulent passports.

I agree with Chairman Cardin that the GAO, and the GAO, that the State Department's continued inconsistent application of data verification and counterfeit fraudulent detection techniques must be corrected.

This information from GAO makes us all continue to wonder just how many individuals are fraudulently obtaining U.S. passports. GAO I think accurately calls this the most sought after travel document in the world. So we're talking about something very important.

Back in February of 2008, partially a result of the 2007 Joint Homeland Security FBI Threat Assessment, Senator Feinstein and I asked GAO to report on passport fraud. In March of 2009, it reported on state's weaknesses surrounding the issuance of passports. Senators Cardin, Feinstein, Lieberman and I asked them in

early 2010 for an update on the issue and that is what we are receiving today.

There are a myriad of corrections the State could make to correct some of the vulnerabilities in the passport process. Irrespective of whether State Department passport adjudicators have law enforcement authority, State could work more collaboratively with Social Security Administration to ensure that accurate and appropriate and near real time information about Social Security members is pursued by those approving passport applications.

Additionally, the State Department could work more proactively with the Department of Homeland Security to make sure that the electronic vital events system project, which digitizes birth records, is completed and the State Department in my view should always work to confirm a birth certificate's authenticity.

It is troubling that DHS was required to complete a spending plan for 2010 for the $10 million in appropriations for that consortium project but only yesterday, 10 months into the fiscal year 2010, sent the spending plan up to Congress.

Mr. Chairman, I want to follow up with some more specific questions for our witnesses, but I do want to make clear that the problems that GAO has effectively highlighted both before and today are really indicative of overall identity theft issues that we face as a nation. We've got to continue to work to make sure that individuals cannot fraudulently obtain drivers licenses, passports, visas, border crossing cards and other documents in this country.

I very much look forward to the testimony of our witnesses and again I appreciate your calling this hearing.

Senator CARDIN. Thank you very much, Senator Kyl. Today we will be hearing from two witnesses.

Greg Kutz is the Managing Director of GAO's Forensic Audits and Special Investigation Unit which conducts forensic audits, evaluates security vulnerabilities and conducts investigations of fraud, waste and abuse for Congress. He is also a certified public accountant and certified fraud examiner.

He has been with GAO for nearly two decades and prior to his present position, he was Director of Financial Management at GAO.

Brenda Sprague is Deputy Assistant Secretary for Passport Services in the Consular Affairs Bureau of the Department of State. Ms. Sprague has been Deputy Assistant Secretary of State since July 20, 2008 and she previously served in the State Department's Bureau of Diplomatic Security in its Office of Language Services.

She has also served in the foreign service. Ms. Sprague testified in our hearing on May 5th, 2009. We'll start with Mr. Kutz.

STATEMENT OF GREGORY D. KUTZ, MANAGING DIRECTOR FORENSIC AUDITS AND SPECIAL INVESTIGATIONS UNIT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, D.C.

Mr. KUTZ. Mr. Chairman and Ranking Member Kyl, thank you for the opportunity to discuss passport fraud. Today's testimony highlights the results of our most recent investigation.

My testimony has two parts. First I will discuss what we did and second I will discuss the results of our undercover testing.

First in March of 2009, we reported that State's passport issuance process was vulnerable to fraud. Specifically, we obtained four genuine U.S. passports using counterfeit and fraudulently obtained documents. This is important because as you mentioned and as this posterboard shows, with a U.S. passport, the world is yours.

One year later at your request, we submitted seven fraudulent applications simulating the use of identity theft. For these tests, we used counterfeit and fraudulently obtained documents such as drivers licenses and birth certificates. These documents were prepared using publicly available hardware, software and materials.

We also used seven different Social Security numbers from fictitious and deceased individuals. Two undercover agents applied for passports at six postal service and one State run location. Our tests were done in five different States and here in the District of Columbia.

Now that I have said what we did, let me turn to the results of our undercover testing. As the Chairman mentioned specifically, State issued passports for five of our seven tests.

I have in my hand the three genuine passports that we obtained. The posterboard shows on my right the actual breeder documents that we used to obtain these genuine U.S. passports. Some of the key flags that State missed include a 62-year-old using a Social Security number issued in 2009, counterfeit drivers licenses and birth certificates as shown on the monitor to my right there, one application with a vast age difference between the passport and drivers license photo and one application with a California mailing address, a West Virginia permanent address and drivers license, and a Washington, D.C. telephone number.

This time as you mentioned there was improvement as State denied two of our applications after determining that they were fraudulent. For the first one denied according to State, they identified issues with our Social Security number. Subsequently they determined that our Florida birth certificate and our West Virginia drivers licenses were bogus.

For the second denial, State identified discrepancies again in our Social Security number on our application. This time there were discrepancies against the birth date and Social Security records. Once again they determined that our drivers license and birth certificate were bogus.

It also appears in this case that they had questions as to why the application was filed in Illinois, but the mailing address and drivers licenses were from Virginia and West Virginia.

For the last two applications, physical passports were issued. However, according to State, these two passports were flagged when facial recognition technology linked the photos to our prior applications. State then recovered these two physical passports from the mail system.

It is not clear why State was in some instances able to identify fraud and in other instances was not. As you both mentioned, one of the reasons for us being here today is to provide you with a status report on State's progress and its improvement initiatives. Another important benefit from today is for State to take these seven applications, and use them to improve their human capital, processes and the use of technology.

In conclusion, significant concerns remain about State's ability to prevent passport fraud. With hundreds of different drivers licenses and birth certificates out there, recognizing counterfeits is a significant challenge.

We look forward to continuing to work with this Subcommittee and State to improve passport fraud prevention controls.

Mr. Chairman, that ends my statement, and I look forward to your questions.

Senator CARDIN. Thank you very much. Ms. Sprague.

STATEMENT OF BRENDA S. SPRAGUE, DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE, WASHINGTON, DC

Ms. SPRAGUE. Thank you for the opportunity to discuss the Department of State's response to concerns raised by the Government Accountability Office in their latest undercover investigation of passport operations.

Today I also seek your support for initiatives to assist the Bureau of Consular Affairs to detect and prevent passport fraud.

We are fully committed to continually improving our system in order to maintain the most secure passport issuance system possible. That system, however, is not yet foolproof. We have made dramatic improvements over the past year and we will continue to work diligently to improve training, procedures and oversight of the passport application and adjudication processes.

Through existing fraud detection procedures, we recently discovered that the GAO was conducting an undercover investigative operation of passport services. Investigators trained in document fraud submitted seven passport applications. They used legitimately issued Social Security numbers, counterfeit birth certificates and fake drivers licenses.

We immediately identified fraud in two of their applications and identified fraud in two more prior to delivery. However, they successfully obtained three passports.

Immediately upon discovering this GAO undercover operation, we took action. We placed all personnel involved in the issuance of those passports on 100 percent audit, conducted fraud training for all adjudicators and for the acceptance facilities involved, accelerated an aggressive deployment schedule of enhancements to our issuance system, which incorporated facial recognition technology, strengthened requirements for use of out of state identity documents, and developed a training module for all adjudicators on the adjudication and fraud issues raised by the GAO probe.

We also initiated several longer range projects which include conducting a pilot of commercial database identity scoring, acquiring forensic document expertise in the development and delivery of our training programs, developing standardized on-line fraud indicator check sheets for our adjudicators and incorporating enhanced front end data checks into our document issuance system.

Following a similar GAO operation 2 years ago in which we failed to detect any of the four applicant's fraudulent applications, we made process improvements and were more successful in detecting GAO's latest efforts. Even one passport issued in error is one

too many and I am more upset than anyone that this has occurred. However, it was exactly the improvements which we put in place after the 2009 GAO operation that allowed us to recognize this operation before the GAO notified us.

Following the first GAO investigation, we undertook the systematic review of our operations and developed a remedial plan that included revising adjudication standards and processes. Recalculating production standards, doubling the number of personnel devoted to fraud detection, enhancing data checks as part of our front end processing, introducing facial recognition technology and expanding the training provided to both specialists and supervisors in adjudication and in fraud detection.

We have done much to address the vulnerabilities, but let me ask your help to eliminate them. The greatest threat to the integrity of the passport issuance process is document fraud. We need additional tools and stronger authority.

First, we seek your assistance to pass legislation to designate Consular Affairs as a law enforcement entity for the purpose of data sharing. We need full access to state registries of births and death, and other identity information. Currently our access is restricted by the lack of such designation.

Second, we seek the subcommittee's support to encourage standardization of the birth documents that we accept as proof of citizenship. There are more than 6,400 jurisdictions issuing birth certificates in the United States with more than 14,000 versions in circulation.

Thirteen states allow open access to birth records allowing virtually anyone to purchase copies of birth certificates on file. Differences in paper, format, signatures and security features make the detection of fraudulent birth certificates daunting.

This is a challenge we face, and we face it every day. It is crucial that Congress encourage standardization of the birth documents that we accept as proof of citizenship.

Third, we request your support to pass legislation to mandate that all passport applicants provide their Social Security numbers. In addition to birth documentation, we rely heavily on Social Security data to verify the identity of passport applicants. We seek legislation mandating that applicants provide Social Security numbers.

Finally, we need your support for continued retention by the State Department of the WHTI surcharge as requested in the President's fiscal year 2011 budget. We need these funds to strengthen our systems and to combat fraud. Our request is part of a larger fee retention package which is in the President's 2011 budget.

Distinguished members of the subcommittee, I appreciate the constructive approach of this committee. I believe that all of us in the federal government are committed to enhancing our services so that they are safe, secure, efficient, equitable and responsive to the needs of the American people.

I hope that you will support the initiatives I discussed, for they are essential to detecting and preventing passport fraud. I am ready to take your questions. Thank you.

Senator CARDIN. Well, thank you for your testimony. Mr. Kutz, let me at least clarify one part of the investigation so I understand it.

In all seven of the efforts there was a false drivers license used, am I correct on that?

Mr. KUTZ. Yes. Six from West Virginia and the one in D.C. we used an actual D.C. counterfeit, correct.

Senator CARDIN. And none of these fake drivers licenses triggered the rejection of a passport, is that correct?

Mr. KUTZ. Not initially. We understand the two that were caught were initially because of the Social Security number discrepancies that then led to further investigation. That's our understanding.

Senator CARDIN. So it was the Social Security number that triggered the first two, and then there were facial differences I understand it on the next two that——

Mr. KUTZ. Not a facial difference, a facial match. In other words, we had multiple people, same faces with multiple passports. That's what we understand triggered the other ones.

Senator CARDIN. None of the triggering was, I guess my point is that you were able to use false, fake drivers licenses without getting detected basically?

Mr. KUTZ. The initial intake of those documents you see on my right, we don't believe anyone ever recognized those as counterfeits, that's correct.

Senator CARDIN. Thank you, that's helpful. Ms. Sprague, let me take you back to the May, 2009 hearing. You expressed some of the same sentiments at that hearing as you are now about how disappointed you are that you're not 100 percent, and that you take these issues very, very seriously.

You also said that you were going to use your own red teams because you knew that the GAO would be back looking and you wanted to make sure that you were ready for that. Did you use red teams?

Ms. SPRAGUE. Yes, we did.

Senator CARDIN. How well did you do?

Ms. SPRAGUE. There were six attempts and we caught five of them.

Senator CARDIN. So GAO is better than your red teams?

Ms. SPRAGUE. GAO can get real Social Security numbers and diplomatic security can't.

Senator CARDIN. So I guess the other thing that has me a little bit concerned in your response is that you said that you detected the two, therefore you knew that GAO was after you, or at least was doing their investigation, and then you changed your procedures it looks like in order to counter what GAO was doing, which is fine.

But we thought you would have the procedures to detect what terrorists, criminals, those who want to harm us, or those who just want to get a passport who are not entitled to a passport would do.

My point is wouldn't you have taken these precautions from the beginning rather than just as a preemptive measure against a GAO investigation?

Ms. SPRAGUE. Detecting passport fraud and making certain that passports don't go to people who aren't entitled to them is our num-

ber one priority. However, we are taking advantage, if that's the appropriate word, of what we learned from these tests to make our process better.

We also learned from what diplomatic security did and we were able to make our process better, so in that sense. But I do want to clarify one thing and that is that we are in the process of rolling out facial recognition. It is not rolled out across the entire system.

After we realized that, or we believed that it was GAO in process, we wanted to check our system and see if there was anything more, and we were able at the headquarters level using software that is at a very early stage to go out and identify that in fact there were seven pictures that matched prior attempts. So that's how we identified the additional two.

It wasn't that we changed our procedures because of the GAO. It was that we took advantage of a tool that is still in the developmental phase although it is well along and will be in complete operation by the end of September at all our agencies. It is already at six of them. Unfortunately those six were not tested. They were tested at ones where they were not yet functioning. But we didn't change anything just because of the GAO, except that I'd certainly like to think that we get smarter as we go through these things.

Senator CARDIN. But you did use that technology that was being used at other locations, you I guess switched them to where GAO was active.

Ms. SPRAGUE. No, what we are doing across the board is to have facial recognition of all incoming passport applications. We are rolling that out gradually across the network.

However, we have a second tool which is facial recognition on demand where we can take a single photograph when we suspect fraud and run that against the entire database.

As of this moment, it is rolled out to all the agencies. It wasn't there in April and May, but it is a secondary tool. There are actually two parts to our facial recognition technology. One, to do it as part of the up front of the application process, and the other one is to have a secondary check when we encounter a fraud that we can go back and look and see if it's there.

Senator CARDIN. And the purpose of the facial identity is to see whether there is duplicate requests or that you have a visual identification of someone who is not entitled to a passport?

Ms. SPRAGUE. The real thing it does is to identify if there have been multiple issuances to the same individual. So far at the agencies we have, we have not identified anybody using this.

On the facial recognition on demand, we have successfully where we suspected fraud actually identified people not who had passports already, but who were in our Visa lookout file.

So we have used that here and there on spot occasions. That tool is now available to all our fraud managers. It has been in development and it was only available to a handful before this.

Senator CARDIN. Just one more question on this. This technology is used where you suspect there is a problem, it is not used routinely? Even when it is fully implemented it won't be used routinely for every application? Or will it be used for every application?

Ms. SPRAGUE. The facial recognition that was part of our front end process will involve every application that is——

Senator CARDIN. And when will that be fully implemented?

Ms. SPRAGUE. By the 15th of September.

Senator CARDIN. I guess my last question is what should our expectations be here? What is a realistic goal? Are you saying that you can get to 100 percent? I know there is always things that can get by, but should we be expecting that you have the capacity to stop the type of fraudulent applications that GAO is participating in, or is this just a hopeless cause?

