S. HRG. 111–212

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MAY 5, 2009

Serial No. J–111–19

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

54–246 PDF WASHINGTON : 2010

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 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

PATRICK J. LEAHY, Vermont, *Chairman*

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

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

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

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
RON WYDEN, Oregon
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 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	1
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	3
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	2

WITNESSES

Ford, Jess T., Director, International Affairs and Trade, U.S. Government Accountability Office, Washington, D.C.	19
Sprague, Brenda S., Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. Department of State, Washington, D.C.	5

SUBMISSIONS FOR THE RECORD

Ford, Jess T., Director, International Affairs and Trade, U.S. Government Accountability Office, Washington, D.C., statement	27
Sprague, Brenda S., Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. Department of State, Washington, D.C., statement	35
Verma, Richard R., Assistant Secretary, Legislative Affairs, Department of State, Washington, D.C., letter	40
Walle, Colin Patrick, Vice President, National Federation of Federal Employees (NFFE), Washington, D.C., statement	44

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD

TUESDAY, MAY 5, 2009

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

The Subcommittee met, pursuant to notice, at 2:40 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Benjamin L. Cardin, Chairman of the Subcommittee, presiding.

Present: Senators Cardin, Feinstein, and Kyl.

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

Chairman CARDIN. The Subcommittee on Terrorism and Homeland Security will come to order. I want to thank our witnesses for being here today. I particularly want to thank Senator Kyl and Senator Feinstein for the purpose for why this hearing has been called, looking into the security of the issuance of passports. It was Senator Feinstein and Senator Kyl who asked GAO to undertake a study to proactively test the effectiveness of our current passport-issuing process to determine whether malicious individuals could use counterfeit or fraudulently obtained documents to obtain a genuine U.S. passport.

Now, this is an extremely important issue for us because the passport is the gold standard for identification in this country. It is used for so many purposes, and it also, of course, gives an individual an ability to travel, which is an important tool for someone who wants to do harm, including terrorists.

The GAO report that we have before us—and we will be hearing from GAO today—concludes that terrorists or criminals could—I am quoting from the report. "Terrorists or criminals could steal an American citizen's identity, use basic counterfeiting skills to create fraudulent documents for that identity, and obtain genuine U.S. passports from the State Department. 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 State Department and the United States Postal Service employees did not identify GAO's documents as counterfeit. GAO's investigators later purchased an airline ticket under the name used on the fraudulent passport and then used the passport to check in for the flight, get a boarding pass, and passed through security checkpoints at the airport."

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

Now, that should alarm all of us—four out of four able to obtain fraudulent passports. In one case, the applicant used the Social Security number of a 5-year-old fictitious child, and the applicant was 53 years old. In another case, the applicant used the Social Security number of a deceased individual who died in 1965, and we have records where that could have been checked out.

Now, the State Department acknowledges the problems, and I know recommendations have been made by GAO, and we are talking about making modifications in the system. And that may give us some comfort if this was the first time that these issues were brought to our attention. But there have been previous GAO reports with similar findings and similar efforts and commitments made to correct the failures of the system.

So as has been pointed out in the report, "State officials have known about the vulnerabilities in the passport-issuing process for many years, but have failed to effectively address these vulnerabilities."

That is a serious statement, one in which this Committee is going to ask questions today. We are concerned of whether GAO's recommendations will be effectively acted upon.

Now, I want to submit for the record the National Federation of Federal Employees Local 1998, statements talking about the pressure on passport specialists to act quickly on approval. And I understand that. You are probably getting calls from our office telling you to move these passports a little bit more expeditiously, people have planes to catch, and get these passports issued. There is pressure. I understand that. But we have got to get it right. We cannot issue fraudulent passports in this country. We have got to take every step to make sure that cannot be done. There is too much reliance on the reliability of a passport that goes through our international borders.

So, today, we will hear from Brenda Sprague, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs at the U.S. State Department, and from Jess Ford, the Director of International Affairs and Trade at the GAO.

With that, let me turn to Senator Kyl, who has been the moving force behind the GAO report and this hearing.

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

Senator KYL. Thank you, Mr. Chairman, and thanks also to Senator Feinstein, as you mentioned, who was also active in seeking to get this information. I appreciate the work of the GAO. Obviously, we will learn at the time that Mr. Ford testifies a little bit more about their evaluation of the extent to which this is a problem. But certainly in the report, it is evident that we do have a problem.

I want to acknowledge—and, incidentally, I totally agree with everything you said in your opening statement, Mr. Chairman. The passport is supposed to be the gold standard for documents in the United States, and yet this GAO report verifies that it is not as reliable as we thought it was.

There are some corrective actions I understand State has indicated that it is taking, but I think there are some other common-

sense things that have not yet been done, and perhaps the best thing I can do is just presage some of the questions that I will be asking, and perhaps in opening statements you can address these: first of all, why so many individuals' applications were approved even though there were no Social Security numbers sought or supplied. Something like 72,000 applicants, according to GAO, in just a 6-month period last year received passports without supplying a Social Security number.

And then, conversely, in those situations where there was a number supplied, the State Department approved thousands of applications without any feedback from Social Security as to whether the number was accurate or whether the individual was connected to the number. And, also, whether it is current policy—this is the way current policy at least is described, in which case obviously policy was breached in many of these cases—whether it is current policy to approve applications from only individuals who have presented a Social Security number and only after word has come back from the Social Security Administration confirming the information relative to that number. If that is the policy, it has obviously been breached. If it is not the policy, why isn't it?

And, finally, asking whether—and I will be primarily focused on this from our GAO witness, but whether weakening the REAL ID driver's license requirements will also end up making it possible for more criminals, terrorists, and others to get fraudulent passports and thereby pose an additional risk to the country.

As I said, the U.S. passport is thought to be the most secure identification that we have in this country, and clearly that is not the case, according to the GAO report. We need to make sure that enough changes are effectuated that we can return to that gold standard, and that will be up to our colleagues at the State Department to ensure that this is accomplished.

Thank you, Mr. Chairman.

Chairman CARDIN. Thank you.

As I mentioned at the beginning of the hearing, we thank Senator Feinstein and Senator Kyl for bringing this issue to our Subcommittee's attention and to the American people's attention. Senator Feinstein is the former Chairman of this Subcommittee, and as I have said many times, I look to her for continuing the priority that this Committee has had in protecting the security of our country.

Senator Feinstein?

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

Senator FEINSTEIN. Well, thank you very much, Mr. Chairman, and I thank you for your leadership. It is very much appreciated. And thank you for continuing the tradition that Senator Kyl and I began. I think we spent a lot of time on this issue in this Subcommittee, and we now have the GAO report. And so if I may, as you know, I went on to chair Intelligence, and so I have got an Intelligence meeting. But I believe this is important, so I would like to make a brief statement, if I might.

Chairman CARDIN. Certainly.

Senator FEINSTEIN. When the GAO uncovered in its investigation—what it uncovered I think is very alarming. A GAO undercover agent attempted to get a United States passport based on counterfeit documents and fraudulent Social Security numbers and succeeded in four out of four attempts. That is 100 percent of the time.

The State Department failed to clear all four of these passports through the Social Security number clearance check—first mistake—which takes only 24 hours.

The State Department did not identify the counterfeit birth certificates or the counterfeit driver's licenses. It also issued all four passports to the same individual and had no system to pick this up. One passport, as we know, was issued to a middle-aged man based on a 5-year-old's Social Security number, and another was issued even though the Social Security number was from a deceased individual.

Now, the question arises: How many passports are out there that were wrongly issued and are being used by those seeking to do others harm?

The State Department will testify today that it has made concrete steps to begin to close these vulnerabilities. While this is encouraging, State Department officials have known about these vulnerabilities for many years, but have failed to fully secure the process.

For example, the GAO, in a report released in 2005—that is 4 years ago—recommended that the State Department check all Social Security numbers against the Social Security Administration's data base of deceased individuals. But this was not done until December 2008, 3 years later. In addition, it is my understanding that employees processing the passports had raised this solution with the State Department as early as 2001.

Now, the GAO's report contains problems and solutions, and let me run through a few of them.

Problem: Applications were not held for 24 hours to allow for Social Security numbers to clear a system. Solution: No passports should be issued before the 24-hour Social Security check is clear.

Problem: Adjudicators did not identify counterfeit birth certificates. Solution: A birth certificates data base to provide greater access to a national data base verifying birth certificates. This is in existence.

Problem: Adjudicators did not identify counterfeit driver's licenses. Access to a national driver clearinghouse is available. Bureau of Diplomatic Security can request that the passport office gain access to this data base.

Problem: All four passports were processed to the same person. Solution: Develop the technology to have the photograph matched against existing data bases. The State Department is building a facial recognition system currently.

Problem: Social Security number did not match with date of birth given, was flagged by computer, but missed by adjudicator on the screen. This is a human error. Training and oversight for all adjudicators is presented as the solution, along with regular audits and undercover checks internally of passport issuance process.

Problem: Social Security number that belonged to deceased was not caught. Solution: Again, the Social Security death match system is now up and running since December of 2008.

And the final problem: The State Department did not know it had wrongly issued the passports until the GAO told them. And the solution is to require an audit for passports issued wrongfully.

So there are solutions to every one of these problems, but, you know, I think that the passport is more and more becoming the common identity document. And if this passport is easily forged and so easily obtained that the clearances are not gone through by State, I think it jeopardizes the whole system.

In my view, this is a very important hearing, Mr. Chairman. I thank you for holding it, and hopefully the State Department will be willing to take the necessary actions.

Chairman CARDIN. Thank you, Senator Feinstein.

I would ask that Ms. Sprague and at the same time if Mr. Ford would just be prepared to take the oath, that way we could do both of you at one time. Thank you. If you would raise your right hand. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth?

Ms. SPRAGUE. I do.

Mr. FORD. I do.

Chairman CARDIN. Thank you. Ms. Sprague, we are pleased to hear from you.

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

Ms. SPRAGUE. Chairman Cardin, Senator Kyl, Senator Feinstein, and distinguished members of the Subcommittee, I appreciate this opportunity to discuss the passport issuance process and the plans we have to address our fraud vulnerabilities. We take seriously our responsibility to protect U.S. borders and the integrity of the U.S. passport through vigilant adjudication. The Bureau of Consular Affairs works diligently to improve training, procedures, and oversight throughout the passport adjudication process. The outcome of the General Accountability Office's recent investigation shows that we need to do more. We have already taken a number of immediate actions and are in the process of devising a detailed plan to enhance our entire process and program.