Ms. SPRAGUE. I certainly hope it's not a hopeless cause.

Senator CARDIN. It's our fourth investigation. It is my second as Chairman and it is disappointing to see that there was the success in again compromising our system.

I guess—I have confidence in the work that our people are doing but I think we need to have an honest assessment as to whether our passports are going to be safe or not.

Ms. SPRAGUE. I think we have to look at all the aspects of passport safety. First of all, we have achieved great success against counterfeiting of our passport document with our new E-passport and that has been corroborated by studies and we are very proud of it.

But as we have made our documents more and more counterfeit proof, and I realize somebody is out there right now trying to figure out a way to counterfeit it, it makes it harder on the adjudication side because people attempt to obtain good passports with bad breeder documents. This is a problem that we discussed in the international forum at ICAO and others. It is common to all countries that are issuing travel documentation.

We have got a lot of people working against us and we are always going to be addressing vulnerabilities. Can we get to 100 percent? That is certainly our objective. It is an uphill climb. It requires lots of work, it requires focus every day, it requires resources and we're willing to address all of that.

Senator CARDIN. It just seems to me that a drivers license is a common instrument used and that there needs to be a capacity at the State Department to identify fraudulent drivers licenses. To me that seems like a basic security issue.

Ms. SPRAGUE. And it seems like a basic security issue to me, too. But let me explain to you where we are that we weren't last year. We have with the sponsorship of the Bureau of Diplomatic Security, we have received limited access to the nationwide verification system known as N-LES. We don't have access to all 50 states yet, but we have access to 43. Only one state has turned us down flat.

It is a big leap for them to have done this because we do not have law enforcement identification or identity. I am missing the word there. But they have given us limited access.

Unfortunately, that access, we only have 242 accounts for the whole world and I have 1,200 passport adjudication specialists. So we have focused those both here and overseas in the fraud offices. When we suspect fraud, we can go in and do a limited check of those drivers licenses.

The second thing that is available to us on drivers licenses is that there are machines available. We have done some tests with

them and we are moving forward with the procurement right now for our passport agencies where they will have the ability to see if the drivers license has been tampered.

I have to be honest with you, we did two pilots with them and we didn't catch any counterfeit drivers licenses. We are going to go ahead anyway. But we only see one of ten drivers licenses. The other nine go to the postal acceptance agencies or the non-postal acceptance agencies. They don't have that capacity. Since our largest partner here is the postal service, they really aren't in a position to invest in this technology.

We would have to help the postal service in some way. I would see that as the beginning of the solution. It would detect counterfeit. It would not detect those drivers license which people obtain in another identity other than their true identity. Those will come through as perfect drivers licenses. That is a much harder challenge for us and that requires each of the states to tighten their regulations.

Some states like Colorado and Virginia have done a fantastic job. Other states have not stepped up to the plate. That is a problem that I cannot solve.

Senator CARDIN. Senator Kyl.

Senator KYL. What state turned you down flat?

Ms. SPRAGUE. South Dakota. But in fairness to the good people of South Dakota, they have a very rigid privacy restriction and they absolutely cannot share anything with someone who is not a law enforcement entity.

Senator KYL. By the way, is it Kutz? I don't want to mispronounce your name.

Mr. KUTZ. It is Kutz.

Senator KYL. Kutz. I'm sorry, sir. Well, Mr. Kutz, my understanding is that in your testimony here you have not recommended any additional recommendations because of the view that the previous recommendations have not been implemented.

I wonder if you could tell us your evaluation of the degree to which there has been implementation of your prior recommendations.

Mr. KUTZ. With respect to training, we understand there has been training with respect to passports and the breeder documents that go into getting those. So to the extent that they have done better recognizing those, I think in most cases they are not recognizing the counterfeit breeder documents and that is difficult because there are hundreds or thousands of different birth certificates and drivers licenses out there.

We do understand that they are doing more of a match with Social Security and the death records. Two of the cases here we understand they caught based upon a match. Last time they weren't checking the death file, for example, so we think that they've made some progress there.

She talked about getting the ability to validate with the DMVs and the Vital Statistics on birth certificates. Those are critical elements of being able to authenticate the hundreds of different drivers licenses and birth certificates. We certainly support them doing red team. That was one of the things we recommended. We would suggest doing more than six tests a year, but certainly it is up to

their discretion to what they do, but that's a valuable exercise to do the exact same thing that we do to continually test yourself, especially because things here are going to emerge.

One of the things I will just mention because there are a lot of them, but requiring Social Security numbers of people is important. They don't have the authority at this point to require a Social Security number. So you have people who can actually get a U.S. passport without having to provide a Social Security number. That seems to be a significant issue to us.

Senator KYL. Let me ask you both. Ms. Sprague, you indicated I think three specific things here that would be helpful to you. The standard birth certificate, a legal requirement for Social Security numbers and I'm not sure what specifically with respect to real ID drivers licenses, but some further support for assurance that drivers licenses were not bad breeder documents, is that correct?

Ms. SPRAGUE. We are asking for designation as law enforcement so that we can get access to state and local records verification which we are precluded from because of privacy.

Senator KYL. Understood. But even if you had that, if you had bad breeder documents, you're going to have the same problem that other agencies have in verifying the fraudulent nature of the document.

Ms. SPRAGUE. It would only help us with counterfeits. It would probably not identify breeder documents routinely.

Senator KYL. Right. But the standard birth certificate might help in that regard.

Ms. SPRAGUE. It might. And I want to clarify that I am not asking for a national birth certificate that every state has to follow. The states, if we just were dealing with 50 birth certificates, it would be heaven.

Senator KYL. If they were digitized. In fact maybe you could, either one of you can relate to this program for digitization of the records. How far would that go toward satisfying this requirement?

Ms. SPRAGUE. Well, certainly one of the things that is holding back EVVE is that the states are in such different places in terms of how they have recorded and stored their data. If EVVE could get up and running, that would be a God send to us because we would be able to verify at least that a document was not counterfeit. You can only do that electronically.

So to the extent that the records have not been presented in a somewhat common electronic format, EVVE'S task is daunting.

Senator KYL. With respect to the breeder documents that go into drivers licenses, what recommendations would you have to ensure that the document that you receive is a valid document? This appeared to be 100 percent of the cases you had a bad drivers license. Is that correct?

Mr. KUTZ. Yes. All the drivers licenses were counterfeit. The one in D.C. actually would have traced back to a real drivers license we got using counterfeit breeder documents from another test. So if they did a match on that, they would have actually determined that that person appeared to be real, but the actual drivers license we presented here in D.C. was a counterfeit drivers license.

Senator KYL. OK. So can you answer my question then, ma'am?

Ms. SPRAGUE. I would really like someone who is smarter than I am about the specifics of that to get back to you on it. But I can say in short that we would like the states to make a serious effort to verify that the person who is standing in front of them is in fact the person that they say they are.

I can only speak, for example, for the State of Virginia or the State of Colorado which we are very familiar with because they have worked with us. In the State of Colorado they actually fingerprint people. They do facial recognition. Facial recognition would be terrific for drivers licenses because it would get people who do repeat drivers licenses.

In addition, in the State of Virginia you have to have proof of residence, you have to come up with documents that link you and that gives us a much better trail to go back and say that the people are who they say they are.

Of course what happens now is that people just avoid states that are tough and go to states that have a reputation for being more lenient.

We also very much like those states, Colorado does it, where they indicate when you first got that drivers license so you're just not going that this is a renewal. You can see that the State of Colorado can corroborate this identity back to when someone was 16 years of age. Our passport specialists love that.

Senator KYL. Obviously the percentages in cases where your folks were fooled are not good percentages. I gather there is no way of knowing how many fraudulent or how many genuine passports you might be issuing that are based upon fraudulent data.

Ms. SPRAGUE. Any study that we have done post issuance or when we did our live audit last year, we did not, were not able to discover even when we were going back a significant number. That means either that we're really not doing very many and I believe that is true, but I also believe it is true that once someone gets a good passport with bad documents, it is hard for anybody to find it.

So I don't know what the numbers are. I would like to believe that they are low. Every evidence I have is that they are low, but even one is too many.

Senator KYL. Would you say that if someone, say a terrorist, is bound and determined to get a U.S. passport and has a working knowledge of the kinds of things that you've been talking about here that it is more likely than not that if they use the techniques available to them, including the use of bad breeder documents for obtaining a drivers license, that they would be able to get a genuine passport from the State Department?

Ms. SPRAGUE. I would say, I would remind you that there are two things that we determine. One is identity and the other is citizenship.

I think it is much more difficult for people to try and pass themselves off as Americans than it is for Americans to pass themselves off as other Americans. So if we are looking at homegrown terrorists who wanted to have a separate identity, that causes me tremendous concern.

If you are asking me if I thought a foreigner could come in and easily obtain a passport in his own or another name, I would like

to believe that that would be a far more difficult challenge. We focus a lot of attention on verifying citizenship.

I think that, I would return to my comment. It is easier for an American to pose as another American than it would be for someone who is not an American to pose as one.

Senator KYL. All right. You might need to be careful in view of the judge's decision in Arizona yesterday putting an extra burden on the United States government when you seek to verify U.S. citizenship. They seem to be very fragile in this regard, at least according to the affidavits that were submitted in the case I say facetiously, thank you very much for both of you testifying.

Senator CARDIN. Senator Hatch.

Senator HATCH. Well, thank you, Mr. Chairman. Some of my questions may have been asked because I got here just a little bit late, so if they have, I apologize. Just say they've been answered.

You suggest that the Bureau of Consular Affairs be designated a law enforcement entity in order to access data sharing among Federal, state and local governments.

How would this help your consular officers in combating passport fraud?

Ms. SPRAGUE. I mentioned before but I'm happy to mention it again because I really would like to leave a very strong impression.

This is, the various states have privacy regulations and that is appropriate. Almost all of them have an exception that data from their vital statistics, be it drivers licenses, birth certificates or death records can be shared with law enforcement.

For us, the most effective way to hit against those databases is at the front end of the process. We can't do that at this time because there is not an easy work around with each of the 50 states, the District of Columbia, the city of New York, the Commonwealth of Puerto Rico to get that other than as a blanket exception that we are involved in a law enforcement function.

We are not interested in law enforcement for anything other than for getting access to records which are otherwise protected from disclosure because we need them to protect the people of the United States more than anything else.

Senator HATCH. Now you, I understand you'd like to require Social Security numbers on all passport applications and I regularly hear from my constituents about identity theft and privacy concerns which often stem from the fraudulent use of Social Security numbers.

So it is hard for me to advocate for another opportunity for potential misuse. But that being said, I would like to hear how requiring Social Security numbers would combat fraud within the passport issuance process, and we know there are so many false Social Security numbers out there.

Ms. SPRAGUE. Although there are many false Social Security numbers out there, the Social Security database is still a source of tremendous, is a tremendous resource for us because it enables us to quickly identify legitimate Americans, people who have longstanding identities and that we can issue their passports expeditiously.

It also enables us to single out into a smaller subset people about whom we have some question, particularly if someone is operating with a false Social Security number.

Right now if someone does not submit a Social Security number, we certainly give that application additional scrutiny. It takes them longer to get through the process. But our hands are tied because this data is so useful to us and we don't have it available to us.

The Social Security Administration is able to confirm back to us and does on an overnight basis the name, the date of birth, the Social Security number, whether or not they are dead, which is obviously an important thing, and their gender. We lose all those things if we don't have the Social Security number up front.

I would agree that we have tremendous concerns about the misuse of Social Security data or privacy data in general and I will be very candid with the committee. A passport application is the mother load for somebody who wants to commit identify theft. It is all there. For that reason, we have been very, very attentive to the need to protect that data.

Not only by ourselves, but by our colleagues in the acceptance facilities. This year we required that they begin to send us all their applications by traceable mail. Our new acceptance facility oversight program, that is one of the primary points of their investigations to make sure that this data is being appropriately protected in the post office.

So your constituents are right to have legitimate concern about this. We do, too. But we don't know how else we can find out who they are before we issue them a passport.

Senator HATCH. Part of the initial passport application process, acceptance agents as the U.S. postal facilities must review various applicants' identity and citizenship documents as well as their submitted photos.

These agents are also required to fill out an observation checklist regarding any concerns about the validity of the applicant's documents.

In your experience, what are the challenges presented by using a U.S. postal acceptance agent in the passport process?

Ms. SPRAGUE. The post office and the clerks of court who support us, 9,400 of them around the country, are good partners. Obviously it is always a risk when you are entrusting such an important duty to someone who doesn't work for you directly.

But I would have to say that almost universally, especially the postal service has tried very hard to meet our expectations. Our new acceptance facility oversight program has gone out. They have been received. In only a little over 6 months we have done over 1,300 inspections. We have been received enthusiastically. People are anxious to learn, they are anxious to do it right.

Having said that, they have their own challenges. Particularly the postal service has many financial strains. As people leave, the new people are not trained immediately, it causes them to have a disruption in being able to provide the service. Some of the people take to this better than other people and that's why we have the new acceptance facility oversight program because we are very anx-

ious to make sure they are doing the best possible job. They don't work for us but they do a very good job of working with us.

Senator HATCH. Thank you. Thank you, Mr. Chairman. I appreciate this opportunity.

Senator CARDIN. Thank you for your questions. Let me come back to the point that you raised about greater access to identification information.

Obviously if someone has used fraudulent documents to get an ID document, that's not going to show up if you have a valid drivers license that was obtained through fraudulent means. But that was not the essence of the concerns at least expressed by GAO and that is that there is fraudulent documents being used to obtain a passport.

Looking at drivers licenses, looking at the birth certificates and also Social Security numbers, that technology exists to be able to verify that information. Admittedly there is just so many types of birth certificates that you point out and we have at least 50 jurisdictions with drivers licenses. And then I think you pointed out, Ms. Sprague, that the postal services do not have that equipment readily available.

My question is why not? Why shouldn't we have the ability to verify the information from a drivers license? We can swipe cards today pretty quickly. Why don't we have that similar type of technology that's implemented in terms of passport verification? The legislation that I mentioned in my opening statement would designate you as, the Consular Affairs as law enforcement, so it does take care of the issue that you raised initially and with Senator Hatch. It also gives you access to a lot of these databanks.

The question is would you have then the capacity to use that information? It seems to me, and I guess I'll start with Mr. Kutz first, isn't that the key here? Doesn't the examiner have to have access to the databanks in order to be able to verify the validity of the documents that are being used?

Mr. KUTZ. Well, the first line of defense is at the post office. Most of these passports the post office is the initial contact. For example, in all of our cases we went to the six post offices and one of the first things they did was took our drivers license, went to a copy machine and made a copy of it and gave the original back.

So right there you are operating with a copy of a counterfeit document. There is no way you could ever determine a copy of a counterfeit. So that is something that is very important why I think you're talking about having the ability to match with other state records.

If you had real time access to match the drivers license number with the state database while that person is sitting right in front of you, that would be critical. That would deter people from coming in in some cases if they knew that someone was going to actually do that or if they had the machine there that was going to actually try to authenticate the drivers license, that might deter people from even coming in in the first place which to me, prevention is the most important part of this.

Senator CARDIN. Well, I agree. I think that's the point. If you make a copy, as you pointed out, make a copy of a fraudulent document, to be able to trace that later is going to be very difficult. You

have got to do it while the person is there. The technology exists. So is this a funding issue?

Ms. SPRAGUE. It is a funding issue, but it is also an access issue. I cannot envision a circumstance in which N-LETS would enable us to have that kind of verification access at point of sale, if you will, for the post office.

However, if they can determine if it is counterfeit or not, which they could do with a very simple device that is available commercially, that would take us a long way. We would get to the counterfeit.

Then when the actual drivers license comes into us, we would be able to hit against N-LETS and at that point we would be able to figure out if it was in fact a validly issued drivers license. So you eliminate the counterfeit right at the beginning and then at the N-LETS point of view as it comes into passport, we're able to identify it.

We really don't want our postal people to try and confront people who are committing a fraud. We would rather that be taken on by skilled professionals. In fact, even at our agencies when we have someone who is committing fraud, we bring in reinforcements from diplomatic security and our guards onsite to handle how that particular apprehension will take place.

Senator CARDIN. So just so I understand before I get Mr. Kutz's response to this, if I might. If the intake person at the postal service determined that the drivers license was fraudulent, what would that person do? Allow the applicant to leave?

Ms. SPRAGUE. They would, and we would, they would provide us a check sheet and then we would take it from there. We do that whenever they suspect fraud and we have had some terrific leads from postal people and the people in the clerks of court who have spotted somebody as being suspicious, provided that back to us and we have successfully traced it back.

Remember, the person really wants to get their passport, so they are going to be somewhere where they can pick that passport up. So we do have a second chance at them if we do want to apprehend them.

In passport fraud, obviously whenever we can, we work with the U.S. Attorney to prosecute, and that is the best outcome. But if we are successful in preventing the issuance of the passport and identifying the person as a fraud, that is too a very good outcome.

So considering the disbursion and the sensitivity of the data and the sensitivity of the states to the exposure of their data, I think that that model would be successful for us.

Senator CARDIN. Mr. Kutz, do you have a view about that? Whether at the intake make a determination on fraudulent on the drivers license, but then the rest being done at a centralized location?

Mr. KUTZ. I would just say this. I think that if you look back at history, this goes back, it is almost set up like a pre-9/11 process in a post-9/11 world. If you were to start this all over again, would you set this up at the post office from the security standpoint? Perhaps not.

But we have what we have at this point, so two layers of defense here. If you had the machines to authenticate the drivers license

and subsequent we have the ability to validate or authenticate with the DMVs, to me those two together would work in this environment.

Senator CARDIN. So how far away are we from having that equipment located at the service centers?

Ms. SPRAGUE. At my counters and agencies, as soon as the procurement is finished we will have it done. It's relatively straightforward for us to move ahead with that.

The post office wants to do it. They have showed us a machine that they'd like that actually does a whole lot more than that, but they simply don't have the capital to invest in that.

Now, they are paid for what they do for us. The passport applicant gives them $25 and they use that to cover their costs. The problem is they need some way to capitalize it up front.

I am not an expert on these things, but in the back of my mind I have thought if we could set up some sort of rotating capital fund which they could reimburse with what they collect from the applicants, because of course everything we do in passports and in fact most of what we do in Consular Affairs is funded, so that we are able to establish what it costs and that and only that is what we charge to the users of it whether it is visa applicants, overseas or Americans who are seeking services.

Senator CARDIN. Would you just make available to our Subcommittee the cost issues here?

Ms. SPRAGUE. I would be happy to do that.

Senator CARDIN. Just so we get a better understanding of that cost.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman. I wonder if maybe we could work with the Committee that Chairman Lieberman and Ranking Member Collins, Homeland Security, to determine whether or not postal service has ever requested any assistance from the Congress, and if so, what has happened to it. If not, why not and then work with you all to see if we could obtain that.

If it's just a matter of funding for a commercially available program and it could be as effective as you say it is and the ramifications of not finding these things are as serious as the GAO has said and we totally agree with that, then this is something we ought to pursue.

Do you agree with GAO's assessment that you have not implemented, not you, but the department has not implemented the previous recommendations of the GAO?

Ms. SPRAGUE. I would say that we have implemented a great many of them, but we haven't solved all our problems. For example, the acceptance facility oversight program is something that was first recommended in 2005. We rolled it out this year. I'm very proud of it.

It took us too long, but it's a good program. Some of our verifications with Social Security we got beat up and we should have been beat up because we didn't have it a year ago.

We have got an excellent relationship with Social Security. They are working with us right now to have real time access. Right now we get 24 hours. They are going to give it to us real time. We are actually at the point of figuring out how much it is going to cost

and making exchanges of business requirements and we are very optimistic that we will get this problem solved.

The only reservation I have when I talk about what we can and cannot do is, neither the Social Security Administration nor the states can give us what they don't have.

For example, the death master file is a wonderful thing and in fact Social Security in our 24-hour turnaround gives us access to all of the death data that they have. But it isn't complete. In the case of two of the applications that we looked at, the people who died were not in the Social Security death master file.

After the fact, we couldn't figure out why their Social Security number came up as an absolute perfect match. We did a little bit of research and our managers figured it out, and it was that they weren't in the death master file. In this particular instance we figured out how we can address it. But the death master file is not perfect. Social Security makes no claims that it is perfect.

Another tool that we use, and in this instance was not as successful as we would have hoped, is the SSN validator is what we call it where you can figure out by using an algorithm when and where the Social Security number was issued. The GAO likes to beat us up with that and they beat us up with that again this time.

Social Security doesn't maintain that. It is sort of a separate entity and we have to maintain it as separate from what we get back from Social Security. But it doesn't matter because Social Security is going to abandon that algorithm for very good reasons, but it is going to leave us in a hole in terms of any newly issued Social Security numbers. It is not only children, it is also immigrants, remember. We won't be able to tell when it was issued because it won't be in the algorithm.

Social Security doesn't maintain their data in that way that they can share it with us. So we've got a big problem that we can figure out a solution to. We are working very closely with Social Security, we hope we can find a solution, but we are anxious about that.

Senator KYL. Mr. Kutz, do you have a response to what Ms. Sprague has just said?

Mr. KUTZ. Yes. I would say in one area that they did improve, we used the first four we got last time, one of them was a child, a legitimate SSN we got with counterfeit documents several years ago. They didn't catch that last time.

This time we used another child we have that had a legitimate Social Security number and they did catch it, so that was an improvement in that Social Security matching. So that's why I think they're making progress in that issue of validation of deceased or regular Social Security numbers.

It is not easy, but I think the real time, as real time as you can get on that access, that is an important element of this.

Senator KYL. It just strikes me that you are now identifying some additional problems that you're going to have to contend with and you've told us that you are working with Social Security to try to resolve this last problem that you mentioned.

I think it might be helpful for us if you could give us a brief report, memorandum, that tells us all of the things that you think are necessary for you to do your job the very best in issuing passports to people only who are entitled to them and then to the ex-

tent that some of those things require the executive branch to get people together, perhaps it can do that. To the extent legislation might be necessary, we can address that.

To the extent that GAO has identified things that your department can do better, address that in the memo as well. If you think yes, they're right, you can do better, fine. If you think there is some reason why you can't would you put that in the memo for us?

Ms. SPRAGUE. I would be happy to do that.

Senator KYL. I know I'm asking you to do something here that the Chairman hasn't requested, but I think probably all of us could benefit by such a report.

Ms. SPRAGUE. I would be happy to do that.

Senator KYL. Thank you.

Senator CARDIN. Senator Hatch.

Senator HATCH. I'm happy with what I heard.

Senator CARDIN. Let me just underscore the point that Senator Kyl made on information. As I try to analyze, and the question I asked at the end of the first round is what should our expectations be and it was a serious question.

I understand that this is a process that we can do a lot better and we need to do a lot better, but what is reasonable for us to expect here as far as performance is concerned? I think there have been many worthwhile suggestions that have been made that don't seem to be overly burdensome from the point of view of the timeliness of the passport applications and the cost for processing it.

As you pointed out, Ms. Sprague, this is a fee generated reimbursement structure, so therefore the people of this Nation are entitled to get the services for the fees that they are paying.

What it seems to me is that there are different layers of protection here. Each one helps us. On the drivers licenses, it seems to me that the technology is there to be able to determine a fraudulent document through a relatively efficient process at the application stage that should be implemented. It also seems to me that access to the databanks will also help you detect fraudulent applications. Now, that may need to be done at a centralized location, but it is a second layer.

On the Social Security numbers, the records kept on those who are deceased is one method, but as you point out, it's not foolproof. So therefore you look at the Social Security number which gives you some indication, but that's not foolproof. So it seems to me you have to combine all these issues in the most efficient way and by doing this, the net will be tight enough that you're going to increase dramatically the denial of those fraudulent applications.

Then when we get to the birth certificates, I couldn't agree with you more that this is a task that we really need to work with local governments, and try to figure out a more effective way of verification of birth certificates that are fraudulent. Because again, that information is available, it is just not in a very useful way and it seems to me we need to make greater progress there.

As I have been informed, there are other identification documents that we haven't really gotten to today, but it seems to me that those are less problematic than some of these other forms that we're talking about.

I would ask that you get us the information that we requested. We do have legislation that we're looking at. I really do know that the people are working extremely hard to get this right and we know it's not an easy task. Congress doesn't always show its appreciation in the right way when we have our budgets that we can take up, but we need to do better.

I think GAO has pointed out that we can do better. It is not that we should be doing better. So I think all of us are going to have to sort of work together and figure out a way to reduce the error rates and to make the passport, which is considered the gold standard, really the gold standard, minimizing any fraudulent applications being successful.

Mr. Kutz, I thank you very much for the work that your agency does. I think it is done in a very up front way with the Congress. Ms. Sprague, I thank you for the seriousness in which you have always treated the information, and your presentation and cooperation with this committee. And we look forward to working with you for better results.

Senator KYL. May I just add one more thing? If there is another 9/11 and people obtain fraudulent documents as they did in that case like drivers licenses, for example, and people ask why it happened, I think every one of us has to be able to say we did everything we could to prevent it from happening.

I think maybe we take it too lightly because it has been a long time now, but we tend to forget what happened back then and why it was that people could operate freely in this country because they had obtained fraudulent documents.

So I think some degree of urgency is required here as well.

Ms. SPRAGUE. Thank you, Senator.

Senator CARDIN. The hearing record will remain open for 1 week for additional statements and questions for the record. If there are additional questions that are propounded, I would ask the witnesses to respond in a timely manner to any of those written questions. With that, the Subcommittee will stand adjourned. Thank you.

[Whereupon, the hearing was adjourned.]

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

QUESTIONS AND ANSWERS

United States Government Accountability Office
Washington, DC 20548

August 27, 2010

The Honorable Benjamin L. Cardin
Chairman
Subcommittee on Terrorism and Homeland Security
Committee on the Judiciary
United States Senate

Subject: *Posthearing Responses to July 29, 2010, Hearing on the Passport Issuance Process: Closing the Door to Fraud, Part II*

Dear Mr. Chairman:

On July 29, 2010, we testified before your subcommittee at a hearing entitled *The Passport Issuance Process: Closing the Door to Fraud, Part II.* This letter responds to your request that GAO respond to a number of post-hearing questions. The questions and our answers are provided in the enclosure. The responses are based on work associated with previously issued GAO products, which were conducted in accordance with generally accepted government auditing standards and investigative standards from the Council of the Inspectors General on Integrity and Efficiency. We did not obtain comments from the Department of State.

If you have any further questions or would like to discuss these responses, please call me on (202) 512-6722.

Sincerely yours,

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

Enclosure-1

Responses to Questions for the Record
Subcommittee on Terrorism and Homeland Security,
Committee on the Judiciary
The Passport Issuance Process: Closing the Door to Fraud, Part II
July 29, 2010

1. ***The Passport Identity Verification Act.***

   a. **Does GAO support the Passport Identity Verification Act (PIVA), S.3666?**

   b. **Does the GAO agree that if PIVA is enacted, it will greatly improve the State Department's (State) ability to verify the identity of a passport applicant and detect passport fraud?**

Answer:

a. We support the Passport Identity Verification Act.

b. We agree that if PIVA is properly implemented and consistently applied, it should enhance State's ability to verify the identity of passport applicants. According to State, limited access to relevant federal and state level agencies' records, because privacy concerns and the fact that State is not a law enforcement agency, has been a long-standing vulnerability in the passport issuance process. For example, State officials told us that limited access to such records enabled GAO to obtain the four genuine passports we reported in our March 2009 report. According to State, passport specialists did not wait for the results of a required Social Security Administration (SSA) database check before approving our fraudulent applications; further, in all four of our tests State failed to identify the fraudulent birth certificates we used. We have also reported that State has difficulty verifying driver's license information presented by passport applicants. Improving State's access to citizenship and identity information contained in databases maintained by relevant federal, state, local governments, private entities, or other organizations, to verify the authenticity of passport applicants' information, as called for in PIVA, should strengthen the State Department's ability detect fraud during the passport issuance process.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00027 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.002

2. ***GAO's 2009 Recommendations.*** **In its May 2009 testimony, GAO made a number of recommendations with respect to changes the State Department needed to make to the passport issuance process. Please list those recommendations and the degree to which the State Department has implemented them.**

Answer:

In our May 2009 testimony, we suggested that the Secretary of State take the following corrective actions to address vulnerabilities in the passport issuance process:

1. **Improve the training and resources available to passport-acceptance-facility employees for detecting passport fraud, especially related to detecting counterfeit documents.**

   In Progress. State told us that it has established an Acceptance Facility Oversight Program (AFOP). The goal of the program is to develop an integrated database that will provide enhanced statistics to evaluate, track, and monitor acceptance facility performance. To do this, program analysts monitor, inspect, and report acceptance facility adherence to Passport Services' policies, practices, and procedures. In addition, the program includes enhanced Web-based and classroom training for non-State Department acceptance agents at the 9,400 designated facilities where the general public may apply for a U.S. passport. While the program presents some worthy goals, there is no indication that it will provide the Postal Service with the necessary training and resources to detect counterfeit documents, such as fraudulent drivers' licenses, submitted by passports applicants. Our most recent test shows that passport-acceptance-facility employees continue to have problems identifying counterfeit documents.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00028 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.003

2. **For applications containing an SSN, establish a process whereby passport specialists are unable to issue a passport prior to receiving and reviewing the results of SSN and Death Master File checks, except under specific or extenuating circumstances and after supervisory review.**

   No Progress. Based on the results of our most recent tests of State's passport issuance process, State has not made progress on this recommendation. Similar to our first series of tests, five of the bogus applications that we submitted in our most recent tests were based on information and SSNs we had previously obtained from the SSA for the purpose of conducting undercover investigations. State immediately detected that two of the applications contained SSNs that did not match SSA data but failed to crosscheck the SSNs in the three remaining applications before they were approved for passport issuance. If State had taken sufficient action to implement this recommendation, it would have detected the erroneous SSNs in the remaining three passport applications before they were approved for passport issuance.