As you already have been briefed, a GAO investigative team informed Consular Affairs on February 10, 2009 that they had performed a probe of the passport issuance process. The team reported that a GAO investigator submitted four passport applications—three at local postal acceptance facilities and one at a passport agency—utilizing a combination of counterfeit or fraudulently obtained documents. All four applications resulted in U.S. passports being issued in error. The subsequent GAO report specifically identified two major/significant vulnerabilities in our process: one, that passport specialists were unknowingly approving applications before all information checks were completed; and two, passport spe-

cialists and acceptance agents did not recognize fraudulent documents.

CA immediately initiated a number of measures to address these vulnerabilities and to mitigate potential fraud in the future. Some measures taken or contemplated would be more appropriately discussed only in a closed session.

First, upon receiving information from the GAO regarding the four passports issued in error, we promptly identified each passport, and in accordance with standard operating procedures, we revoked the passports and posted corresponding "lookout alerts" in our internal systems and with U.S. border officials and Interpol.

We suspended adjudication approval authority for the four passport specialists who issued the four GAO applications.

We suspended the authority of the acceptance facilities that accepted the three GAO applications.

We immediately provided counterfeit document detection refresher training to all passport agency managers and specialists. Biweekly case study meetings are being held by agency supervisors with the passport specialists regarding unfamiliar or fraudulent documentation received in the office. The GAO report was shared with passport agency staff to reiterate the importance of carefully reviewing identification and citizenship documents, as well as the information on passport applications, to detect fraud. In addition, we revised performance standards for passport specialists to reemphasize the importance of quality adjudication and fraud prevention performance standards.

We instituted a 100-percent audit of all live applications. Passport specialists were released from the audit only when they had demonstrated to their supervisors that they were processing work in full compliance with adjudication standards as related to both proper annotation and attention to possible fraud indicators.

We revised our procedures regarding the processing of same day "will call" service cases. Additional supervisory oversight is required for all same day applications. Agencies have been directed to complete all information checks prior to the issuance of the passport. These procedural changes enhance our ability to identify potential fraudulent applications or documents. Additionally, passport acceptance agents at post offices and courthouses and passport specialists at our passport counters must now photocopy all identification documentation submitted by applicants so that it can become a permanent part of the passport record.

Second, we created an Adjudication Policy and Process Review Working Group in mid-March to help further identify necessary improvements. This working group consists of five subgroups, which are:

One, Restructuring of Adjudication Process and Oversight: This subgroup is reviewing the current adjudication program and working on recommendations to restructure our processes. Additionally, the subgroup is working on recommendations for a new adjudicative managerial oversight function.

Adjudication Requirements and Standards: This subgroup is developing standardized desk and counter adjudication procedures. Additionally, it is developing standardized procedures for passport

specialists regarding the use of the Social Security number and other commercial data-bases.

Post-Issuance Audit: This subgroup is developing a statistically valid audit process for previously issued passports. The results from this audit will be used for future training purposes.

Training Initiatives: This subgroup is identifying enhancements for fraud training for all passport specialists, supervisors, and fraud prevention managers. It is reviewing the curriculum of the National Training Program, which we use for training our new employees, to ensure that it appropriately and thoroughly addresses the document verification requirements used by passport specialists. Also, the subgroup is identifying and recommending standard requirements for on-the-job training for new hires once they complete the National Training Program and begin working with "live"—unapproved—applications. Additionally, it is developing standardized fraud awareness training for our courthouse and post office acceptance facilities.

Technology: This subgroup is identifying technical and procedural vulnerabilities to the integrity of the passport process. Additionally, it is working on recommendations for improvement to our automated systems through access to additional data-bases. In connection with this initiative, we have already developed the business process requirements for introduction of a facial recognition tool by the end of the calendar year.

Formal recommendations from the subgroups are expected by the summer of 2009. Shortly afterward, they will be compiled, finalized, and forwarded for Department management approval.

Third, CA is already working on some long-term initiatives to address our process vulnerabilities. We are currently pursuing an initiative to combine the systems platforms for domestic and overseas passport adjudication and issuance to ensure consistency and improve overall quality control. The combined system will utilize as many automated adjudication checks as possible.

The GAO report recommended that we work with State-level officials to develop a strategy to gain access to their data-bases and incorporate reviews of these data-bases into our adjudication process. Prior to the GAO undercover test, CA officials had held ongoing meetings with Federal and State government agencies regarding access to information and data-bases for citizenship and identity verification. As a result of the GAO's recent recommendation, I also sent a letter to all State Registrars asking for their assistance in providing the Department access to their birth and death records for verification purposes. We plan to vigorously continue this effort.

I appreciate the opportunity to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. We appreciate GAO's constructive recommendations and look forward to working with Congress and the GAO to produce the most secure passport possible. Let me end by assuring you that the Department is fully committed to a secure passport issuance process and deterring and detecting fraud.

Mr. Chairman, thank you again for the opportunity to be here today. I will be pleased to answer any questions that you, the

Ranking Member, and other distinguished members of the Subcommittee might have.

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

Chairman CARDIN. Well, Ms. Sprague, thank you very much for your testimony. I think everything you said, it is hard to disagree with any of the changes that you are putting in place.

I want to point out that I will confer with Senator Kyl and Senator Feinstein after this hearing to determine whether we need a closed session to go over the recommendations that cannot be done in a public session, and we will make a determination.

But I want to just ask you first, tell me the reaction in your Department when you found out about the GAO report that four out of four fraudulent passports were obtained by the use of fraudulent information.

Ms. SPRAGUE. Speaking for our management team, I would say the correct reaction would be they were heartsick, horrified, embarrassed. Speaking for the passport specialists with whom I have spoken, they were horrified, upset, anxious, concerned, and they have cooperated in a tremendous way with us, all of them, to try and address these vulnerabilities and find ways to improve our situation and to make things better.

Chairman CARDIN. I appreciate that.

Senator Feinstein pointed out something I had read earlier, that these passports were used to obtain boarding passes for flights. It is very conceivable that this method could have been used by a terrorist in order to gain into travel and then having a passport that would not reflect any sign of concern to the security people at the border. That obviously is a significant breach in the security system of our country.

What concerns me is that this is not the first time. There have been previous GAO reports and there was your own internal report in 2008 that showed the issuance of passports that should not have been issued to criminals.

Why is it different this time? Why should this Committee expect that these recommendations will be effectively implemented when in the past they have not been effectively implemented?

Ms. SPRAGUE. Mr. Chairman, we have a very difficult challenge facing us, and we have addressed it in a number of ways.

When we look at a passport and we sit down to adjudicate it, we are trying to establish three things: No. 1, the identity of the individual; No. 2, whether or not this individual is a citizen; and, No. 3, whether or not there is some reason this person should be prevented from traveling.

I would like to address the alert system first. We have, since 2005, done a great deal of work on our alert system working with the Terrorism Screening Group, working with NCIC, working with our own colleagues in the visa office, to make a system, a lookout system that is first class. We believe that people who have been identified to us by law enforcement who apply in their own names would, in fact, be intercepted.

The second part of that is identity. Identity is very difficult. We rely upon, for the most part, driver's licenses. There are difficulties with driver's licenses. We, of course, have difficulties verifying the

identity of driver's licenses. But even when we can verify that a driver's license was issued to a particular individual, we have no guarantee that that person is, in fact, who——

Chairman CARDIN. I also understand you do require in almost all cases a Social Security number.

Ms. SPRAGUE. We do require a Social Security number, but we cannot refuse to adjudicate a passport if someone does not provide a Social Security number.

Chairman CARDIN. Let us first start with those who do supply a Social Security number.

Ms. SPRAGUE. Yes.

Chairman CARDIN. We have data banks which could have discovered in, I would think, both of the cases in which the fraudulent Social Security numbers were used that they were fraudulent. Why were they not used? And has that been corrected? Will there be routinely the use of the data banks to determine whether the number given is from a person who is alive and at the proper age?

Ms. SPRAGUE. We have a system—it is a 24-hour batch process—that we rely upon to confirm the validity of the Social Security number. Actually, the overnight check provides us a hit against the Social Security Death Master File as well as giving us a match/no-match. But it also provides us with reasons that there is not a match so that we can further resolve it, because in many instances the Social Security data-base will have errors or there will be data entry errors, and we are able to resolve those with the help of Social Security.

The reason this happened—and this was something that GAO brought——

Chairman CARDIN. But my question is——

Ms. SPRAGUE.—to our attention—is that the 24-hour batch did not run. For probably the first time in our history, we were able to move passport applications so quickly that we were unaware of the fact that the check had not been run. We——

Chairman CARDIN. I do not follow that. I cannot follow that. You lost me.

Ms. SPRAGUE. The applications——

Chairman CARDIN. You are saying that there was a system in place for the Social Security number checks, you thought they had been done, but they were not done?

Ms. SPRAGUE. Yes. The short answer is yes. At headquarters——

Chairman CARDIN. That is even more concerning.

Ms. SPRAGUE. It is a concern.

Chairman CARDIN. Because how do we know that that will not happen—that is not happening right now?

Ms. SPRAGUE. Because we have given directive to the field that no application is to be processed until the 24-hour match is.

Historically, passport applications did not move through the system as quickly, and after the passport surge, we had hired a great deal more people, and then when passport demand went down in 2008, the work began to move through the system so quickly that, unbeknownst to the people who were processing it and unbeknownst to us at headquarters, it actually was given to the adjudicators before the check had been run. And just looking at the

batch, there was no way for the supervision or the individual employee to realize that had not been done.

Chairman CARDIN. How would they know today that it has been done?

Ms. SPRAGUE. Because we are not going to permit anything to go faster than 24 hours. It simply will not be turned over.

Chairman CARDIN. Well, how will they know that the actual check has been done? Let us take the case that there is—that the system is down that does the checks or that someone does not show up that is responsible for it or it is one of those that gets lost through the system and no check was done. How will the individual who approves the passport know that the actual check has been done?