3. **Explore commercial options for performing real-time checks of the validity of SSNs and other information included in applications.**

   No Progress. Our most recent testing shows that State still does not conduct real time checks of the validity of SSNs and other information included in applications. If State had implemented this recommendation, it would have likely detected all seven of our passport applications as fraudulent as they all contained recently issued SSNs, counterfeit birth certificates, and counterfeit or fraudulently obtained drivers' licenses. Anecdotally, State showed some ability to conduct searches of SSNs and other identity information using commercial software such as LexisNexis, which it used to conduct research on our multiple addresses, SSNs, and other identifying information. However, this research was generally conducted only after State discovered our tests and realized that it had issued passports based on erroneous application information.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00029 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.004

4. **Conduct "red team" (covert) tests similar to our own and use the results of these tests to improve the performance of passport acceptance agents and passport specialists.**

   Implemented. According to State, this recommendation has been implemented and will remain a part of its ongoing efforts to strengthen the passport issuance process. In September 2009, State launched "red team" testing through the Passport Integrity Testing and Training Program (PITT). As of April 2010, three fraudulent passport applications were submitted by Diplomatic Security personnel with accompanying counterfeit birth certificates; of these, two applications were submitted through passport acceptance facilities and one was submitted at a passport agency public counter. State indicated that in each case, the fraudulent passport applications were detected by Passport Services.

5. **Work with state-level officials to develop a strategy to gain access to the necessary state databases and incorporate reviews of these data into the adjudication process.**

   In Progress. State has increased data and information-sharing with relevant federal, state, local, and private organizations that possess information. According to State, it has deployed the National Law Enforcement Telecommunications System Information Sharing Network, Inc. (NLETS) system, which gives the State Department access to drivers' license data for 49 States (South Dakota has declined to participate), Puerto Rico, and the District of Columbia. To verify questionable birth certificates, State's Fraud Prevention Managers employ the Electronic Verification of Vital Events (EVVE) system available through the National Association for Public Health Statistics and Information Systems (NAPHSIS). We do not know the effectiveness of these systems. Nor do we know the extent to which they are utilized by State during the passport issuance process. Our recent tests show that State does not consistently conduct data verification at the front-end of the passport application process because all of the applications for which passports were issued contained counterfeit or fraudulently obtained birth certificates and drivers' licenses.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00030 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.005

Questions for the Record Submitted to
Deputy Assistant Secretary Brenda S. Sprague by
Senator Benjamin Cardin (#1)
Senate Committee on the Judiciary
July 29, 2010

Question:

GAO's 2009 Recommendations. In its May 2009 testimony, GAO made a number of recommendations with respect to changes the State Department needed to make to the passport issuance process. Please list those recommendations and the degree to which the State Department has implemented them.

Answer:

Below is a list of the recommendations made by the GAO and the status of the Department's efforts to implement them:

1. **Improve the training and resources available to passport acceptance facility employees for detecting passport fraud, especially related to detecting counterfeit documents.**

The Department implemented the Acceptance Facility Oversight Program (AFOP) in 2009 to provide oversight and guidance to the more than 9,400 non-Department acceptance facilities nationwide (primarily U.S. post offices and county clerk's offices). The program is intended to improve the accountability, integrity, and performance of these facilities. AFOP staff monitor acceptance facilities' adherence to Department policies; recommend corrective actions for deficiencies; identify and recommend training needs; develop standardized policies and procedures, and recommend technological improvements to the acceptance process.

Since December 2009, the AFOP staff has completed more than 1,800 acceptance facility site assessments. Reports of site assessments are shared with the Customer Service Manager at each agency and center in order to track deficiencies and ensure targeted training is provided to address specific areas in need of improvement.

64705.006

The Department is developing the Integrated Acceptance Facility Oversight Database (IAFOD) which will collect information on acceptance facilities performance and training.

In addition, over the past year, the Department has undertaken the following improvements in training and resources available to Passport Acceptance Agents:

- Updated and enhanced the web-based training course for Passport Acceptance Agents;
- Revised the Passport Agents Reference Guide (PARG) to add policies and procedures designed to strengthen the acceptance process and provide additional training to acceptance facilities;
- Issued new annual certification requirements for acceptance facilities;
- Revised the Passport Agent Observation Checklist, which is used by Acceptance Agents to alert the Department of suspicious behavior on the part of the applicant or irregularities on the passport application; and
- Provided all acceptance facilities with the "I.D. Checking Guide," which provides samples of driver's licenses and identification cards issued in the United States and Canada.

2. **For applications containing an SSN, establish a process whereby passport specialists are not able to issue a passport prior to receiving and reviewing the results of SSN and *Death Master File* checks, except under specific or extenuating circumstances and after supervisory review.**

The Department enhanced the procedures of the issuance process to ensure that passport applications do not proceed to issuance without checks against the SSN and death files databases of the Social Security Administration (SSA). SSNs are now automatically checked against the SSN database at the front end of the issuance process prior to applications reaching the adjudication stage. The results of this database check

are displayed in the Travel Document Issuance System (TDIS) used by Passport Specialists to process passport applications.

While there is no systems modification to prevent a Passport Specialist from approving applications without reviewing SSA results, the Department's Standard Operating Procedures require this review. The Standard Operating Procedures were distributed to all Passport Specialists by memo in January of this year. They were updated to further clarify actions taken when reviewing SSN results and redistributed in July. SSN checks are done as a batch process and take 24 hours from the time the data is submitted.

Utilizing SSA's Death Master File database, the Department implemented a system that instantly alerts if a SSN is associated with a deceased person. TDIS will not allow a Passport Specialist to approve an application that has a SSA Death Record. If the application were determined to be issuable, approval must be done at the manager level. The Standard Operating Procedure for handling these types of alerts was created in March, 2009, and distributed to all Passport Specialists.

If the customer's travel plans require issuance of the passport in less than 24 hours, the applicant's information including the SSN is checked in Consolidated Lead Evaluation and Reporting (CLEAR), a commercial database that verifies the "social footprint" for a given identity. The Passport Specialist compares the data from the CLEAR database to the information provided by the applicant. If a comparison of the information meets established criteria, the application is approved.

Working with SSA, the Department is exploring options to have SSA provide real-time verification for all SSNs. The Department re-submitted a formal request to SSA in June 2010.

SSA has recently announced a change in the SSN numbering system. This change lends added urgency to the need to obtain the SSA real time verification: the

algorithm currently used to determine issuance date and location for SSNs issued might no longer be applicable to numbers issued after implementation. SSA's tentative implementation for SSN randomization is summer 2011. Because of this change, the Department also requested that SSA consider adding the state/year of issuance to our real-time request.

However, SSA indicates that they have no current matching routine to link state/year of issuance with each SSN holder. The Department is coordinating with the SSA to determine if the legal authority exists to share state/year of issuance information for SSNs. A legislative change may be needed in order for SSA to provide the Department with information we require.

3. **Explore commercial options for performing real-time checks of the validity of SSNs and other information included in applications.**

CA is using CLEAR to perform real-time checks on the validity of information submitted by applicants, including SSNs, for all customers whose travel plans require issuance of the passport in less than 24 hours and, in other cases, on an as-needed basis. This method of verifying data is not automated and is extremely time consuming. Access to CLEAR is currently limited to select individuals at each passport agency to conduct these checks. We are currently assessing the value and feasibility of expanding this access to all passport specialists

CA is also exploring enhancing the passport adjudication process by adding a commercial identification verification tool, such as LexisNexis "Identity Solutions" or CLEAR, as a primary automated check in our Travel Document Issuance System (TDIS). Under such a program, each application would automatically be checked against a commercial database to verify the "social footprint" of the given identity prior to the adjudication of the application. We are preparing a test using results from LexisNexis "Identity Solutions" against data from a number of passport applications.

While we explore the use of these databases, we are also mindful of maintaining the privacy rights of applicants and ensuring the protection of an applicant's personally identifiable information (PII).

4. Conduct "red team" (covert) tests similar to our own and use the results of these tests to improve the performance of passport acceptance agents and passport specialists.

Passport Services collaborated with CA's Office of Fraud Prevention Programs and the Bureau of Diplomatic Security to develop the Procedural Integrity Testing and Training (PITT) Program or "Red Teams," to test the effectiveness of our adjudication and anti-fraud efforts, identify and mitigate vulnerabilities, and improve the quality of the passport issuance process. Since the pilot began in late 2009, eight testing scenarios were completed and six were successfully detected. The Department is moving to make the PITT program a permanent part of its fraud prevention effort.

5. Work with state-level officials to develop a strategy to gain access to the necessary state databases and incorporate reviews of these data into the adjudication process.

CA, via sponsorship from the Department's Diplomatic Security Service (DS), has gained "non-law enforcement" access to the National Law Enforcement Telecommunications System (NLETS), an organization that is owned and governed by the states to verify driver's license issuance with states' Departments of Motor Vehicles. While all 50 states plus the District of Columbia and Puerto Rico participate in the NLETS system, CA receives responses from only 43 of the 50 states, the District, and Puerto Rico. Because CA is not a law enforcement authority, the responses received only verify that a driver's license was issued in the name queried; no other information, such as bio-data, which would be extremely valuable to us, is provided.

In an effort to gain access to other federal and state government databases, we believe it would be very helpful to get legislation that, for the sole purpose of data sharing, would facilitate Bureau of Consular Affairs access to certain law enforcement data bases that currently are accessible only to law enforcement entities. For example, such legislation might enable us to gain direct access to states' Department of Motor Vehicles files that contain photographs of license holders, which would greatly enhance our ability to verify the identity of passport applicants and detect fraudulent applications. The Department worked closely with the Subcommittee and, along with Senators Feinstein and Lieberman, you introduced a bill that would serve this purpose on July 29, 2010. If passed, CA would acquire law enforcement designation for data sharing purposes only.

(#2A)

Question:

Social Security Numbers. Ms. Sprague, you indicated in your testimony that the State Department lacks the authority to require Social Security Numbers (SSNs) from passport applicants. However, Title 26, United States Code, Section 6039E, specifically states that "[n]otwithstanding any other provision of law, any individual who . . . applies for a United States passport (or a renewal thereof), . . . shall include with any such application a statement which includes the information described in subsection (b)." Subsection (b) then states that the "[i]nformation required under subsection (a) shall include -- (1) the taxpayer's TIN (if any), (2) in the case of a passport applicant, any foreign country in which such individual is residing, (3) in the case of an individual seeking permanent residence, information with respect to whether such individual is required to file a return of the tax imposed by chapter 1 for such individual's most recent 3 taxable years, and (4) such other information as the Secretary may prescribe." Indeed, on page 3 of the passport application the State Department provides to applicants, Form DS-11, it states that "Section 6039E of the Internal Revenue Code (26 U.S.C. 6039E) requires you to provide your Social Security Number (SSN), if you have one, when you apply for a U.S. passport or renewal of a U.S. passport."

a) As a result, why do you believe additional legislation is necessary?

Answer:

The State Department seeks legislation requiring that passport applicants issued a Social Security Number (SSN) provide their SSN on the application and the authority for the Department to deny passports to those applicants who fail to do so.

Title 26, United States Code, Section 6039E does not specifically authorize the Department to require a SSN on the application nor does it authorize the Department to deny a passport for failure to do so. We have recognized that Section 6039E requires applicants to provide certain information to the IRS and provides for the IRS to impose a monetary penalty for failure to do so. However, we have never interpreted that IRS statute to authorize the Department to compel disclosure of the SSN and to then deny a passport to an applicant for failure to comply.

We therefore prefer that legislation specifically requiring disclosure of the SSN on the passport application with authority for the Department to deny issuance upon refusal be passed by Congress.

(#2B)

Question:

If legislation is enacted which provides additional authority to the Secretary of State to require SSNs of passport applicants, how would that additional authority improve the State Department's ability to verify the identity of a passport applicant and detect passport fraud?

Answer:

Each year, nearly a quarter of a million applicants fail to provide their SSN. The SSN assists the Department with verifying an applicant's identifying information and

detecting fraudulent applications early on in the adjudication process, as well as combating identity theft. Requiring applicants to provide their SSN will permit the Department's front-end system of processing to more efficiently and effectively review the information and examine the validity of the SSN automatically, even before the adjudicator begins review. The Department can use the SSN when utilizing other identity verification tools, including commercial databases such as LexisNexis or the Consolidated Lead Evaluation and Reporting (CLEAR).

The requirement will also help discourage persons who may be attempting to use counterfeit identity document in instances where an SSN has not been acquired in the false identity. Additionally, the SSN requirement will help the Department to further combat the use of improper SSNs by enabling the Department to associate more applications with valid SSNs.

(#3A)

Question:

Technology. Ms. Sprague, you indicated in your testimony that the technology exists for passport acceptance facilities to determine whether a drivers' license is counterfeit at the time the passport application is submitted. You also noted that while passport applications are fee generating, the initial capitalization for this technology poses a challenge for non-State Department facilities.

If all passport acceptance facilities had technology to verify the authenticity of a driver's license or birth certificate, what impact would that have on the ability to detect passport fraud?

Answer:

Card readers at passport acceptance facilities would aid in detecting passport fraud by enabling Acceptance Agents to determine at the time of application acceptance

that a document is counterfeit. However, an Acceptance Agent has no authority to approve or deny an application; he or she is solely required to forward the passport application and accompanying documents to the Department of State for adjudication. If a card reader machine detected a fraudulent driver's license, the Acceptance Agent would be expected to annotate the false nature of the document on the application, to assist the Passport Specialist at an agency or center in determining whether the application is fraudulent.

Providing document verification systems would improve the capability of Acceptance Agents to detect counterfeit documents and improve our ability to detect fraud. However, these systems do not address another prevalent and complex form of passport fraud: the use of legitimate documents that were attained illegitimately (i.e., impostor fraud).

Document authentication systems are helpful to our overall goal of reducing passport fraud. However, access to the detailed information in Federal and state databases, currently available only to law enforcement authorities, is the tool that would have the most significant impact on reducing passport fraud.

(#3B)

Question:

What are the initial procurement costs for the installation of this technology at non-State Department acceptance facilities around the country?

Answer:

The initial procurement cost to provide card reader technology at non-State Department acceptance facilities will be approximately $44 million. This estimate includes the cost of one card reader machine per facility, first year software support costs, a computer, monitor and printer for each facility, and for data updates to the software via CDs.

(#3C)

Question:

Please identify the states that do not presently issue drivers' licenses that can be scanned or "read" to be counterfeit.

Answer:

At this time, the State Department believes that all states issue driver's licenses that can be scanned to verify authenticity.

(#4)

Question:

The U.S. Postal Service is facing a budget deficit. What effect, if any, could this have on U.S. postal employees being able to verify the identity of passport applicants and detect passport fraud?

Answer:

The Department recognizes that financial difficulties and cutbacks might result in some postal acceptance facilities being unable to continue to participate in the Passport

Application Acceptance Program. However, U.S. Postal Service officials continue to pledge their support and commitment to the Program.

The Passport Acceptance Agent's primary role is to facilitate "accepting" passport applications from the public. In this role, "acceptance" as it is done by the Acceptance Agent is not an approval of the application or an adjudication of the applicant's entitlement to the passport. Acceptance Agents are not trained adjudicators and do not perform the wider range of adjudication functions that include greater anti-fraud responsibilities.

Should passport fraud be suspected, Acceptance Agents are instructed to complete an "Observation Checklist" to be submitted with the passport application package directly to the Fraud Prevention Manager's Office at their regional passport agency.

(#5A)

Question:

Does the State Department maintain a centralized fraud library for identity documents which can be accessed by all passport examiners?

Answer:

The Bureau of Consular Affairs' Office of Fraud Prevention Programs maintains an online fraud library which can be accessed by all passport examiners. The library contains a wealth of information regarding birth records and identity documents, as well as training materials regarding those documents including exemplars of both fraudulent and genuine specimens. However, because there are thousands of variations in format

and content of birth certificates (14,000 versions are in circulation) and identity documents issued by federal, state, and local governments, compiling a complete collection of documents remains a challenge. CA continues to update the library with exemplar documents as they are obtained.

The birth certificate is the most common document used to establish U.S. citizenship. It would greatly assist the Department in the discovery of fraudulent or counterfeit birth records if the processes for issuing birth certificates among the various states, counties and cities were standardized, and that available technologies were used to ensure their physical integrity. We seek Congressional support focused on encouraging the standardization of birth documents and legislation that sets minimum standards for official birth certificates and requires each State to issue one official birth certificate.

(#5B)

Question:

What steps does the State Department take to routinely update its knowledge of fraudulent identity documents?

Answer:

The network of Fraud Prevention Managers (FPMs) across the nation routinely share and exchange information regarding known and emerging fraud trends as they pertain to fraudulent identity and citizenship documents. The State Department routinely enhances and updates its knowledge of fraudulent identity and citizenship documents by building and maintaining relationships with state bureaus of vital statistics, licensing bureaus, and other national entities that document vital events.

Domestic FPMs must complete training which includes an annual fraud awareness training seminar as well as other training events that cover program management, fraudulent identity and citizenship document detection, and fraud prevention. They also regularly participate in seminars pertaining to current and emerging fraud trends specific to their region of the United States. Additionally, FPMs deliver training to passport specialists twice each month to ensure that passport specialists' knowledge of current identity and citizenship documents is as up-to-date and accurate as possible. Finally, the Department maintains a National Fraud Library that contains a wealth of information pertaining to fraudulent identity and citizenship documents and passport fraud.

(#6A)

Question:

What training does the State Department provide to passport acceptance facility employees to identify fraudulent identity documents?

Answer:

The Department's Fraud Prevention Managers provide in-person training to Passport Acceptance Agents. This training focuses on suspicious behavior and inconsistencies on applications that might indicate an impostor.

Passport Acceptance Agents are required to verify that the photographs with the application match the person standing before them. The Department provides all

Acceptance Agents with a copy of the "I.D. Checking Guide." This guide gives samples and descriptions of identity documents issued by all states and territories, as well as Canada. Acceptance Agents are urged to refer to this guide when they are unfamiliar with an identification document, especially in circumstances where out-of-state identification is presented. Acceptance Agents attach photocopies (front and back) of the identification and alert the passport agency if the identification is suspicious. In cases of irregularity, Acceptance Agents complete an "Observation List" and submit that document together with the passport application package directly to the Fraud Prevention Manager's Office at their regional passport agency.

(#6B)

Question:

Does any of that training include input from representatives from each of the 50 states and territories in regard to how to identify legitimate drivers' licenses and birth certificates from those states and territories?

Answer:

No. Passport Acceptance Agents currently do not receive training from representatives of the 50 states and territories. Acceptance Agents do receive and are urged to use the "I.D. Checking Guide," which includes samples and descriptions of driver's licenses and other identity documents issued by all states and territories.

(#6C)

Question:

Are there ongoing training requirements with respect to the identification of fraudulent breeder and identity documents for employees at passport acceptance facilities?

Answer:

The ability to readily identify fraudulent breeder and identity documents such as driver's licenses and birth certificates is a very specialized skill that requires extensive training which is beyond the scope of what we can reasonably expect of the Acceptance Agent and the acceptance facility that conducts other primary business in addition to the acceptance of passport applications. However, in the general training for our Acceptance Agents, the Department focuses on proper procedures for accepting passport applications as well as suspicious behavior on the part of the applicant and irregularities on the application that may indicate fraud.

The Department provides all Acceptance Agents with a copy of the "I.D. Checking Guide." This guide gives samples and descriptions of identity documents issued by all states and territories, as well as by Canada. Acceptance Agents are urged to refer to this guide when they are not familiar with an identification document, especially in circumstances where out-of-state identification is presented.

As Deputy Assistant Secretary Sprague and GAO Director Kutz agreed, the use of document verification readers at non-Department passport application acceptance facilities would enhance the Department's ability to better detect and deter passport fraud by identifying counterfeit identification documents at the point of application acceptance.

About ninety percent of first-time passport applicants submit their applications through a non-Department acceptance facility.

(#7A)

Question:

Does the State Department support the Passport Identity Verification Act (PIVA), S. 3666?

Answer:

The Administration is continuing to review PIVA (S. 3666) and looks forward to working with the Committee on this legislation in the new Congress.

(#7B)

Question:

Does the State Department agree that if PIVA is enacted, it will greatly improve the State Department's ability to verify the identity of a passport applicant and detect passport fraud?

Answer:

The Administration is continuing to review PIVA, (S. 3666) and looks forward to working with the Committee on this legislation in the new Congress.

(#8A)

Question:

On June 3, 2010, more than two months ago, GAO informed the State Department that it intended to conduct a forensic audit of passports issued by the State Department during two fiscal years, pursuant to Title 31, United States Code, Section 716. That information was sought at my request as Chairman of the Terrorism and Homeland Security Subcommittee of the Senate Judiciary Committee. Senators Feinstein, Kyl, Lieberman

and Collins have now joined my request. The Subcommittee had originally sought three years of data, but then agreed that two years of data would be sufficient. Ms. Sprague then wrote a letter to GAO on June 24, 2010, and stated that the State Department would "share appropriate information with GAO when it has a clear mandate to obtain it." To date, despite GAO's efforts to assure the State Department that it will protect the confidentiality of this data, the State Department still has not provided any data to GAO.

Does the State Department believe there is a legal impediment to complying with GAO's and this Subcommittee's request?

Answer:

The State Department does not believe there is a legal impediment to complying with GAO's and this Subcommittee's request. However, there are certain limitations that are necessary to protect the various equities involved. Over the last several weeks the Department raised and discussed these issues with GAO and is working towards a satisfactory solution for all involved. The Department is available to discuss these issues in greater detail in a closed session with the Subcommittee.

(#8B)

Question:

When will the State Department provide the requested data to GAO?

Answer:

The Department is reviewing GAO's request which triggered privacy and other security concerns. The Department will propose a response which will provide responsive data in a way that both meets GAO's needs and protects the equities involved.

NOTE: Since the date of the hearing, the Department provided GAO with a letter and a Data and Security Agreement to be executed by the parties which recognizes and

protects the various equities involved with the request. Once GAO executes the Agreement, the Department will move forward with providing the data to GAO.

SUBMISSIONS FOR THE RECORD

STATEMENT OF

ROBERT ARNOLD

NATIONAL VICE PRESIDENT
OF
THE NATIONAL FEDERATION OF FEDERAL EMPLOYEES (NFFE)

FOR THE RECORD

BEFORE

THE SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

REGARDING

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

ON

JULY 29, 2010

On behalf of the National Federation of Federal Employees (NFFE) and the 110,000 federal employees our union represents throughout the United States and abroad, including 1,400 employees at the Department of State's (DOS) Passport Services (PPT) division, I thank you for the opportunity to share our views on how to combat passport fraud.

Passport Services once again finds itself in the spotlight, explaining its performance on a second GAO fraud detection test. It is important to admit up front that the issuances of the GAO cases were caused partly by passport specialist errors. Some details were clearly overlooked when the applications and documents were reviewed. Of the seven GAO applications – all handled by passport specialists - two were caught, four were approved in error, and one was denied by the specialist, but overruled and approved by a supervisor.

Unlike the results of the GAO's 2009 test, the decisions to issue passports this time were reached in four different offices, and by specialists of varying experience. The specialists approved the applications during a year when they had received more extensive training on fraud, as well as more training on adjudication, and did so under lower production standards. Yet we believe that the same decisions to issue the GAO applications could easily have been made by any passport specialist under the agency's current system.

In the Union's written testimony to this Subcommittee in 2009, we made the following assessment of problem areas:

1. **Too little focus on fraud prevention in the passport specialists' performance elements, awards and overall work culture.**

   This observation is still applicable today, although there have been some improvements at PPT. For the first time, performance in fraud detection will now account for at least 10% of the agency's awards. The Union had requested a larger percentage of the awards money be devoted to fraud recognition[1], but was met with resistance.

   Also, since our testimony in 2009, Passport Headquarters lowered the hourly production requirements, which was a welcome departure from the strong emphasis on quantity

[1] The 10% figure does not cost the taxpayers more; it just reapportions where the awards budget is allocated.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.025

previously displayed by the agency. However, we also experienced revised passport specialist critical elements in 2010 to make production numbers more prominent.

2. Insufficient fraud detection training, information, and tools.

The department has done a significantly better job on fraud training. However, there is still room for improvement on the number and type of document samples available for reference, and the national intranet website could be more efficient[2]. Also, there is a trend toward stressing fraud detection in training provided by the fraud office, while emphasizing production in adjudication team training. This discrepancy causes specialists to receive mixed messages. And even the perfect training curriculum won't suffice if specialists do not have adequate time to examine the documents. Just this month, the agency had all passport specialists take a training course on detecting fraudulent documents. Headquarters required all specialists to certify under signature that they have absorbed the material, yet only provided one hour for employees read the 52 pages (which ended with a quiz). Instances of employees being given too little time to possibly know the material is an ongoing issue.

Passport fraud managers can only train employees on their areas of expertise. Since much of the passport specialist's job is to evaluate state-issued documents, additional training from state DMV and vital record officials on security features would prove beneficial.

Three of the fraudulent GAO cases were issued at large processing centers that handle work from all corners of the nation. Considering the thousand-plus types of state, county and city birth certificates, there are too many formats for any one person to memorize. Becoming familiar with the document formats from one region of the country is a much more obtainable goal. Fraud detection would improve if specialists were able to apply their expertise of their own region. Transferring applications is unavoidable for workload balance reasons, but currently occurs more than necessary.

3. Insufficient permanent fraud prevention staffing.

The department has made large strides in this area, hiring a number of new fraud program managers, and enlarging the national Fraud Prevention Program. Because of these improvements, this suggestion no longer seems to apply.

[2] For example, searches of agency online resources frequently bring up results listing dozens of fraud reports, with no indication of which report pertains to the search.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.026

4. Organization and interagency information sharing roadblocks.

The information provided to PPT by the Social Security Administration represents a significant step forward in fraud detection capabilities. This collaboration proved that data can be shared between agencies in a manner that still respects the privacy of personal information. The exchange of information with other agencies needs to be a high priority. Citizenship and Immigration Services is the next logical candidate for information sharing, both from a customer service and fraud prevention standpoint, but efforts at data-sharing should not stop there.

Technology gaffes played a role in the mistaken issuances to the GAO in 2010, just as in 2009. Even so, the information at the specialist's fingertips is improved from previous years. Work still needs to be done to ensure the information is consistently accurate.

Some of the data issues are beyond the Department of State's control, but not all of them. In disputing errors charged against an employee[3] in October of 2009, the Union pointed out that Passport Services' online social security information was incomplete and could be easily fixed. The Union made the same request for the database to be updated in March of 2010. This incomplete SSN database resulted in 10 times as many "alert" icons popping up during adjudication. They occurred so often that they ceased to register as a meaningful alert to adjudicators. This factor played a role in several of the cases of passports being issued in error. In the weeks since the last GAO test, the agency has addressed this problem.

5. Insufficient oversight and restrictions on the passport acceptance function.

Passport Services expanded its oversight of passport acceptance facilities, creating a new division which audits the post offices and county courthouses that accept applications. This program will eliminate loopholes in the facilities' security procedures. It will hopefully improve the overall acceptability of the applications from the facilities, as well as improve their detection of fraud.

In addition to the new acceptance facility oversight positions, there are now four new nationwide regional directors, each with several research analysts. A new section was formed to consider internal control requirements. The agency is in the process of creating a new adjudication section that will examine rules and procedures. All of these new

[3] The employee was ultimately fired.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.027

management positions perform worthy tasks. But it is critical that the benefit of these additional agency resources be felt at the adjudication level, and thorough passport adjudication made more attainable.

6. **Failing to adequately seek out and consider employee input, through their union, when making changes to systems, applications, processes, and procedures.**

The agency welcomed union/employee involvement in layout of the new passport application (which pertains to fraud detection), but the invitation was not extended to any other facet of agency operations. Although the Union was invited to speak to several committees, the suggestions made in those one-time meetings were rejected or forgotten by the time the committees issued their recommendations. NFFE Local 1998 believes that providing more of a voice for the employees would have produced a better agency performance on the GAO's test.