Ms. SPRAGUE. There is a screen that appears on the—there is a box that appears on the screen that says "No record found." We have instituted new procedures that when that happens, it must immediately be turned over to a supervision. So, in this particular instance, the passport adjudicators got the "No record found" and proceeded anyway. We have put a stop to that.

Chairman CARDIN. I am still not comfortable that we have a system in place that will stop the issuance of a passport, checks have been made as to whether this person has a valid Social Security number or not. You are telling me that on the screen of the person who is going to approve the application there will be a reply saying "No record found," or something like that.

Ms. SPRAGUE. It says "No record found," and in that case it must be pulled and handed over.

In the case of a death match, for instance, adjudication stops and the application cannot be processed anymore.

Chairman CARDIN. OK. Let us take both cases, and let me just finish this up. If it shows that the person is deceased, the Social Security number used, obviously you are not issuing the passport, at least that is——

Ms. SPRAGUE. That is correct.

Chairman CARDIN. What do you do? Do you then send it to investigation?

Ms. SPRAGUE. We send it to the fraud prevention manager, and after he has conducted his investigation, it can be turned over to Diplomatic Security for further investigation, and that is normally the route that it would go.

Chairman CARDIN. And that could lead to prosecution or——

Ms. SPRAGUE. It could indeed.

Chairman CARDIN. And now, if you find no record found, previously if it was 24 hours later, the passport would have been issued, and now you are telling me it will not be issued, it will be sent to a supervisor?

Ms. SPRAGUE. It should never have been issued, but we have taken additional steps to ensure that the "No record found" will, in fact, stop the adjudication.

Chairman CARDIN. Can you override that?

Ms. SPRAGUE. At this time we can, but that is one of the things we are going to be looking at and making it impossible to do so.

One of the problems that we have with Social Security is that there can be a lot of errors in the Social Security data-base.

Chairman CARDIN. I understand.

Ms. SPRAGUE. And as a result of that, we do want to enable the supervisor, and at times even the adjudicator, to be able to override what can be easily identified, for instance, transposition of a number. But we have to——

Chairman CARDIN. I just want to make sure it is not overridden because of an anxious traveler.

Ms. SPRAGUE. I agree with you.

Chairman CARDIN. I want to make sure that there is someone looking at it that is satisfied that this person is entitled to have a passport issued. I am still not satisfied that you have that in place. And I must tell you, you are not giving me a comfort level that I would like to have today.

I have some more questions for the second round. Let me turn it over to Senator Kyl.

Senator KYL. Senator Feinstein, do you need to leave?

Senator FEINSTEIN. I have just—if I may just for a minute and then I will excuse myself.

Ms. Sprague, we have been looking at this for a while now. I think the only way to really know if your reforms are effective is in 6 to 9 months ask for another GAO investigation. I found when I was mayor of San Francisco, I sent an undercover officer out to San Francisco airport with a concealed weapon and said, "See if you can go through the magnetometers. I want to see how good they are." Again, four out of four times they got through, which sent a very loud message of what we had to do, and I think this sends a very loud message of what you have to do.

My view is that no passport should be issued until these checks are complete. No system should be overridden to give a passport. And what I suspect has happened—and I cannot prove this—is that somebody has said, you know, move those passports. And so they go out before the checks have been adequately performed.

I think as the Chairman referenced—and the Ranking Member knows very well—this is really the soft under-belly of our country, and it really puts us in harm's way if these checks are not made.

So I have no question other than to say to you it is really up to you, and I believe that the Senate will support you in this matter. We cannot put out passports that are gained with fraudulent documents, ever.

Ms. SPRAGUE. Absolutely.

Senator FEINSTEIN. So thank you very much for being here, and we will do another report, and we will see how good you did.

Ms. SPRAGUE. Senator Feinstein, I did want to tell you that, in response to the GAO investigation, we are working with the Bureau of Diplomatic Security to create red teams who will test our system and give us a heads up, so the next time that GAO comes, we will be ready.

Senator FEINSTEIN. Good.

Chairman CARDIN. Will we get those reports from what your red teams find?

Ms. SPRAGUE. I think we can arrange for that.

Chairman CARDIN. Senator Kyl.

Senator KYL. Thank you——

Senator FEINSTEIN. Thank you, Senator Kyl.

Senator KYL. Sure, you bet.

There are so many questions here. This may seem a little scattershot, but let me just fire away here. One of the things that Mr. Ford's report says is that the limitations in the access to interagency information contribute to vulnerabilities related to processes. Do you concur with that?

Ms. SPRAGUE. I think that we get very excellent cooperation from our Federal partners. We work very closely with the Department of Homeland Security, with the FBI, and with other organizations. Our difficulties arise when we are attempting to assimilate and work with the data from the 50 States and the District of Columbia.

Senator KYL. So to the extent that he may be referring to State agencies, you concur, but you do not agree that limitations and access to interagency information—"interagency" sort of seems to me within the Federal Government. You would not agree with that aspect of the report?

Ms. SPRAGUE. No, I would not. I think that we get very good support from Homeland Security, from the intelligence community, everybody does——

Senator KYL. So there is no Federal data-base that you are not able——

Ms. SPRAGUE. No. Some of the Federal data-bases, we wish they were a little bit better than they are, but——

Senator KYL. But no limitations on access to them.

Ms. SPRAGUE. No limitations.

Senator KYL. Thank you. OK. You indicated you are in the process of designing a plan. You proceeded then to indicate a lot of other things that are already being done, but with regard to this plan, do you have an estimate of when that will be done?

Ms. SPRAGUE. I am sorry. I do not——

Senator KYL. One of the very first things you said when you began your testimony was that you are in the process of designing a——

Ms. SPRAGUE. Oh, OK. We are going to have—we have the preliminary reports of the working group are being done this week. We have our regional directors here in town. They have done some outstanding work. I have had a pre- briefing from the five groups. I think we will be moving forward on implementing most of those recommendations before the end of the summer, some of them even sooner than that.

Senator KYL. You will let us know when that has occurred and provide that to us.

Ms. SPRAGUE. Absolutely.

Senator KYL. Thanks. You said that you cannot refuse to issue a passport if there is no Social Security number supplied. Is that correct?

Ms. SPRAGUE. That is correct.

Senator KYL. What is the reason for that?

Ms. SPRAGUE. Because we do not have legislative authority to do that.

Senator KYL. What legislative authority do you have to deny a passport?

Ms. SPRAGUE. Someone is not a U.S. citizen or they are not a person who—they are not the individual—they are not applying in the correct name, obviously, identity, but also they——

Senator KYL. So it is the judgment that they are not a citizen or they should not be able to travel?

Ms. SPRAGUE. Yes. And there are also some other holds on the issuance of passports such as active warrants, if people have child care——

Senator KYL. OK. So they—excuse me for interrupting here, but so the bases for denial certainly could be that there is no valid Social Security number supplied, but you cannot deny it simply based on that fact. Is that what you are saying?

Ms. SPRAGUE. That is what I am saying. The lack of a Social Security number is considered a very significant fraud indicator.

Senator KYL. Right.

Ms. SPRAGUE. And it immediately subjects the application to additional scrutiny.

Senator KYL. OK, or at least should have and will in the future.

Ms. SPRAGUE. Absolutely.

Senator KYL. Is the same thing true with regard to a driver's license? Because you said that mostly for identity purposes you rely on driver's licenses.

Ms. SPRAGUE. Driver's licenses are a serious problem for us, and we have been working with, for example, the American Association of Motor Vehicle Administrators and seeking to have access to a data-base. There is a law enforcement data-base. The Bureau of Diplomatic Security is working on getting us access to it.

For our purposes, we would like to have front-end access so that all that information is available to the adjudicator before they start. At this stage, what it appears would be the only thing available to us is query access, which does not give us as good a feeling as it would be if we could check everything, as we do with warrants, for example.

Senator KYL. Failing to prove identity of proving the wrong identity is a basis for refusal.

Ms. SPRAGUE. Absolutely.

Senator KYL. Using the driver's license is one of the key things that you use to determine identity.

Ms. SPRAGUE. Yes.

Senator KYL. Theoretically, you could identify a person through some other means and still issue a passport. Is that what you are saying?

Ms. SPRAGUE. Well, not everyone has a driver's license.

Senator KYL. Right. So the answer is, yes, theoretically you could.

Ms. SPRAGUE. Yes.

Senator KYL. OK. What would be the impact if the REAL ID requirements were loosened in some way?

Ms. SPRAGUE. I will candidly tell you I am very disappointed at the idea that we will back away from some of those requirements. We were very enthusiastic about tougher standards for driver's licenses.

Senator KYL. One thing. Based on the comprehensive immigration bill that I helped to draft a couple years ago, the two-stage

process of checking the Social Security and then verifying the identity of the individual based upon a visual check of the driver's license. One of the ideas that had come out of that was that there is some kind of association of State driver's license bureaus, whatever that is called, and that it should be possible to get that group to compile all of their information together for at least an accessing of information, if not pre-access to it.

Are you aware of that? Or is that what you were referring to?

Ms. SPRAGUE. We are aware of that, and we have been in touch with the American Association of Motor Vehicle Administrators, and they are doing work in this area. However, they are encountering significant difficulties because of privacy requirements on a State-by-State basis.

Senator KYL. Could you, as a part of the follow-up to this hearing, give us a little memo on what you would like to see there, how it might be useful to you, what problems you are encountering?

Ms. SPRAGUE. We would be delighted to do that.

Senator KYL. I appreciate that. You talked about the facial recognition tool and said that you hope to have that in effect by the end of the year. But that is only for a certain number of people or, I guess, as a pilot or what?

Ms. SPRAGUE. We are hoping to have the whole program in place, and we will be using some of the technology that we have developed over the years working with visa applicants. The State Department has been doing that for a long time, and we are going to draw upon the expertise of those people.

It is a daunting technical challenge because we are going to be screening these pictures against a 92-million-file data-base, and that can be very daunting. And we are going to have to figure out how we are doing it.

As a first step, which we hope to implement even sooner, we will be doing facial recognition against the fraud information that we have in our own fraud library, and that will be step one.

Senator KYL. But that is not in every case.

Ms. SPRAGUE. You would only catch people who were known to be frauds.

Senator KYL. Yes, right.