In a 2006 nationwide survey, Passport employees named passport integrity the highest priority topic for this Union. NFFE Local 1998 officers have provided numerous unsolicited additions to agency fraud libraries over the years. And despite standing nothing to gain, passport employees lobbied in support of 2008's H.R. 5752, designed to stop passport security features from being produced in overseas in nations, which causes numerous security concerns.[4] Passport employees have consistently shown a commitment to the security of their product.

The agency has held passport specialists more accountable since the results of the first GAO test. A number of specialists have been dismissed from their positions. But the process of adjudicating applications has become more confusing; the procedure for what should be done in any given situation changes regularly.

The agency introduced an allowable error percentage in 2009, a percentage the Union felt nearly impossible to achieve[5]. Faced with scores of Passport Specialists that were over the allowable rate[6], Management retracted the criteria, and replaced it in 2010 with another arbitrary error rate.

---

[4] Facilities in Thailand were still being used for production of security features this year, though not by choice of Passport Services.
[5] The rate allowed for an error on 2% of all applications; since each application contains at least a dozen required notations, a specialist could not incorrectly record more than 1 out of 600 notations.
[6] Some regional offices declined to even implement it

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.028

To grossly simplify the current adjudication approach, if a passport specialist would previously transpose digits in copying a date or document number, it almost never led to dismissal; while in 2010, it leads to dismissal. The specialist's focus is now forced onto distinct fields of the application, but not towards assessing the case as a whole. Specialists now adjudicate more cautiously, but this increased caution is not translating into better fraud detection.

For this reason, the drop in hourly production requirements has not yielded improved anti-fraud performance; the extra seconds per application are eaten up rechecking notations instead of looking out for counterfeit documentation. In fact, one of the two successful detections of GAO applications was made by a specialist who is under fire for not adjudicating quickly enough.

The Union suggested that specialists receive a 15 minute exception to the production quota for each case researched/referred for fraud. Currently, taking any option other than issuing a passport lowers the likelihood of meeting the production quota. Due to regional fraud disparities, specialists at some agencies are at a great disadvantage in meeting their production quotas; they see three times as many poorly-established identity cases. Extra minutes to research/write up fraud cases would create a more level playing field and erase the production disadvantage for some locales.

The agency is currently introducing facial recognition into the adjudication process. Like other developments, facial recognition will be a major advance in deterring fraud, but will add more time to process. Extra time should be provided for the added task of comparing photographs.

The GAO's test results do not support the agency's latest assumptions about the adjudication process. The absence of notational errors on the seven GAO applications proves that the employees *were* concentrating; they just didn't have the time to concentrate on detecting fraud.

Based on the results of 2010 test, it seems inevitable that the GAO will conduct another test. If Passport Services is to detect these applications the next time around, the Union believes the following improvements should be made:

- Allow more time for adjudication of passport applications.
- Tweak the current adjudication approach to make fraud detection the main focus.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.029

- Expand the agency's inventory of identification, county/city birth certificates, and foreign citizenship exemplars.
- Lift restrictions on access to new fraud detection databases, making them available to passport specialists.
- Encourage more variety in assignments (and thus minimize the trap of employees adjudicating on "auto pilot"). There are plenty of separate assignments within the adjudication sections and no necessity for employees to perform solely desk adjudication for weeks.
- Involve the Union and employees in the development of nationwide adjudication/fraud detection procedures. The Office of Inspector General's 2009 report recommended that the Union be part of these task forces, yet it has not been.
- Continue and increase interagency sharing of information.

We thank the Subcommittee for considering this statement.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.030

OPENING STATEMENT OF
SENATOR BENJAMIN L. CARDIN
CHAIRMAN, TERRORISM AND HOMELAND
SECURITY SUBCOMMITTEE
OF THE SENATE JUDICIARY COMMITTEE
HEARING: THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II
July 29, 2010

I want to thank our witnesses for being here today. Before we begin, I also want to thank Senator Kyl, the Ranking Member of the Subcommittee, as well as Senator Feinstein, for their strong and continuing interest in ensuring the integrity and security of the passport issuance process.

On May 5, 2009, over 14 months ago, I chaired a Terrorism Subcommittee hearing entitled "The Passport Issuance Process: Closing the Door to Fraud." Today we are holding Part II of that hearing.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.031

During the hearing last year, we learned about a Government Accountability Office (GAO) undercover investigation that had been requested by Senators Kyl and Feinstein to test the effectiveness of the passport issuance process, and to determine whether malicious individuals, such as terrorists, spies or other criminals, could use counterfeit documents to obtain a genuine U.S. passport. What we learned at that time concerned me a great deal. GAO reported to the Subcommittee, and I am quoting from GAO's 2009 report, that:

> ''Terrorists or criminals could steal an American citizen's identity, use basic counterfeiting skills to create fraudulent documents for that identity, and obtain a genuine U.S. passport. . . . GAO conducted four tests simulating this approach and was successful in obtaining a genuine U.S. passport in each case. In all four tests, GAO used counterfeit and/or fraudulently obtained documents."

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.032

The May 2009 GAO report went on to note that State Department and U.S. Postal employees "did not identify GAO's documents as counterfeit," and further noted that:

> "GAO's investigator later purchased an airline ticket under the name used on one of the four fraudulently obtained U.S. passports, and then used that passport as proof of identity to check in to his flight, get a boarding pass, and pass through the security checkpoint at a major metropolitan-area airport.''

But that 2009 GAO report was not the first report that identified problems with the passport issuance process. In 2005 and 2007, GAO brought these issues to light. As a result, GAO's 2009 report stated, and again I am quoting from GAO's report, that: ''State [Department] officials have known about the vulnerabilities in the passport issuance process for many years, but have failed to effectively address these vulnerabilities.''

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.033

Those were very serious findings back in May of 2009 because the U.S. passport is the gold standard for identification. A U.S. passport can be used for many purposes in this country, and it gives an individual the ability to travel internationally, which is an important tool for someone who wants to do us harm, including terrorists, spies and other criminals. So the integrity and security of the passport issuance process is extremely important because it can have a profound impact on the national security of the United States.

More than 14 months have elapsed since that first GAO report, and today we will be learning about a new GAO undercover investigation that I requested, along with Senators Kyl, Feinstein, Lieberman and Collins. In this new investigation, GAO undercover investigators used fraudulent identity documents, including fake drivers' licenses and birth certificates to see if they could obtain genuine U.S. passports.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.034

So what happened this time? Once again U.S. Postal and State Department employees failed to detect the use of fraudulent identity documents. GAO undercover investigators sought 7 passports, and most of them were approved by the State Department. Moreover, four of the passport applications that were submitted used a photograph of the same GAO undercover agent. And two passport applications that were initially approved used Social Security Numbers of deceased persons.

But it is not all bad news. There is some news that is a credit to the State Department, because the State Department detected two fraudulent passport applications before they were approved.

As the Subcommittee attempts to get to the bottom of this, we must not forget that dedicated people are working very hard to correct these problems, and they take their responsibilities seriously. But we must do better – much better!

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.035

Congress can help by giving the State Department all the tools it needs. In that regard, I am introducing, along with Senators Feinstein, and Lieberman, legislation that will help to close the door on passport fraud. Today, I am introducing the "Passport Identity Verification Act." This legislation is a common-sense solution that will give the State Department the legal authorities that it needs to access information contained in federal, state and other databases that can be used to verify the identity of every passport applicant, and to detect passport fraud, without extending the time that the State Department takes to approve passports.

I will also be submitting for the record a letter from the National Federation of Federal Employees, which has previously made a number of recommendations to the State Department about how to improve the passport issuance process.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.036

And from my perspective, management in the State Department needs to partner with its employees to ensure that their helpful and constructive ideas are implemented. I understand that there is pressure on passport examiners to act quickly. And I understand that the American people can become concerned when their travel plans, whether for leisure or business, are linked to their ability to obtain a passport in a timely fashion. But we have got to get this right, and it is not simply a question of process, techniques and training. We need to make sure that the agencies that are responsible for processing passport application documents are concerned about national security as well as customer service, and we need to make sure that they have the legal authorities, the resources and the technology to verify the identity of a passport applicant and to detect passport fraud.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.037

We simply cannot issue U.S. passports in this country on the basis of fraudulent documents. There is too much at stake. We have the technology and the information to prevent such issuance.

Today, we will be hearing from Greg Kutz, Managing Director of GAO's Forensic Audits and Special Investigations Unit, and Brenda Sprague, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs at the U.S. State Department.

Finally, I would now like to recognize the Ranking Member of this Subcommittee, Senator Kyl, who joined with me in making this latest request to GAO, for any comments he would like to make at this time.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.038

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Thursday, July 29, 2010

STATE DEPARTMENT

Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud

Statement of Gregory Kutz, Managing Director
Forensic Audits and Special Investigations

GAO-10-922T

July 29, 2010

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-922T, a testimony before the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

STATE DEPARTMENT

Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud

Why GAO Did This Study

A U.S. passport is one of the most sought after travel documents in the world, allowing its holder entrance into the United States and many other countries. People attempting to obtain a U.S. passport illegally often seek to use the guise of a U.S. citizen to conceal their involvement with more serious crimes, such as terrorism, drug trafficking, money laundering, or murder.

In March 2009, GAO reported on weaknesses in State's passport issuance process that could allow a terrorist or criminal to fraudulently acquire a genuine U.S. passport. Specifically, GAO easily obtained four genuine passports from State using counterfeit documents. In April 2009, GAO suggested that State take 5 corrective actions based on these undercover tests and State acknowledged those corrective actions. GAO was asked to perform additional proactive testing of State's passport issuance process to determine if it continues to be vulnerable to fraud.

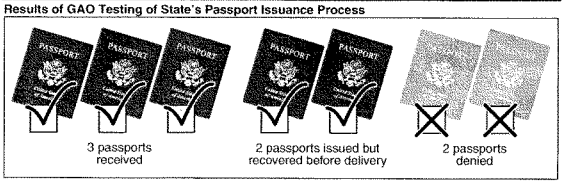
To do this work, GAO applied for seven U.S. passports using counterfeit or fraudulently obtained documents, such as driver's licenses and birth certificates, to simulate scenarios based on identity theft. GAO created documents for seven fictitious or deceased individuals using off-the-shelf, commercially available hardware, software, and materials. Undercover investigators applied for passports at six U.S. Postal Service locations and one State-run passport office.

View GAO-10-922T or key components. For more information, contact Gregory Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

State's passport issuance process continues to be vulnerable to fraud, as the agency issued five of the seven passports GAO attempted to fraudulently obtain. While there were multiple indicators of fraud and identity theft in each application, State identified only two as fraudulent during its adjudication process and mailed five genuine U.S. passports to undercover GAO mailboxes. GAO successfully obtained three of these passports, but State had the remaining two recovered from the mail before they were delivered. According to State officials, the agency discovered—after its adjudication process—that the two passports were part of GAO testing when they were linked to one of the passport applications it initially denied. State officials told GAO that they used facial recognition technology—which they could have also used during the adjudication process—to identify the two remaining applications.

Results of GAO Testing of State's Passport Issuance Process



Source: GAO.

GAO's tests show that State does not consistently use data verification and counterfeit detection techniques in its passport issuance process. Of the five passports it issued, State did not recognize discrepancies and suspicious indicators within each application. Some examples include: passport photos of the same investigator on multiple applications; a 62 year-old applicant using a Social Security number issued in 2009; passport and driver's license photos showing about a 10 year age difference; and the use of a California mailing address, a West Virginia permanent address and driver's license address, and a Washington, D.C. phone number in the same application. These were fraud indicators that should have been identified and questioned by State. State also failed to crosscheck the bogus citizenship and identity documents in the applications against the same databases that it later used to detect GAO's other fraudulent applications. State used facial recognition technology to identify the photos of GAO undercover investigators and to stop the subsequent delivery of two passports but not to detect fraud in the three applications that GAO received, which all contained a passport photo of the same investigator.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.040

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss the results of our investigation of the State Department's (State) passport issuance process. My testimony today highlights the results of our most recent tests of this process, which we have previously shown to be vulnerable to fraud.[1] According to State, over 13 million U.S. passports were issued in fiscal year 2009. U.S. passports are one of the most sought after travel documents in the world, allowing its holders entrance into the United States and visa-free passage into many other countries. People attempting to obtain a U.S. passport illegally are often seeking to use the guise of a U.S. citizen to conceal their involvement with more serious crimes, such as terrorism, narcotics trafficking, money laundering, and murder. For example, in December 2009, an alleged leader of a white supremacist gang was sentenced to 3 years in federal prison for making a false statement on a passport application in order to flee a double-murder investigation.

In March 2009, we reported on weaknesses in State's passport issuance process that could allow a terrorist or criminal to fraudulently acquire a genuine U.S. passport. Specifically, we easily obtained four genuine passports from State using counterfeit and fraudulently obtained documents. Over the years State has taken steps to protect against the fraudulent use of U.S. passports by, for example, issuing only electronic passports.[2] However, terrorists and other criminals could still circumvent these security measures by using stolen identities and fraudulent breeder documents,[3] such as birth certificates and drivers' licenses, to obtain genuine passports. For example, in late 2006, State's Bureau of Diplomatic Security initiated a multiyear investigation, uncovering a criminal

[1] GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C.: Mar. 13, 2009). GAO, *Addressing Significant Vulnerabilities in the Department of State's Passport Issuance Process*, GAO-09-583R, (Washington, D.C.: April, 13, 2009). GAO, *State Department: Significant Vulnerabilities in the Passport Issuance Process*, GAO-09-681T (Washington, D.C.: May 5, 2009).

[2] The electronic passport, or e-passport, is like the traditional passport booklet with the addition of a radio frequency identification (RFID) chip embedded in the back cover, which provides for electronic storage of biographical and biometric data. This addition allows for a comparison of the photo in the passport with the photo in the chip, and can provide greater assurance that the photo, as well as the biographic data, has not been altered or counterfeited.

[3] A breeder document is an ID document issued to support a person's identity and obtain another document of privilege or of greater perceived value.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.041

enterprise through which Jamaican and West African nationals bought counterfeit New York City birth certificates to fraudulently obtain U.S. passports. As a result, agents confiscated 17 fraudulently obtained U.S. passports and intercepted 10 fraudulent passport applications. Further, the fraudulent use of Puerto Rican birth certificates to obtain U.S. passports was so widespread that in December 2009, the Puerto Rican government enacted a law that invalidates all birth certificates issued before July 1, 2010.[4]

This testimony responds to your request that we perform additional proactive testing of State's passport issuance process to determine whether it continues to be vulnerable to fraud. To perform this work, we designed three test scenarios—similar to those we used in our previous testing—that would simulate the actions of a malicious individual who had access to another person's identity information, a practice commonly known as identity theft.[5] We then applied for seven genuine U.S. passports and supported our applications with counterfeit or fraudulently obtained documents, such as birth certificates and drivers' licenses, and the Social Security numbers (SSN) and identities of fictitious or deceased individuals. We fabricated these documents using publicly available software, hardware, and materials.