Ms. SPRAGUE. The repeats, such as the ones we had in this, will not come about until we get the full facial recognition.

Senator KYL. And you hope to have that by the end of the year, but it is only the first type of facial recognition, then you are going to make it more—well, you describe to me what it is. I am still not sure.

Ms. SPRAGUE. The fraud—the hit on the fraud——

Senator KYL. That is all you will have by the end of the year?

Ms. SPRAGUE. We hope to have by the end of the summer. The larger program we hope to have by the end of the year.

Senator KYL. OK, and describe the "larger program."

Ms. SPRAGUE. The larger program would be that trained specialists at the National Visa Center in Kentucky would be looking at the application before it comes to the adjudicator, reviewing it against the hits that come out of the system, and saying this likely——

Senator KYL. What hits would come out of the system?

Ms. SPRAGUE. They would be looking for look-alikes, and they have a technology in which they try and do that facial recognition and identify characteristics and present people who are possible matches. The applicant applies——

Senator KYL. Can I just take one more minute here on this? The applicant applies and presumably has a driver's license with a photograph?

Ms. SPRAGUE. We are using the photograph that he has submitted in connection with——

Senator KYL. With the passport, OK. And then you run that against a data-base——

Ms. SPRAGUE. Of 92 million records.

Senator KYL. OK. And that data-base, does it purportedly have in it all of the driver's licenses that have been issued in the country?

Ms. SPRAGUE. No. It has passport photos, and we would be reliant on passport photos to do this check.

Senator KYL. So it would be past passport photos.

Ms. SPRAGUE. Exactly.

Senator KYL. So if somebody had a previous passport and it was validly issued, you should have a match.

Ms. SPRAGUE. Exactly.

Senator KYL. If they had a previous passport invalidly issued, you would still have a match.

Ms. SPRAGUE. Yes, if they were applying now under a different name, there would be a match to the picture.

Senator KYL. And that would not show up as a "to be checked" item in that case.

Ms. SPRAGUE. Absolutely—well, if you have not—if we had a picture come up——

Senator KYL. If it is a different name.

Ms. SPRAGUE.—With a different name and it was the same person, that would be an absolute——

Senator KYL. Double-check it.

Ms. SPRAGUE. Yes.

Senator KYL. Yes, OK. All right. And I gather at some point you would hope to be able to check it against driver's license photos. Is that correct?

Ms. SPRAGUE. I do not know that we would want to go that far because I do not know we would have access to that kind of record. What we would very much like to do is be able to take the driver's license number and check it against a data-base that would give us the picture, and then we could compare that to the passport photo. That would be a wonderful——

Senator KYL. And if I just could, Mr. Chairman, in the bill, again, on the comprehensive immigration reform, which was not passed, that is exactly the system that was set up, that the Association of Motor Vehicle Departments would house the photos of all the people with driver's licenses, and when the applicant for a job came to the individual and the computer screen showed—you punch in the driver's license information, it would show the driver's license photo taken on the day that the driver's license was issued, and the individual would then have the opportunity to match vis-

ually the photograph on the driver's license with the individual standing in front of him or her.

Ms. SPRAGUE. Yes.

Senator KYL. Is that a potential way to help resolve this situation?

Ms. SPRAGUE. Obviously, that would be terrific.

Senator KYL. Could you, in that little short memo I asked you to do for us, discuss that possibility for us?

Ms. SPRAGUE. Yes.

Senator KYL. Thank you very much.

Ms. SPRAGUE. Happy to do that.

Chairman CARDIN. Thank you, Senator Kyl.

I just want to expand on that. I want to give you an opportunity. If there is a need for us to strengthen the laws on passport issuance, we want to hear from you. So if you believe that the law is inadequate as it relates to those people who have Social Security numbers and providing information for you to do an adequate check, then let us know so that we can consider strengthening the law. Or if you do not have adequate resources to get this job done, we want to know about it. So maybe I can just tag onto Senator Kyl's request, make his memo a little bit longer and include those points. But if there is a need for us to consider changing the law, or if you do not have the resources to get the job done, we want to know about it.

Ms. SPRAGUE. Our most striking need is to have better access to State data-bases—death, birth, and also driver's license. If we could have that, it would take us a long way. It would not solve all our problems because you do not necessarily have a direct link between a birth certificate and what happens to an individual later on. But it would certainly enable us to know that a certificate was issued in this name at that time and that the number matched to a number in their system.

Chairman CARDIN. And Senator Feinstein alluded in her opening comments to data banks being created in this area. Can you give us the status on births? What is the status?

Ms. SPRAGUE. The National Association of Public Health Statistics Information Systems has been given a grant by the Department of Homeland Security to create a consolidated data-base of all the 50 States and the District of Columbia, and they are hard at work on that. They anticipate that that will be available for all the 50 States and the District of Columbia by 2010. We are working with them. They have given us access, and we are routinely accessing those States which are already participating, but it is not a complete list. It is not even half. And we have actually worked with them to approach some States to accelerate because these are States in which we have a very high number of people applying, and we would very much like to verify it. And they are working with us on that, but we are not there yet.

Chairman CARDIN. And it is on track now for 2010?

Ms. SPRAGUE. They tell us December of 2010.

Chairman CARDIN. The end of 2010. And on the driver's licenses, you have already covered a good part of this, but with the current requirements for driver's licenses, that, of course, will be imple-

mented over the next several years, absent further delays. Will that give you better access for verification of identification?

Ms. SPRAGUE. It would give us greater confidence in the documents that we do see, but the ability to verify that these are validly issued driver's licenses would still rely upon a national database. When we have spoken to the people from the American Association of Motor Vehicle Administrators, they have given us a rather bleak assessment of when such a data-base would be available.

Chairman CARDIN. Is there a commitment to have a national data-base?

Ms. SPRAGUE. The law enforcement community does have a national data-base. It is not available to us at this time. But the Bureau of Diplomatic Security is acting as a sponsor for us to have access to it.

Chairman CARDIN. Is there a reason why you should not be able to do a Social Security number check with everyone who has Social Security numbers?

Ms. SPRAGUE. No, there is not.

Chairman CARDIN. But currently that information is not necessarily given to you?

Ms. SPRAGUE. It is given to us in the 24-hour batch processing, and we have it within 24 hours after we submit that information to the Social Security Administration.

Chairman CARDIN. And you are implementing a process that that check must be returned before the passport can be issued.

Ms. SPRAGUE. Yes. Our Inspector General just completed an investigation, an ongoing audit of our activities, and they recommended that we stop the process if there is any Social Security problem, and we are responding to the OIG's recommendation.

Chairman CARDIN. I am not sure we all agree with Senator Feinstein that there should be no exceptions to the rule, but I think we all agree that there has got to be some really good reason for issuing a passport if you have not gotten the information back. It should not be a routine decision made because of time or those types of considerations. We have to have confidence that the person has cleared the basic data checks.

Ms. SPRAGUE. At the present time, we have restricted same-day issuances, which would be the only instance in which we would issue such a—we would issue before the 24-hour batch to truly life-and-death emergencies. And we have the ability, even for those, to get an instant check with this Social Security Death Master File, so that no one is getting a passport until that check is completed.

Chairman CARDIN. And I would ask that you would share with our Committee, with our staff, your internal audits that you do or inspections that you do so that we have an understanding of where we are in that process. I think that would be helpful for us to be able to get that information, and I appreciate your willingness to make that available to us.

Let me just tell you, I think your first response to the first question I asked was a very telling response and one that I really sincerely appreciate, because obviously this is a very difficult situation for dedicated people who are working very hard, and we are all very concerned about it.

I would just make one final observation, and that is, you know, we are under pressure to allow other countries more liberal access for their citizens coming into America, and we base that upon their reliability and the people who come here as being eligible to visit our country. And I think that if we would have seen this type of a survey from one of the countries that was seeking visa waiver, we may have been very reluctant to grant that country a visa waiver. So this is a very serious issue, and I think your first response indicated that, and we want to work with you to get this corrected. We know how important a passport is to a person who is applying for it, so it is a very anxious moment until they get that passport in their hands. We understand that, particularly if they have vacation plans. So we want to work with you to make sure we can get this done as efficiently as possible, but we cannot compromise our national security.

Senator Kyl.

Senator KYL. Thank you.

Back to the use of the Social Security numbers, according to the GAO report, in the last 6 months before the end of 2008, close to 72,000 applicants received passports without supplying a Social Security number. Why did that happen?

Ms. SPRAGUE. In looking at the records quickly—and I cannot tell you we did a complete audit review, but we did look at it quickly—most of those were children under the age of 1. It was out of a universe of 6-million-plus passports, I believe, and most of those were children or people living abroad who had never acquired a Social Security number.

Senator KYL. You talk about a batch process. Is the reason why this takes overnight because you bundle them all up and send them in all at once?

Ms. SPRAGUE. It is the way we best interface with Social Security to provide data of that volume.

Senator KYL. OK. Well, you know that the E-Verify system works almost on a real-time basis. If I am an employer and I want to check the Social Security number of an applicant, I take the information from him, type it into the computer, it goes to Social Security, and within a matter of seconds I get the information back, it is a match or no match. Why can't you do that?

Ms. SPRAGUE. We don't do it for two reasons. First of all, because we want to make sure that it is done, and so that is the reason that we want it to be available to the adjudicator before he even starts.

Second of all, by going through the batch process, they give us a lot more information. When you go with the E-Verify process, which is the other alternative that they can offer, they give you a match or a no-match. We get information—and I am not as up on this as I should be. But we will get information, for example, that will indicate to us that a number has been transposed, and we can look on the screen and see that someone read a 7 as a——

Senator KYL. OK, so if you had to——

Ms. SPRAGUE. So that has been very useful to us.

Senator KYL. If you had to, you could use it in the E-Verify system and get an immediate response, but you get more useful information by taking the 24-hour period.

Ms. SPRAGUE. Exactly.

Senator KYL. OK. Thank you.

Ms. SPRAGUE. Exactly.

Senator KYL. The only other thing I wanted to ask you to do, you answered my question that reducing the requirements under REAL ID would be a real problem. I have forgotten—I do not mean to put words in your mouth, but it was——

Ms. SPRAGUE. We are extremely disappointed.

Senator KYL. Extremely disappointed in any effort in that vein.

In the ever lengthier memo that we are asking you to send us, could you just describe the reasons for that, what your concerns really are and the reasons for that? Because there is still a lot of debate about exactly what we should do with that, and I think your weighing in, indicating how important it is to have good information there, could be influential with colleagues who may simply not be aware of the reasons why the State Department needs to have this information.

Ms. SPRAGUE. I would be delighted.

Senator KYL. Great. That would be much appreciated.

Thank you, Mr. Chairman.

Chairman CARDIN. Thank you.

Thank you, Ms. Sprague. We appreciate your testimony. We appreciate the work that you all do, and we look forward to working with you.

Ms. SPRAGUE. Thank you, Senator.

Chairman CARDIN. Mr. Ford, we have the GAO report to Congress that was made available at the request of Senator Feinstein and Senator Kyl. The report will be made part of our Subcommittee record. We thank you for the work that you have done in this area, and we look forward to hearing your testimony.

STATEMENT OF JESS T. FORD, DIRECTOR, INTERNATIONAL AFFAIRS AND TRADE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Mr. FORD. Mr. Chairman, members of the Subcommittee, thank you for the opportunity to discuss our recent work on significant fraud vulnerabilities in the passport issuance process. My testimony today will highlight the results of our March 2009 report, which you just referred to, and also will summarize a letter we sent to you in April which catalogued a number of suggestions that we had for the State Department to try to remedy some of these vulnerabilities.

As you know, a passport not only allows an individual to travel freely in and out of the United States, but it also can be used further as an identification document to prove U.S. citizenship and set up bank accounts, among other things. Because passports issued under a false identity help enable individuals to conceal their movements and activities, there is great concern that passport fraud could facilitate acts of terrorism. Further, passport fraud facilitates other crimes such as illegal immigration, money laundering, drug trafficking, tax evasion, and alien smuggling. Malicious individuals may seek to exploit vulnerabilities in the State Department's current passport issuance process by using counter-

feit or fraudulently obtained documents as proof of identity and U.S. citizenship.

In March of 2009, we reported on the results of our investigation into the vulnerabilities of State's passport issuance process. Specifically, our undercover investigator was able to easily obtain four genuine U.S. passports using counterfeit or fraudulently obtained documents. We attempted to obtain the four genuine U.S. passports by using counterfeit or fraudulently obtained documents, such as birth certificates and driver's licenses, and Social Security numbers of fictitious or deceased individuals. In the most egregious case, our investigator obtained a U.S. passport using counterfeit documents and a Social Security number of a man who had died in 1965. In another case, our undercover investigator obtained a U.S. passport using counterfeit documents and the genuine Social Security number of a fictitious 5-year-old child—even though the individual applying for the passport was 53 years old.

The results of our investigation confirmed that the State Department continues to struggle with reducing fraud risks that we had previously identified in reports we issued in 2005 and in 2007. In 2005, we reported that using stolen identities and documentation was a primary tactic of those who sought to obtain a U.S. passport. We also reported weaknesses in the State Department's information-sharing system. For example, we reported that State did not receive information about U.S. citizens contained in the Federal Government's consolidated terrorist watch list, and the State Department did not routinely obtain the names of other individuals wanted by both Federal and State law enforcement authorities. We also found that the information that the State Department received from the Social Security Administration was limited and did not include access to Social Security death records, although State Department officials said at the time they were exploring the possibility of using these records.

A little over 2 years later, in July of 2007, we reported that the State Department lacked a formal oversight program over its 9,500 acceptance agencies and noted that State lacked a formal oversight effort to ensure that the individuals who worked in these facilities—primarily postal offices—had adequate controls to ensure that fraud was not perpetrated by applicants.

The State Department, as you have heard, has responded to many of the vulnerabilities that we recently reported. With regard to adjudication, the State Department told us that human error and a lack of access to information contributed to failures to identify our recent undercover tests. According to the State Department, passport specialists did not wait for the results of a required Social Security data-base check before approving our fraudulent applications.

In all four of our tests, State failed to identify the fraudulent birth certificates that we used. State officials attributed these failures to a lack of access to the State-level vital records data that would have allowed them to verify the authenticity of the birth certificates. State officials indicated they were exploring ways to access vital records and the Department of Motor Vehicle records nationwide to help address this problem.

In the case of our most egregious application in which we fraudulently obtained a passport using the Social Security number of a man who had died in 1965, State officials said that the lack of an automated check against Social Security death records had been a longstanding vulnerability in the passport system. In an attempt to provide automated death record information in all cases reviewed during the adjudication, passport officials told us they recently purchased a subscription to the Death Master File, which includes weekly updates of deaths recorded by the Social Security Administration.

With respect to the passport acceptance process, State officials told us they are working toward improving oversight of the passport acceptance facilities that we had recommended from our 2007 report. They said that in September of 2008, they announced a new oversight program, and they are currently in the process of staffing that office to provide oversight over all of the acceptance agencies.

In addition, the State Department told us they have taken several actions with respect to our undercover investigation. As was mentioned, they suspended the adjudication authority of the passport specialists responsible for approving the fraudulent applications and the authority of the facilities that accepted the applications. It revised the performance standards for passport specialists to eliminate production targets while all other aspects of performance standards were left intact. The State officials added that Passport Services will be conducting a study working with its union to develop new targets.

In conclusion, Mr. Chairman, we made several recommendations to the Secretary of State to help reduce the vulnerabilities, and I will quickly just cite these, and we can discuss these further.

No. 1 is they certainly need to do more training and devote more resources to the whole issue of passport fraud, particularly with detecting false and counterfeit documents.

Second, we recommended that they explore using commercial options to providing real-time checks on the validity of Social Security numbers and other information on applicants.

Third, we recommended that they develop what we call "red teams" to do intrusive tests similar to our own to test their system to make sure that the system does not have the same vulnerabilities that we identified.

We also indicated that they should work with State-level officials to gain better access to the key information that they need on driver's licenses and vital statistics to help ensure that the documents they receive are authentic.

We also recommended that they wait 24 hours before they approve passports from Social Security except under extenuating circumstances.

With that, Mr. Chairman, I would like to stop and answer any of the questions you may have.

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

Chairman CARDIN. Senator Kyl?

Senator KYL. Mr. Chairman, thank you for letting me go out of order here. I am going to have to leave in just a moment. But I wanted to thank you, Mr. Ford, and thank the folks that you work

with that produced this report. It is very valuable to us, and one has to wonder if you had not done this and brought these matters to the attention of the State Department, would they still be making the same errors that they were making that your report verified?

While I have a lot of questions, I may submit one or two to you for the record. I would like to just highlight one matter and ask for you to respond for the record. You do not need to do it right now. But if you share the same view that weakening the REAL ID driver's license requirements would be a bad thing, as the previous witness, could you expound on that a little bit in a written response to the Committee?

Mr. FORD. I would be happy to do that. I think in general we would—given what has happened here in terms of using fictitious driver's licenses, clearly this is an issue.

Also, I might add that in one of our tests, we did obtain using counterfeit documents a D.C. ID and used that as part of our test. So we have at least one example where we were able to obtain an authentic D.C. Government identification document, which we in turn used to acquire one of the passports.

Senator KYL. I really appreciate it. Thank you very much, and, again, I apologize for having to leave, but I just got a notice that I have got to run. So thank you very much.

Chairman CARDIN. Thank you, Senator Kyl. I think you do raise a good point, though, about the identification documents that are used to support application for a passport. There may well be some follow-up that we need to do to protect the integrity of being able to obtain those types of documents. It does not relieve the passport office from its responsibility, but we do not want to see fraudulent documents being able to be obtained. You showed several vulnerabilities in the system, in addition to just the passport problem itself.

Would it be helpful for you to have access to the red team tests that the State Department indicates that they are going to be implementing? Would it be useful for—I have an idea that we are going to be asking you to do this again, and prior to that, I assume there is going to be some covert tests done by the State Department. Is it useful for you to have that information?

Mr. FORD. Absolutely. If we are asked by Congress to look into this matter, to the extent that we can see whether the State Department has done its own internal tests, we certainly would find that beneficial. Of course, we have our own investigative unit here in GAO, and we can certainly do those ourselves. And given the fact that many of these vulnerabilities we reported 4 years ago, certainly we are concerned about whether these tests need to be done. They need to be done more frequently than they currently are.

Chairman CARDIN. I believe I read in the report—and maybe I am inaccurate, so correct me if I am wrong. One of the things I found very troubling is that one of the applicants in seeking the application was pretty much assured that the passport would be ready pretty quickly and got the impression there was not going to be much of a review done.

I guess my concern is this is at least your third time down this road. Some of these recommendations are similar to recommenda-

tions that have been made in the past. I assume as a result of the prior investigations there were good-faith commitments made by the State Department to implement the type of changes needed. Is there something that you have seen in the response from the State Department this time that would give you greater confidence that the recommendations will be acted upon?

Mr. FORD. Well, first of all, let me say I applaud the fact that the Department took our investigation seriously. They met with our investigators. They met with those of us on the audit side at GAO, and they sincerely indicated that they needed to address the vulnerabilities that we found.

I would like to say that I have a high level of confidence that some of these vulnerabilities will be closed, but I will also say that we have been down this road before with them in prior reports. I think that it is clear that they did close some vulnerabilities that we reported in the past, but I am not sanguine about the fact that we will not have similar problems like this in the future.

I think there is an issue of vigilance that the Department needs to maintain, and I think there is also an issue of commitment, you know, that they make this part of their everyday way of doing business. And I think if they do that, there is a likelihood that we can reduce the risk of these types of things happening. But I am not sure we will ever get to a point where we can say with certainty that these risks will be 100 percent remedied by the Department.

Chairman CARDIN. We had received a statement from the National Vice President of the National Federation of Federal Employees telling us that there is tremendous pressure put on the workers here to process a large number of applicants, that there is a lot of community pressure for these passports to be issued, and that at least at one point there seemed to be quotas installed, although that has been denied as to any quotas existing today.

Did you find this in your report that there was pressure put on the employees to complete applications so that the numbers were adequate to meet the public demand?

Mr. FORD. That was not one of the focuses of our review. However, we have done some prior work related to the issue from last summer—or 2007 when the Department was under extreme pressure to process passports because of the delays, and the American public was quite concerned about being able to get their passports.