Our seven tests simulate an individual stealing another person's identity and using it to obtain a passport. Five of our tests were based on information and SSNs we had previously obtained from the Social Security Administration (SSA) for the purpose of conducting undercover tests. One of these included the identity and SSN of a five year old child to simulate a malicious individual stealing the identity of a real child to get a passport. Finally, in two other tests, we used the identities of individuals who died in 1966 and 1969. For six tests, we submitted our passport applications and supporting materials at United States Postal Services (USPS) locations that accept passport applications. For the other test, we submitted our application and materials at State's regional Washington, D.C., passport-

[4] The law was based on collaboration with State and the Department of Homeland Security (DHS) to address the fraudulent use of Puerto Rico–issued birth certificates to unlawfully obtain U.S. passports, Social Security benefits, and other federal services. A June 2010 amendment to the law extends the validity of these birth certificates through September 30, 2010, to provide a transition for those applying for new documents.

[5] Identity theft occurs when an individual steals another individual's personal identifying information and uses it fraudulently.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.042

issuing office. We also briefed State officials on the results of our investigation and discussed their actions on our tests.

We conducted our work from January 2010 through July 2010 in accordance with quality standards for investigations as set forth by the Council of Inspectors General on Integrity and Efficiency.

Background

A U.S. passport is not only a travel document but also an official verification of the bearer's origin, identity, and nationality. Each day, Americans submit them as identification to board international flights, obtain drivers' licenses, cross the border from the United States into Canada and Mexico, apply for loans, and verify their employability. To acquire a U.S. passport for the first time, an applicant must provide evidence of citizenship, or non-citizen nationality,[6] such as a certificate of birth in the United States or a naturalization certificate, and a valid government-issued identification document that includes a photograph or physical description of the holder (most commonly a state-issued driver's license or identity card).[7]

Most passport applications are submitted by mail or in-person at one of almost 9,400 passport application acceptance facilities nationwide. The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document matches the applicant. Then, through adjudication, passport examiners determine whether State should issue each applicant a passport. Adjudication requires the examiner to scrutinize identification and citizenship documents presented by applicants to verify their identity and U.S. citizenship or non-citizen nationality.

Since 2005, we have issued several reports on fraud vulnerabilities within the passport issuance process and the subsequent actions taken by State

[6] Non-citizen nationals, such as individuals born in American Samoa, comprise only a small portion of eligible passport recipients.

[7] Valid government-issued documents include, for example, state drivers' licenses, state identification cards, or military identification.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.043

to prevent individuals from fraudulently securing passports.[8] For example, we reported that identity theft was among the most common means used to commit passport fraud. In March 2009, we reported that our covert testing of State's passport issuance process demonstrated how malicious individuals might use identity theft to obtain genuine U.S. passports. Through our work, we have identified two major areas of vulnerability in State's passport issuance process.

- Passport acceptance agents and passport examiners have accepted counterfeit or fraudulently acquired genuine documents as proof of identification and citizenship. We reported in March 2009 that State issued four genuine U.S. passports to GAO investigators, even though the applications that we submitted contained bogus information and were supported by counterfeit drivers' licenses and birth certificates.[9] The sheer variety of documents that are eligible to prove citizenship and identity also complicate State's verification efforts.

- State's limited access to information from other federal and state agencies hampers its ability to ensure that supporting documents belong to the bearer. In 2005 we reported that the information State used from SSA to corroborate SSNs was limited and outdated.[10] Although State and SSA had signed a memorandum in April 2004 giving State access to SSA's main database, the memorandum had not been implemented. Moreover, the memorandum did not include access to SSA's death records, though State officials said they were exploring the possibility of obtaining these records. Yet, in one case from our covert testing in 2009, we obtained a U.S. passport using the SSN of a man who died in 1965. In response to our prior findings, State officials said that the lack of an automated check against SSA death records was a long-standing vulnerability, but noted that Passport Services had recently purchased a subscription to the Death Master File, which included weekly updates of deaths recorded by SSA. State also indicated that federal agencies limit its access to records due to

[8] GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-477 (Washington, D.C.: May 20, 2005); GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-853T, (Washington, D.C.: June 29, 2005); GAO, *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use*, GAO-07-1006 (Washington, D.C.: July 31, 2007); and GAO-09-447.

[9] GAO-09-447.

[10] GAO-05-477.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.044

privacy concerns and the fact that State is not a law enforcement agency. For example, it could not conduct real-time authentication of the birth certificates presented by passport applicants. The agency added that these documents present an exceptional challenge to fraud detection efforts, due to the thousands of different acceptable formats that the documents can be presented in. It further indicated that there are also difficulties with verifying the authenticity of drivers' licenses.

Covert Testing of State's Passport Issuance Process Shows That Vulnerabilities Remain

State's passport issuance process continues to be vulnerable to fraud, as the agency issued five of the seven passports GAO attempted to fraudulently obtain. Despite multiple indicators of fraud and identity theft in each application, State identified only two as fraudulent during its adjudication process and mailed five genuine U.S. passports to undercover GAO mailboxes. GAO successfully obtained three of these passports, but State had two others recovered from the mail before they were delivered. According to State officials, the agency discovered—after its adjudication process—that the two passports were part of GAO testing when they were linked to one of the passport applications it initially denied. State officials told us that they used facial recognition technology [11]—which it could have also used during the adjudication process—to identify our two remaining applications.

According to State, one of our applications was denied in April 2010 during processing at the National Processing Center in New Hampshire by an examiner who was suspicious that the application in totality was likely an "imposter." The examiner sent the file to a fraud manager in Florida who subsequently determined that the Florida birth certificate was counterfeit. State detected the second fraudulent application after the SSN used was flagged as recently issued by SSA. This application was then sent to the same fraud manager in Florida who processed the first application, since they both contained Florida birth certificates. State officials indicated that they then uncovered GAO's undercover tests by crosschecking the fraudulent Florida birth certificate with the state's Bureau of Vital Statistics.

[11] Facial recognition technology is used to compare an individual's face or photo against multiple "galleries" of images. According to State, staff trained in facial comparison techniques use this technology to help prevent the issuance of U.S. passports to individuals using false identities and individuals who should be denied passports for other legal reasons.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.045

After State discovered our undercover test, the agency used methods and resources not typically utilized to detect fraud during the normal passport adjudication process to identify our remaining tests. For example, according to State officials, they subsequently identified the two remaining GAO applications by using facial recognition technology to search for the photos of the applicants, who were our undercover investigators. State could have used the very same technology to detect fraud in the three applications for passports that we received, because all three passports contained the photo of the same GAO investigator. One of the passports that were recovered after issuance also included the photo of the same investigator.

Our most recent tests show that State does not consistently use data verification and counterfeit detection techniques in its passport issuance process. Of the five passports issued, State failed to crosscheck the bogus citizenship and identity documents in the applications against the same databases that it later used to detect our other fraudulent applications. In addition, despite using facial recognition technology to identify the photos of our undercover investigators and to stop the subsequent delivery of two passports, State did not use the technology to detect fraud in the three applications for passports that we received, which all contained a passport photo of the same investigator. Table 1 and the text that follows provide more detail about each of our tests.

Table 1: Results of GAO Undercover Testing of State's Passport Issuance Process

Test number	Date of Application	State Where Application Filed	Fraud Indicators	Date of Disposition	Final Disposition
1	3/10/10	Washington	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	3/24/10	Passport Issued
2	3/31/10	California	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	5/31/10	Detected, No Passport Issued

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.046

Test number	Date of Application	State Where Application Filed	Fraud Indicators	Date of Disposition	Final Disposition
3	4/19/10	Washington, D.C.	• Identity of a 65 year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit D.C. driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	4/20/10	Passport Issued
4	4/22/10	California	• Identity of a 62-year-old applicant using recently issued SSN • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	5/10/10	Passport Issued
5	5/4/10	Illinois	• SSN of a child being used by a 55-year-old applicant • Counterfeit FL birth certificate • Counterfeit WV driver's license • Different height on application and license • Same photo used in multiple passports	Unknown	Detected, No Passport Issued—Linked to GAO Covert Testing
6	5/25/10	Georgia	• Identity of a deceased individual • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	6/15/10	Recovered After Issuance and Determination That GAO was Conducting a Covert Test
7	5/26/10	New York	• Identity of a deceased individual • Counterfeit FL birth certificate • Counterfeit WV driver's license • Various states used for license, mailing and permanent addresses • Same photo used in multiple passports	6/11/10	Recovered After Issuance and Determination That GAO was Conducting a Covert Test

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.047

Test One (Washington): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual	State issued a genuine passport even though the application contained multiple indicators that should have raised suspicion of fraud, either independently or in aggregate. First, this application included both a counterfeit Florida birth certificate and West Virginia driver's license, both using the same fictitious name that was on the application. If State had confirmed the legitimacy of these documents, it would have easily discovered that they were bogus and thus, not representative of the true identity of the bearer. Second, we utilized an SSN that was recently issued to us by the SSA. If State had authenticated the SSN, it would have detected the fact that its issue date did not closely coincide with the date of birth and age of the U.S. citizen represented in the application. Specifically, the applicant listed was a 62-year-old man born in 1948 while the SSN was issued by SSA in 2009. Finally, State did not question discrepancies between our addresses which included a permanent home address located in West Virginia and a mailing address in Seattle, Washington. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.
Test Two (California): State Detected Our Fraudulent Application Before Issuance	State denied this passport after identifying certain discrepancies and indicators of identity theft and fraud that we included in the application. According to State, this fraudulent application was first detected when the applicant's identity information did not match SSA's records. The application was then submitted to an examiner, who determined that our Florida birth certificate was fraudulent after checking it against Florida Bureau of Vital Statistics records. State also identified physical properties of the document that were inconsistent with an original. In addition, State checked our bogus West Virginia driver's license against the National Law Enforcement Telecommunications System (NLETS), which showed that the license did not belong to the bearer.
Test Three (District of Columbia): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual	State issued a genuine passport even though the application contained multiple indicators and discrepancies that should have raised red flags for identity theft and fraud. Our investigator went to the U.S. Department of State Passport Office in Washington, D.C., which provides expedited passport services to applicants scheduled to travel out of the country within 14 days from the date of application. The State employee made a line-by-line examination of the application to make sure that the information coincided with what was provided to him, on the bogus Florida birth certificate and District of Columbia driver's license. Both documents contained the same fictitious name that was used on the application. However, if State had crosschecked the information from

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.048

these two bogus documents against the same records that it did in the previous case, it could have discovered that neither were representative of the bearer. Further, if State officials had checked the SSN in the application, State would have concluded that it was recently issued and did not coincide with the date of birth represented in the application. In addition, our application indicated that our applicant's height was 5' 10" while his bogus driver's license showed a height of 6'. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport. The following day, our investigator returned to the same location and was issued a genuine U.S. passport.

Test Four (California): GAO Obtained a Genuine Passport Using the Identity of a Fictitious Individual

State again issued a genuine passport even though the application contained multiple indicators and discrepancies that should have raised red flags for identity theft and fraud. This application also included a counterfeit Florida birth certificate and West Virginia driver's license, both in the same fictitious name that was used on the application. If State had adequately corroborated the information from these two bogus documents against the same records that it did in case number two, it could have discovered that the documents were counterfeit and not representative of the bearer. In addition, if State had adequately verified the SSN in the application, it would have found that the recent issue date did not coincide with the age or date of birth represented in the application. State also did not identify about a 10 year age difference between the applicant's passport photo and the photo in his driver's license. Finally, the application included suspicious addresses and contact information—a California mailing address, a permanent and driver's license address from West Virginia and telephone number from the District of Columbia. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

Test Five (Illinois): State Detected Our Fraudulent Application Before Issuance

State identified the fraud indicators and discrepancies that we included in this test and did not issue a passport. In addition, the agency identified this application as a GAO undercover test. First, State identified a major discrepancy with the SSN in our application. When our investigator spoke with a State employee about the status of his application, he was told that the birth year in his application did not match SSA records. In our investigator's fabricated explanation, he explained that he was recently a victim of identity theft and had a new SSN issued. Second, the agency determined that our Florida birth certificate was fraudulent after its check against Florida Bureau of Vital Statistics records indicated that the document was counterfeit. State also identified physical properties of the

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.049

document that were inconsistent with an original. Finally, State questioned why the application was filed in Illinois yet listed a mailing, permanent, and driver's license address from West Virginia.

Test Six (Georgia): State Issued Passport Using the Identity of a Deceased Individual But Prevented Its Delivery

State issued a passport for this application even though it contained multiple indicators of fraud. However, after discovering our testing through our fifth application, it subjected this application to further review and recovered the passport from the USPS before it was delivered. Before the application was discovered as a part of a GAO test, State never identified any of the fraud indicators that we included in the application. Officials stated that facial recognition technology allowed them to discover that the photograph in this application was the same used in previous applications. State then checked our bogus West Virginia driver's license against NLETS, which showed that the license belonged to a person other than the bearer. State officials never questioned why the application was filed in Georgia yet listed a mailing, permanent, and driver's license address from West Virginia and phone number from the District of Columbia. State also failed to identify the misspelling of the city in our West Virginia license and discrepancies with the zip code information on our passport application. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

Test Seven (New York): State Issued Passport Using the Identity of a Deceased Individual But Prevented Its Delivery

As with our sixth test, State issued a passport for this application but prevented its delivery after using facial recognition technology to link the photo to one used in previous applications—again, after discovering our undercover testing. Only after discovering our testing did State check our bogus West Virginia driver's license against NLETS, which showed that the license belonged to a person other than the bearer. If State had checked this license prior to issuing a passport, it would have discovered discrepancies regarding information on the license including the misspelling of the city. Further, State never questioned why the application was filed in New York yet listed a Maryland mailing address and a permanent and driver's license address from West Virginia, prior to issuing the passport that it later revoked. According to State, these were fraud indicators that should have been questioned prior to the issuance of the passport.