While that was not the focus of our review, we did hear instances of cases when passport specialists had indicated that they were under pressure to produce as quickly as possible the passports, to get them out.

I know that the union believes that the performance standards that the Department has placed on them, which have certain production goals—I am not sure how they rephrased them; I guess "goals"—of how many passports should be produced in a particular timeframe in their view affected their ability to do quality review for fraud. We have not examined that in detail, but I can say that there is definitely a tension there between the passport specialists who want to get the passports done quickly because of those performance standards and the issue of doing a quality review to make sure that the proper checks are made to ensure that there

is no fraud involved. So that tension certainly existed, particularly in 2007 when they were under the gun to get the passports out.

Chairman CARDIN. I appreciate that. I think there are two separate issues here. I just want to clarify this. If we had the best data bank information available today, the procedures being used by the State Department in issuing passports had such lack of control in it because of the 24-hour turnaround without doing the checks, it is likely that your four cases would have still been able to obtain fraudulent information. It was not the lack of information being out there. It was the process being used and the training of the individuals, and you point that out pretty clearly.

On the other hand, if we correct the first part, if we do all the due diligence, we need to have the adequate data bank in order to make this an efficient system and an effective system. And I think today we have heard how we can improve that. Certainly as it relates to driver's licenses, as it relates to birth certificates, we can certainly improve that type of information, and it would be extremely helpful to the future issuance of proper passports.

But I just really want to underscore the point of your study, which was the fundamentals were not there. They were not doing the necessary due diligence. And it was not the data bank failures; it was more the human failure in this case. Isn't that a fair assessment at this point?

Mr. FORD. Well, again, that is what the State Department told us. We did not investigate whose fault it was for not doing the check. We were told by the Department that it was human error, that they had not filed the checks. However, there was a lot of confusion about what the requirement is. Whether they actually have to wait the 24-hour period or not, whether or not they had a firm policy in place that said you must wait 24 hours, that part we have not really studied in depth. So I cannot say with certainty it is just a human error problem, if that is your question. That is——

Chairman CARDIN. No, I think you have answered it. Using your report based upon their response, it was predominantly a human error problem in the end, using their reaction to it. I know you have not studied how accurate their response has been.

Mr. FORD. Right.

Chairman CARDIN. But a lot of our testimony here has dealt with that issue as well as how we can improve the processing by having more reliable data banks accessible by the passport office to check births and check driver's licenses. We have it for Social Security numbers. That is there now.

Mr. FORD. Right.

Chairman CARDIN. So that could have been done. In at least two cases here, it was not done.

Mr. FORD. That is correct.

Chairman CARDIN. We know that because that information was there. On the driver's licenses and birth certificates, it is unclear whether they could have gotten sufficient information from the search.

Mr. FORD. Well, I think that is true, but I also think that there is also some training involved about, you know, looking at the documents themselves.

Chairman CARDIN. Absolutely.

Mr. FORD. You know, these are the ones we used. Some of these, you know, you can go on your home computer and make them, and, you know, it is not just checking the data-base. In some cases, the person who is accepting your application needs to do at least the rudimentary check to see whether or not does this look like a real birth certificate type document or not. And they ought to have some knowledge, particularly if they are in some State, what kind of birth certificates does the State issue.

It is a little more sophisticated than just, you know, doing a data check. The people who accept these applications need to have some training in authenticity of documentation, whether it be one of these or even driver's licenses, and they should be familiar with the types of documents that are available in the location where they operate.

So there is a training element to this that we have called for in our prior work—and I think it is still valid today—that we need to have trained people out there that have some general knowledge of what does a genuine document look like.

Chairman CARDIN. And that was your first recommendation, if I remember correctly, the proper training of the people who take these applications.

You raise a very, very important point, a very valid point, that at the end of the day, a good part of this will be the training of the person issuing the application as to whether there is something that does not seem right in this application, whether it is the way the document looks or other factors. And you need that human aspect to this, and training is critically important if we are going to be successful in dealing with it. That is all part of national—homeland security is based upon that type of observation by trained professionals.

We have to figure out—I assume the next time we do this test, we are going to try to test that again by using similar type documents and see whether, in fact, they have improved.

Mr. FORD. Yes.

Chairman CARDIN. Well, I thank you. This has been extremely helpful, and I will conclude this hearing where I started, and that is, you know, this is a matter of, I think, extreme importance for national security. We rely more and more on passports in this country. It is a standard that we demand from other countries if they want access of their citizens to America, and we have an obligation to make sure that our system is done in an adequate way. This report was very, very troubling, and I was pleased to see the State Department acknowledge that from the beginning. And we need to now all work together to make sure that the changes are put in place in order to protect the security of our country and the integrity of our passport.

We look forward to working with GAO as we move forward with additional work and working with the State Department so that we accomplish the objectives of the proper issuance of passports.

The hearing record will remain open for 1 week for additional questions and statements from Senators. I would ask the witnesses to respond in a timely manner to any additional written questions that may be propounded.

With that, the hearing will stand adjourned. Thank you all very much.

[Whereupon, at 3:58 p.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

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 a.m. EDT Tuesday, May 5, 20009

STATE DEPARTMENT

Significant Vulnerabilities in the Passport Issuance Process

Statement of Jess T. Ford, Director
International Affairs and Trade

GAO-09-681T

May 5, 2009

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our recent work on significant fraud vulnerabilities in the passport issuance process. My testimony today will highlight the results of our March 2009 report on undercover investigative tests, which confirmed the continued existence of significant fraud vulnerabilities in this process.[1] We also provided a letter to you in April 2009, describing our recent work on passport fraud and summarizing actions the Department of State (State) has taken to address the prior weaknesses related to fraud vulnerabilities we identified.[2] We have found that these vulnerabilities stem from people, process, and technology. For example, the lack of training and resources provided to people contributes to vulnerabilities in the detection of fraudulent applications and counterfeit documents. The limitations in the access to inter-agency information contribute to vulnerabilities related to processes. Finally, the lack of databases and information-sharing technologies contribute to vulnerabilities in the verification of passport applicants' records. I will also discuss the status of prior recommendations and suggested corrective actions we have made to reduce fraud risk in the passport program.

A U.S. passport not only allows an individual to travel freely in and out of the United States, but also can be used to obtain further identification documents, prove U.S. citizenship, and set up bank accounts, among other things. Because passports issued under a false identity help enable individuals to conceal their movements and activities, there is great concern that passport fraud could facilitate acts of terrorism. Further, passport fraud facilitates other crimes such as illegal immigration, money laundering, drug trafficking, tax evasion, and alien smuggling. Malicious individuals may seek to exploit vulnerabilities in State's current passport issuance process, such as a lack of due diligence on the part of examiners who screen applications, by using counterfeit or fraudulently obtained documents as proof of identity and U.S. citizenship to obtain genuine U.S. passports.[3]

[1]See GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C.: Mar. 13, 2009).

[2]See GAO, *Addressing Significant Vulnerabilities in the Department of State's Passport Issuance Process*, GAO-09-583R (Washington, D.C.: April 13, 2009).

[3]As required by State's instructions on the Application for a U.S. Passport, form DS-11, applicants must provide proof of U.S. citizenship and proof of identity, along with two recent color photographs and funds to cover the passport application fees.

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00032 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.002

My comments today are based on our previously issued reports, which we performed in accordance with standards set forth by the Council of Inspectors General for Integrity and Efficiency (CIGIE) and generally accepted government auditing standards.

Undercover Investigation Confirms Continued Existence of Significant Fraud Vulnerabilities in the Passport Issuance Process

In March 2009 we reported on the results of our investigation into the vulnerabilities of State's passport issuance process. Specifically, we reported our undercover investigator was easily able to obtain four genuine U.S. passports using counterfeit or fraudulently obtained documents. For this investigation, we designed four test scenarios 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). We then attempted to obtain four genuine U.S. passports by using counterfeit or fraudulently obtained documents, such as birth certificates and drivers' licenses, and the Social Security Numbers (SSN) of fictitious or deceased individuals. In the most egregious case, our investigator obtained a U.S. passport using counterfeit documents and the SSN of a man who died in 1965. In another case, our undercover investigator obtained a U.S. passport using counterfeit documents and the genuine SSN of a fictitious 5-year-old child—even though his counterfeit documents and application indicated he was 53 years old.

The results of our investigation confirmed that State continues to struggle with reducing fraud risks we have previously identified at both the application point and the adjudication point[4]. In 2005, we reported weaknesses in State's information sharing with federal and state agencies.[5] For example, we reported that State did not receive information on U.S. citizens listed in the federal government's consolidated terrorist watch list and State does not routinely obtain the names of other individuals wanted by both federal and state law enforcement authorities. We also found that the information that State received from the Social Security Administration (SSA) was limited and did not include access to SSA's death records, although State officials said they were exploring the possibility of obtaining these records in the future. A little over 2 years later, in

[4]Through a process called adjudication, passport examiners determine whether they 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. It also includes the examination of an application to detect potential indicators of passport fraud and the comparison of the applicant's information against databases that help identify individuals who may not qualify for a U.S. passport.

[5]See GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-477 (Washington, D.C.: May 20, 2005).

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00033 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.003

July 2007, we reported that many previously identified problems in the oversight of the acceptance facilities[6] persisted and noted that State lacked a formal oversight program for its acceptance facilities to ensure effective controls are established and monitored regularly.[7] We concluded more needed to be done because of the critical role acceptance agents play in establishing the identity of passport applicants, which is critical to preventing the issuance of genuine passports to criminals or terrorists as a result of receipt of a fraudulent application.

State Indicated It Is Taking Actions to Address GAO Reports

With regard to adjudication, State officials told us a lack of access to information contributed to the failures identified by our recent undercover tests. According to State, passport specialists did not wait for the results of a required SSA database check before approving our fraudulent applications. In all four of our tests, State failed to identify the fraudulent birth certificates we used. State officials attributed these failures to a lack of access to state-level vital records data that would have allowed passport specialists to verify the authenticity of the birth certificates. State officials indicated they were exploring ways to access vital records and department of motor vehicle records nationwide to address the lack-of-access issues. In the case of our most egregious application—in which we fraudulently obtained a passport using the SSN of a man who died in 1965—State officials said that the lack of an automated check against SSA death records has been a long-standing vulnerability of the passport adjudication process. In an attempt to provide automatic death record information for all cases reviewed during adjudication, Passport Services officials represented that they have recently purchased a subscription to the *Death Master File* which includes weekly updates of deaths recorded by SSA. Passport Services intends for the *Death Master File* check to supplement the other checks in the adjudication process and not replace the current returns from SSA. Further, we note that State issues passports to some individuals who do not provide SSNs, meaning that State cannot rely on an SSN check to identify all fraudulent applications.[8]

[6]Passport acceptance facilities are located at certain U.S. post offices, courthouses, and other institutions and do not employ State Department personnel. The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document (such as a driver's license) actually matches that applicant.

[7] See 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).

[8]According to State, between June 20, 2008, and December 22, 2008, a total of 71,982 applicants received passports without supplying their SSN.

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00034 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.004

With respect to the acceptance process, State officials told us that they are working toward improving oversight of passport acceptance facilities as we recommended in our July 2007 report. In that report we recommended that State establish a comprehensive oversight program for passport acceptance facilities. In September 2008, Passport Services announced the establishment of an Acceptance Facility Oversight Program within the Office of Passport Integrity and Internal Controls. According to State, the oversight program will include audits, monitoring, and reporting on each acceptance facility's adherence to Passport Service's national policies and procedures, and to make recommendations for corrective actions for any deficiencies identified throughout the application process. State plans to implement the program in phases from 2009 to 2013.

In addition, State officials also told us that they took several actions in direct response to our undercover investigation. State suspended the adjudication authority of the passport specialists responsible for approving our fraudulent applications and the authority of the facilities that accepted our applications pending additional antifraud training. It revised the performance standards for passport specialists to eliminate the production targets for 2009, while all other aspects of performance standards were left intact for quality and fraud prevention purposes. State officials added that Passport Services will be conducting a study and working with the union to develop new production targets. These targets will not be in place until 2010. State identified additional tools and systems that would help address vulnerabilities within the issuance process.

Prior Recommendations and Corrective Actions

Since 2005 we have made several recommendations to State to improve the coordination and execution of passport fraud detection efforts, including considering ways to improve interagency information sharing and strengthening fraud prevention training. We also recommended that State consider conducting performance audits of acceptance facilities, agents, and accepted applications. State generally concurred with our recommendations and implemented many of them.

Nonetheless, our recent investigation shows that serious vulnerabilities remain. The Secretary of State should ensure that our prior recommendations are adequately addressed and that all currently planned corrective actions are successfully implemented. We also suggested that the Secretary of State take the following corrective actions:

- improve the training and resources available to passport acceptance facility employees for detecting passport fraud, especially related to detecting counterfeit documents;

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00035 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.005

- 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;
- explore commercial options for performing real-time checks of the validity of SSNs and other information included in applications;
- 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; and
- 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.

Conclusion

In conclusion, Mr. Chairman, State officials have known about vulnerabilities in the passport issuance process for many years but have failed to effectively address these vulnerabilities. Although State has proposed reasonable oversight measures for passport acceptance facilities in response to our prior recommendations, it is too early to determine whether these measures will be effective. Our most recent investigation reveals passport specialists also face challenges. State has indicated that it takes the results of this investigation very seriously, and officials have said that they are taking agencywide actions. Given the potential exploitation of vulnerabilities in State's current passport issuance process by criminals and terrorists, State should take seriously its efforts to maintain the integrity of the passport issuance process to protect U.S. citizens and interests at home and abroad.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittee may have at this time.

For further information about this statement, please contact Jess Ford at (202) 512-4128 or fordj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00036 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.006

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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

Senate Committee on the Judiciary
Subcommittee on Terrorism and Homeland Security
Field Hearing
"The Passport Issuance Process: Closing the Door to Fraud"
Dirksen Senate Office Building
Room 226
Washington, D.C.
May 5, 2009
2:30 p.m.

Testimony of
Deputy Assistant Secretary of State for Consular Affairs
Brenda S. Sprague

Chairman Cardin, Senator Kyl, Senator Feinstein, and distinguished members of the Subcommittee,

I appreciate this opportunity to discuss the passport issuance process and the plans we have to address our fraud vulnerabilities. We take seriously our responsibility to protect U.S. borders and the integrity of the U.S. passport through vigilant adjudication. The Bureau of Consular Affairs (CA) works diligently to improve training, procedures, and oversight throughout the passport adjudication process. The outcome of the General Accountability Office's (GAO) recent investigation shows that we need to do more. We have already taken a number of immediate actions, and are in the process of devising a detailed plan to enhance our entire process and program.

As you already have been briefed, a GAO investigative team informed CA on February 10, 2009, that they had performed a probe of the passport issuance process. The team reported that a GAO investigator submitted four passport applications (three at local postal acceptance facilities and one at a passport agency) utilizing a combination of counterfeit or fraudulently obtained documents. All four applications resulted in U.S. passports being issued in error. The subsequent GAO report specifically identified two major/significant vulnerabilities in our process: one, that Passport Specialists were unknowingly approving applications before all information checks were

54246.009

completed; and two, Passport Specialists and acceptance agents did not recognize fraudulent documents.

CA immediately initiated a number of measures to address these vulnerabilities and to mitigate potential fraud in the future. Some measures taken or contemplated would be more appropriately discussed only in a closed session.

First, upon receiving information from the GAO regarding the four passports issued in error, we promptly identified each passport, and, in accordance with standard operating procedures, we revoked the passports and posted corresponding "lookout alerts" in our internal systems and with U.S. border officials and Interpol.

We suspended adjudication approval authority for the four Passport Specialists who issued the four GAO applications.

We suspended the authority of the acceptance facilities that accepted the three GAO applications.

We immediately provided counterfeit document detection refresher training to all passport agency managers and specialists. Bi-weekly "case study" meetings are being held by agency/center supervisors with the Passport Specialists regarding unfamiliar or fraudulent documentation received in the office. The GAO report was shared with passport agency staff to reiterate the importance of carefully reviewing identification and citizenship documents, as well as the information on passport applications, to detect fraud. In addition, we revised performance standards for Passport Specialists to re-emphasize the importance of quality adjudication and fraud prevention performance standards.

We instituted a 100 percent audit of all live applications. Passport Specialists were released from the audit only when they had demonstrated to their supervisors that they were processing work in full compliance with adjudication standards as related to both proper annotation and attention to possible fraud indicators.

We revised our procedures regarding the processing of same day "Will Call" service and routine cases. Additional supervisory oversight is required for all same day "Will Call" applications. Agencies/centers have been directed to complete all information checks prior to the issuance of the passport. These procedural changes enhance our ability to identify potential fraudulent applications or documents. Additionally, passport acceptance agents at post offices and courthouses, and Passport Specialists at our passport agency public counters, must now photocopy all identification documentation submitted by applicants so it can become part of the permanent passport application record.

Second, we created an Adjudication Policy and Process Review Working Group in mid-March to help further identify necessary improvements. This Working Group consists of five subgroups, which are:

- Restructuring of Adjudication Process and Oversight – This subgroup is reviewing the current adjudication program and working on recommendations to restructure our processes. Additionally, the subgroup is working on recommendations for a new adjudicative managerial oversight program.

- Adjudication Requirements and Standards – This subgroup is developing standardized desk and counter adjudication procedures. Additionally, it is developing standardized procedures for Passport Specialists regarding the use of the Social Security Number (SSN) and other commercial databases.

- Post-Issuance Audit – This subgroup is developing a statistically valid audit process for previously issued passports. The results from this audit will be used for future training purposes.

- Training Initiatives – This subgroup is identifying enhancements for fraud training for all Passport Specialists, Supervisors, and Fraud Prevention Managers (FPMs). It is reviewing the curriculum of the National Training Program (NTP), which we use for training our new employees, to ensure that it appropriately and thoroughly addresses the document verification requirements used by Passport Specialists. Also, the subgroup is identifying and recommending standard

requirements for on-the-job training for new hires once they complete NTP and begin working with "live" (unapproved) applications. Additionally, it is developing standardized fraud awareness training for our courthouse and post office acceptance facilities.

- Technology – This subgroup is identifying technical and procedural vulnerabilities to the integrity of the passport process. Additionally, it is working on recommendations for improvement to our automated systems through access to additional databases.

Formal recommendations from the subgroups are expected by summer 2009. Shortly afterward, they will be compiled, finalized, and forwarded for Department management approval.

Third, CA is already working on some long-term initiatives to address our process vulnerabilities. We are currently pursuing an initiative to combine the systems platforms for domestic and overseas passport adjudication and issuance to ensure consistency and improve overall quality control. The combined system will utilize as many automated adjudication checks as possible.

The GAO Report recommended that we work with state level officials to develop a strategy to gain access to their databases and incorporate reviews of these databases into our adjudication process. Prior to the GAO undercover test, CA officials had held ongoing meetings with federal and state government agencies regarding access to information and databases for citizenship and identity verification. As a result of the GAO's recent recommendation, I also sent a letter to all State Registrars asking for their assistance in providing the Department access to their birth and death records for verification purposes. We plan to vigorously continue this effort.

I appreciate the opportunity to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. We appreciate GAO's constructive recommendations and look forward to working with Congress and the GAO to produce the most secure passport possible. Let me end by assuring you that the Department is fully committed to a secure passport issuance process, and deterring and detecting fraud.

Mr. Chairman, thank you again for the opportunity to be here today. I will be pleased to answer any questions that you, the Ranking Member, and the other distinguished members of the Subcommittee might have.

United States Department of State

Washington, D.C. 20520

JUL 1 0 2009

Dear Mr. Chairman:

During her May 5 testimony before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security, Deputy Assistant Secretary Brenda S. Sprague committed to update the subcommittee regularly on the Department of State's continued efforts to close the door on passport fraud. The Government Accountability Office (GAO) report entitled "Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process," (GAO-09447), identifies corrective actions for the Department of State. The Department has been working diligently to implement the corrective actions listed in GAO's investigative report. This letter is intended to serve as the Department's first update.

The Department is fully committed to a secure passport issuance process, and detecting and deterring fraud. We appreciate the efforts of GAO and the Congress in helping us to strengthen our issuance process and the security of the physical documents.