In conclusion, Mr. Chairman, the integrity of the U.S. passport is an essential component of State's efforts to help protect U.S. citizens from those who would harm the United States. Over the past several years, we

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.050

have reported that State has failed to effectively address the vulnerabilities in the passport issuance process. Our recent tests show that there was improvement in State's adjudication process because State was able to identify 2 of our 7 passport applications as fraudulent and halted the issuance of those passports. However, our testing also confirmed that State continues to have significant vulnerabilities and systemic issues in its passport issuance process. We look forward to continuing to work with this Subcommittee and State to improve passport fraud prevention controls.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you may have at this time.

Contacts and Acknowledgements

For further information regarding this testimony, please contact Greg Kutz at (202) 512-6722 or kutzg@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Andy O'Connell, Assistant Director; John Cooney, Assistant Director; Matthew Valenta, Assistant Director; Lerone Reid, Analyst-In-Charge; Jason Kelly; Robert Heilman; James Murphy; and Timothy Walker.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.051

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper

DEPARTMENT OF STATE

STATEMENT

OF

BRENDA S. SPRAGUE

DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

HEARING

ON

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

THURSDAY, JULY 29, 2010

Mr. Chairman, Ranking Member Kyl, and Distinguished Members of the Subcommittee:

I thank you for this opportunity to come before you today. I am testifying today to discuss the Department of State's response to concerns raised by the Government Accountability Office (GAO), in their latest undercover investigation of passport operations. I also seek the Subcommittee's support of initiatives to better support the Bureau of Consular Affairs (CA) in detecting and preventing passport fraud.

As the GAO recognizes, CA is fully committed to continually improving our processes in order to maintain the most secure passport issuance system in the world. We take very seriously our responsibility to protect U.S. borders through the vigilant adjudication of U.S. passports. We have worked, and will continue to work, diligently to improve training, procedures, and oversight of the passport application and adjudication processes, and to enhance and upgrade the issuance systems and automated checks that support the process.

My career at the State Department spans nearly four decades. I have served overseas as a member of the Foreign Service, and for the past 24 years in Washington in a variety of positions in the Bureau of Diplomatic Security and the Bureau of Administration before joining CA in July 2008.

My tenure with the State Department has been longstanding, challenging, and varied. Yet in the diverse and wide-ranging landscape of my federal career, no assignment has been as demanding, daunting, and critical as my current mission managing the Passport Services Directorate, particularly with respect to combating and preventing passport fraud.

Through existing fraud detection procedures, we recently discovered that the GAO was conducting a second undercover investigative operation of Passport Services. The first one had been conducted in 2008. Expert GAO investigators, who are trained and skilled in document fraud, created and presented fraudulent birth and identity documents to pose as bona fide U.S. citizens. These investigators then submitted seven passport applications at several passport agencies across the country. The applications used legitimately issued Social Security Numbers (SSNs). The investigators provided counterfeit birth certificates and drivers licenses, some of which were based on genuine documents. We immediately identified two of their applications as frauds during the adjudication process, and we spotted two others later in the process prior to passport delivery. The GAO was successful in receiving three passports. We have requested the return of these passports that were issued in error. Had GAO not confirmed that these applications were part of a GAO-sponsored investigation, we would have alerted the Department's Diplomatic Security Service for further investigation and possible criminal prosecution of the responsible individuals.

CA is dedicated to deterring and detecting passport fraud, and we have made significant improvements to the passport issuance system, but the fact is that we did not catch all seven fraudulent applications. Human error and the volume of documents that we produce annually – 13.5 million passport books and passport cards in FY 2009 – will always represent a challenge for combating fraud in the passport issuance process. However, our commitment to improve the security of the passport issuance system is firm.

Immediately upon discovering this second GAO undercover operation, CA initiated action and took the following steps:

- Placed all personnel involved in issuance of those passports on 100 percent audit;
- Conducted "stand-down" fraud training for all adjudicators on the results of the GAO probe;
- Implemented an aggressive schedule of enhancements to the Travel Document Issuance System, which incorporates Facial Recognition technology, to all passport agencies and centers;

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.055

- Provided fraud training, as appropriate, to the non-State Department acceptance facilities involved;

- Tightened reporting requirements for use of out-of-state identity documents as a second form of identification, and provided updated, comprehensive guidance to acceptance facilities and passport agencies and centers;

- Reviewed standard operating procedures to insure that issues raised by this latest GAO probe are appropriately addressed in guidelines; and

- Developed a training module for all adjudicators on adjudication/fraud issue raised by the GAO probe.

This is not the first time that GAO conducted a "sting" undercover audit of State Department passport issuance operations. Following a similar effort two years ago, we made process improvements and were more successful in detecting GAO's latest efforts. As noted above, we are already changing our processes to better detect the methods GAO employed this time.

While even one passport issued in error is one too many, it was exactly the improvements which we put in place after the 2008 GAO operation that allowed us to recognize passport issuance irregularities *before* GAO acknowledged this recent operation. We recognized that the citizenship and identity documents GAO investigators submitted with several of these applications were fraudulent. As we investigated further, we identified other applications submitted with fraudulent identities and pulled them before they were received by the impostors.

Since the 2009 GAO report and recommendations, we:

- Implemented an aggressive, ongoing program of fraud prevention and detection training for our Passport Adjudication Specialists;

- Increased our data-sharing and liaison with federal, state, and local law enforcement and intelligence agencies, the Social Security Administration, and U.S. Citizenship and Immigration Services;

- Established an Acceptance Facility Oversight Program and provided enhanced web-based and classroom training for non-State Department Acceptance Agents at the 9,400 designated facilities where the general public may apply for a U.S. passport;

- Reviewed our adjudication program from top to bottom, and enhanced it with comprehensive standard operating procedures and a standard continuum of training and performance expectations for Passport Specialists;

- Created an Adjudication Office at the national level to support the important work of the Passport Agencies through the development and implementation of standardized adjudication policies and procedures; development and evaluation of production metrics; validation studies; and implementation of an adjudication audit program;

- Established the Procedural Integrity Testing and Training Program, or Red Teams, to test the effectiveness of our adjudication and anti-fraud efforts, identify and mitigate vulnerabilities, and improve the quality of the passport issuance process;

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.056

- Piloted state-of-the-art technologies to support Passport Adjudication Specialists to prevent passport fraud, including the acceleration of the implementation of facial recognition and other biometrics in our passport application adjudication process;

- Procured additional data sources to help us detect fraud; and

- Doubled the number of Fraud Prevention Program Managers at our Passport Agencies.

Ninety-eight million passports are held by Americans. I am proud of the Department's work to provide these millions of Americans with passports that enable them to travel freely in and out of the United States. These passports also serve as proof of identity and U.S. citizenship for many federal and other benefits. No one is more aware of the importance of maintaining the integrity of the passport adjudication process than those of us in the Bureau of Consular Affairs.

As demonstrated by the GAO's most recent undercover operation, the greatest threat to the integrity of the passport issuance process is document fraud. It is the availability of fraudulent documentation that is then used to apply for passports. Passport fraud is often linked to other crimes such as using stolen identities of U.S. citizens, using assumed identities, or using the identity of a deceased person. CA needs the help of this Subcommittee and others in Congress to obtain the necessary tools to strengthen the passport issuance process.

We issue passports based on verification of citizenship and identity documents that are issued by federal, state, and local jurisdictions. We do not control or regulate the physical characteristics of these documents, nor the way in which they are issued. We must have the means to verify the authenticity of these documents and to confirm the information provided on the passport application.

Increased information sharing, within the federal government and with state and local governments, is one of the most effective ways to ensure that only those entitled to U.S. citizenship receive a passport. CA is continually engaged in this effort. However, our efforts to gain access to information are hampered because CA is not considered a law enforcement entity for information sharing purposes. We need this designation.

The State Department continues to work actively with other federal agencies and state governments to establish additional data share programs to augment our ability to confirm information provided by passport applicants. We are working with state vital records bureaus to encourage participation in a national centralized database of birth and death records. We encourage development of standardized birth records. Some of our more recent agreements include:

- Real-Time Verification of Social Security Numbers: CA and the Social Security Administration are working to implement real-time verification of SSNs and other data.

- Verification of Driver's Licenses: The Department is currently using the N-LETS system to verify driver license issuance with state DMVs. We have access to driver's license data for 49 states, Puerto Rico, and the District of Columbia. South Dakota is the only state not participating.

  However, as we are not considered a law enforcement entity, we have limited access to the driver's license data. We are unable to view the data files or photographs of license holders. CA needs greater access to state DMV data files and other data that will assist us to verify the identities of passport applicants.

- Verification of Vital Records (Birth and Death Certificates): We currently verify birth certificates through the Electronic Verification of Vital Events (EVVE) system available through the National Association for Public Health Statistics and Information Systems. EVVE is a

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.057

centralized database that verifies birth certificate data available from 19 states, with plans of expanding the program to all 50 states by May 2011.

Individual jurisdictions participate in the EVVE system to varying degrees. The two major factors deterring standardization are funding, particularly if reissuance of all birth records is required, and complications posed by the disparate levels of technology employed by the various jurisdictions, some of which use little to no electronic recordkeeping.

A national standard birth certificate format for documents submitted in support of passport applications would greatly assist our anti-fraud efforts.

A number of studies have concluded that the misuse of birth certificates is a major factor in perpetrating various crimes. Virtually all federal and state agencies agree that stolen, counterfeit, and altered birth certificates are often used as "breeder documents" that allow the holder to obtain additional documents necessary to create false identities. All seem to conclude that fraudulent birth certificates are easy to obtain.

The number of different types of U.S. birth certificates in circulation is overwhelming. According to the *Birth Certificate Fraud* report issued by the Department of Health and Human Services, Office of Inspector General in September 2000, there are more than 6,400 state and local jurisdictions issuing birth certificates, with over 14,000 versions in circulation. The report revealed that state vital records offices currently issue 113 different types of certified copies of birth records. This number does not account for the number of additional variations in local office issuance. Additionally, 51 of the 53 primary vital records offices issue certified photocopies of actual birth records, 37 issue certified copies of computerized abstracts of birth records, 17 issue wallet-sized birth certificates or cards, and eight issue commemorative birth certificates, each with its own unique security features and signatures.

Even more alarming, 13 states allow "open" access to birth records, which allows virtually anyone to request copies of birth certificates on file. At some vital records offices and issuing entities, requestors can purchase birth certificates without identification or other verification that they are entitled to a copy of the birth record.

The HHS-OIG report concludes what we in Passport Services already know, that the large number of state, county, city, township, and other entities issuing birth certificates vastly increases opportunities for fraud and theft. Differences in paper, format, signatures, and security features of the hundreds of jurisdictions issuing birth certificates make the detection of fraudulent birth certificates daunting. This is the challenge we face, and we face it every day.

The ease with which genuine birth certificates may be obtained and the lack of standardized formatting add significant vulnerability to the passport adjudication process, which hampers our ability to ensure that applicants are legitimately entitled to a passport. We seek the Subcommittee's support to encourage standardization of birth documents.

As this Subcommittee knows, one of the reasons Congress enacted Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) was to limit the number of identity and nationality documents that U.S. citizens could use as proof of citizenship to enter the United States. In doing so, Homeland Security's Customs and Border Protection officials no longer faced the formidable task of verifying U.S. citizenship by examining the more than 14,000 different versions of U.S. birth certificates that could be presented at land and sea borders. However, in our work, CA still must review thousands of different versions.

A birth certificate is the single most common document used to establish U.S. citizenship. It is used to obtain documents such as driver's licenses, Social Security cards, and U.S. passports. It is

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.058

crucial that the processes for issuing birth certificates is standardized, and that the latest technology is used to ensure that their physical integrity.

The Government of Puerto Rico recently passed Law 191 of 2009, invalidating all copies of certified Puerto Rican birth certificates issued prior to September 30, 2010, and prohibiting the retention of certified birth certificates by public and private entities effective January 1, 2010. The law aims to prevent identity theft and passport fraud perpetrated by criminals who illegally obtain copies of certified birth certificates from institutions in Puerto Rico. Approximately 40 percent of the passport fraud cases investigated by the Department of State's Diplomatic Security Service in recent years involved birth certificates issued in Puerto Rico.

CA commends the Government of Puerto Rico for passage of this law. We believe the law will significantly reduce the incidence of fraud involving Puerto Rican birth certificates. We hope that states and local jurisdictions will take similar steps to improve their vital records issuance processes.

To minimize the risks associated with using birth certificates as part of the passport application process, the Department continues to explore a number of options, including:

- Requiring "long-form" versions of birth certificates, which provide additional detail about an individual's parents and place of birth;
- Requiring the acceptance of only one standardized birth certificate format from each jurisdiction;
- Requiring the acceptance of birth certificates only if printed on a jurisdiction's standardized paper; and
- Requiring the acceptance of state-issued birth certificates from a central database.

CA also needs the ability to require SSNs on passport applications. In addition to birth certificates, we rely heavily on data provided by SSA to verify SSNs and other identifying information provided by passport applicants. Our data share agreement with SSA allows us to validate SSNs to ensure that they are correct and not associated with a deceased individual. The previous GAO investigation criticized the Department for not verifying SSNs. In this recent investigation, GAO used legitimately-issued SSNs validated by the SSA batch processing check we now use.

While the Department strongly encourages applicants to include their SSNs on passport applications, we do not have the authority to require applicants to do so. The Privacy Act prohibits the Department from requiring SSNs as a condition for receiving a passport. There are strong security justifications for a requirement to include SSNs on passport applications.

Finally, we need your support for continuation of the Western Hemisphere Travel Initiative (WHTI) Surcharge as requested in the President's FY 2011 Budget.

Currently, we retain a $22 "WHTI Surcharge" for each passport application to build and operate the infrastructure needed to meet the growing demand for passports as we strengthen border crossing requirements. The surcharge will continue to be charged, but we will lose our authorization to retain it at the end of this fiscal year. We need these funds to strengthen our systems and combat fraud and our request is part of a larger fee retention package which is in the President's FY 2011 Budget.

All of us in the federal government are committed to enhancing the safety and security of government services, and to making them more efficient, equitable, and responsive to the needs of the American people. CA is committed to protecting the integrity of the U.S. passport. We are receptive to recommendations from any source that might improve passport operations, detect and prevent passport fraud, and enable us to provide better customer service to passport applicants.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.059

I thank you for this opportunity to discuss with you the Department of State's response to the latest GAO undercover investigation of passport operations. I appreciate the Subcommittee's understanding of the threat document fraud poses to the integrity of the passport issuance system. My hope is that you will support the initiatives I have discussed, because they are essential to detecting and preventing passport fraud and depriving criminals of the ability to cross our borders.

VerDate Nov 24 2008 10:37 Mar 09, 2011 Jkt 064705 PO 00000 Frm 00084 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\64705.TXT SJUD1 PsN: CMORC

64705.080