Upon receiving information from the GAO regarding the four passports issued in error, the Department took immediate corrective actions to mitigate the potential fraud vulnerabilities. The Bureau of Consular Affairs (CA) instituted a 100 percent audit of all active applications and began refresher fraud training for all passport specialists. CA also improved its procedures to ensure the completion of all necessary electronic verifications prior to passport issuance. Additionally, CA created an Adjudication Policy and Process Review Working Group in mid-March to identify necessary improvements in the passport adjudication processes and formulate a Bureau action plan. CA is developing a strategy to gain access to additional state and federal databases, and incorporate reviews of these databases into our adjudication process.

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

54246.014

In response to the GAO undercover test, CA established a program requiring that adjudication supervisors audit 100 percent of all applications approved by specialists prior to issuance of the passport. This provided a vehicle for measuring the quality of the passport adjudication process on a large scale. When a sufficient sample of an individual specialist's work demonstrated that s/he was processing work in full compliance with established adjudication standards, including attention to fraud indicators, that specialist was no longer subject to the 100 percent audit program. CA plans to continue to perform frequent, unannounced quality check audits on all passport specialists.

CA is partnering with the Bureau of Diplomatic Security to explore the use of "red teams" to measure the quality of the adjudication efforts. The first phase will be implemented as a pilot program that would consist of unannounced testing of the processes and procedures for passport acceptance and adjudication. CA expects to identify individual and systematic vulnerabilities better, correlate lessons learned, facilitate debriefing and training to employees and management, provide constructive suggestions on systematic improvements to mitigate these vulnerabilities, and strengthen management controls. CA expects to begin the pilot in the Fall of 2009.

All passport field offices are now required to review the results of Social Security Administration (SSA) Death Master File (DEMF) checks prior to issuing a passport. Direct supervisory oversight is required for all same day "will call" applications. In November 2008, the Department upgraded the Travel Document Issuance System (TDIS) to remove any application with a positive "death hit" from the adjudication process automatically. Passport specialists have instructions to refer any case with a "death hit" to a supervisor for a second review.

In April 2009, CA introduced a "real-time" Social Security Number (SSN) "death check" into the arsenal of resources the passport specialist has available to verify applicant data. This feature is designed to assist passport specialists adjudicating same-day "will call" or emergency passports. CA obtains updated death record information through a weekly subscription with SSA and incorporates it into the Consular Consolidated Database. Adjudicators check the database to confirm that the SSN provided is not one belonging to a deceased person. In addition, SSNs for "will call" or emergency passport applications are checked against related information in commercial databases. All discrepancies are referred to a supervisor for a second review.

CA is working to integrate SSA's DMF into the TDIS automated process. Once deployed, TDIS itself will automatically provide "Death Status" information for applications. CA expects to complete integration of the Death Master File into TDIS later this year.

As a part of the Adjudication Policy and Process Review Working Group, CA is developing standardized fraud training for acceptance facility employees, with a focus on facial recognition and recognizing security features of genuine identification. CA is looking into providing reference materials on current acceptable identification documents to all of our acceptance facilities.

CA officials have held ongoing meetings with state government agencies regarding access to information and databases for identity and citizenship verification. We have reached out to the Department of Motor Vehicles and vital records offices in each state and territory to determine the feasibility of gaining access to their electronic databases.

The Bureau's efforts to gain access to key databases have met some resistance because of two general barriers. First, because CA is not a law enforcement entity, current laws restrict the provision of information to us. Second, the data that we would like to verify – driver's license and birth certificate information – are held at the state level. Each state has its own laws in place regarding the sharing of personal information. Some states are open to providing the information, while others are more reticent to release records. Additionally, many states have not made strides toward converting their records into an electronically accessible format. Given current budget shortfalls, few states have funds available to start or continue making investments in this type of technology.

We are pleased to report that the National Law Enforcement Telecommunications System (NLETS), a not-for-profit organization that is owned and governed by the states, has granted CA access to its system. NLETS manages a technology solution that accesses drivers' license information of all fifty states through a single communications portal. Access to this information will enhance our ability to securely adjudicate passport applications.

CA is working with state-level officials and law enforcement entities to develop a strategy to gain access to the necessary state databases and incorporate reviews of these data into the adjudication process. One very positive result is that CA has recently acquired access to the National Association for Public Health Statistics and Information Systems (NAPHSIS) database, known as the Electronic

Verification of Vital Events (EVVE). EVVE is used by all fraud prevention managers to verify the birth records of all suspect fraudulent applications. This system, designed to access vital event databases in all 50 states, currently allows for verification of birth certificates in 15 states. CA is committed to continue our efforts in strengthening citizenship and identity verification methods. We hope that, in turn, efforts among state agencies to strengthen document and process integrity will continue.

The Department fully supports initiatives that strengthen identity verification. We seek to improve the underlying quality and reliability of documents upon which passport specialists must rely to fulfill their responsibilities to adjudicate citizenship and identity efficiently and with a reasonable level of certainty.

We trust this information is helpful to you and other Members of Congress. We will continue to update you on our progress as we further our efforts to identify and mitigate fraud vulnerabilities in our passport issuance system. Please let us know if we can be of further assistance.

Sincerely,

Richard R. Verma

Richard R. Verma
Assistant Secretary
Legislative Affairs

STATEMENT OF

COLIN PATRICK WALLE

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

ON

MAY 5, 2009

On behalf of the National Federation of Federal Employees (NFFE) and the 100,000 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.

Summary of NFFE's Position on How to Address Passport Vulnerabilities

Closing the door on passport fraud requires a multi-pronged, comprehensive approach. There is no "magic bullet" or any single change in policy, practice or technology that will by itself end the vulnerabilities in the passport issuance process once and for all. There are solutions to the problem that can and should be implemented now, including changes in passport specialist job performance elements, changes in work culture, additional staffing and resources, better connections to other agency's databases, and improvements in the tools, training, and technology available to passport specialists. But what is also needed is constant vigilance and a change in the process used to develop passport fraud prevention and adjudication systems. Specifically, the input and voice of the passport specialists – the employees who are on the front lines and who actually do the job of passport adjudication and fraud detection – needs to be included in the process.

Background on Passport Vulnerabilities and Union Efforts

Between July and December 2008, the Government Accountability Office (GAO) applied for and successfully obtained four U.S. passports, out of four attempts, using fraudulent methods in order to test vulnerabilities in the passport issuance process, as reported in the GAO's March 16, 2009 report #09-447 titled, "Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process." A State Department spokeswoman told the *Washington Post* that the test "certainly opened our eyes" to problems in the passport issuance process. From NFFE's perspective, the GAO's tests did not reveal anything – they confirmed what we have been saying for years.

For over a decade NFFE has been advocating for changes that would enhance the integrity of the passport issuance process. This is the top concern of the employees we represent in PPT. These employees do the actual work of passport adjudication and fraud detection. They are proud of their efforts at maintaining the integrity of the process, but know firsthand that, unfortunately, it can be

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00049 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.019

all too easy for a criminal to fraudulently obtain a passport. The results of the GAO's test were not at all surprising to this union or the employees that we represent.

Criminals and terrorists attempt to commit passport fraud for a variety of reasons and through a variety of means. It serves no purpose to commit passport fraud as an end unto itself. Those committing passport fraud often do so either to flee from a past crime or to facilitate an ongoing or planned crime. They commit passport fraud through a number of means, including submitting counterfeit citizenship or identification documents, by posing as a "look-alike," or by using genuine documents (e.g., obtaining someone's genuine birth certificate, and then fraudulently applying for identification and then a passport in that identity).

Some fugitives have attempted to obtain a passport in their own true identities, without committing fraud in the passport application process, in order to flee from their crimes. The Consular Lookout and Support System (CLASS) is designed to prevent this from happening. The GAO examined vulnerabilities in the passport issuance process, including CLASS, in 2004 and 2005, which led to their report # 05-477 issued in June 2005 titled, "Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts." Among other things, the GAO found that 37 out of 67 fugitives' names that they randomly tested were not included in the CLASS and, indeed, that one of the fugitive's tested had actually successfully obtained a passport in his true identity despite having been wanted by the Federal Bureau of Investigation (FBI) for 17 months prior to the passport issuance. The vulnerabilities discussed in that report were also the subject of the Senate Homeland Security and Governmental Affairs Committee's (HSGAC) June 29, 2005 hearing titled, "Vulnerabilities in the U.S. Passport System can be Exploited by Criminals and Terrorists." Prior to that GAO report and HSGAC hearing, there were only 50,000 names of fugitives in the CLASS Namecheck system for passport applications. As a result of the work leading up to the report and hearing, DOS was able to establish a connection to the FBI and Terror Screening Center (TSC), adding about 1,000,000 names and aliases of fugitives to the CLASS Namecheck system. NFFE is proud of the fact that the whistle-blowing by our representatives directly led to the closing of this vulnerability.

What passport specialists experience on the job is a focus on production and meeting quotas, with too little time to diligently adjudicate and prevent passport fraud. Passport specialists receive too little training and have insufficient resources and tools at their disposal to catch fraudulent attempts to obtain passports. The employees that NFFE represents, and the management officials that

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.020

supervise and direct them, all care about the integrity of the process and desire to prevent every fraudulent attempt. But these good intentions have not been enough. There are systemic problems that have not been addressed, which create gaps that those committing passport fraud can exploit.

NFFE made repeated good faith efforts to address concerns directly to PPT and DOS officials. Those efforts were rebuffed and therefore we requested oversight assistance from Congress in 2004. The GAO report and HSGAC hearing in 2005 were helpful and did advance the cause of preventing passport fraud, but not enough was done by DOS subsequent to that to truly close the door. Since then, NFFE has continued to advocate for improvements through collective bargaining and other processes, but with only some success – and not enough to have helped prevent the GAO from successfully obtaining passports in their four test applications or, more importantly, not enough to stop hundreds of real criminals from fraudulently obtaining passports.

We applaud Senator Dianne Feinstein and Senator Jon Kyl for requesting that the GAO conduct the test of the passport issuance process. We applaud Senator Ben Cardin for holding this hearing to investigate the vulnerabilities and solutions.

NFFE's Analysis of the Vulnerabilities in the Passport Issuance Process

The vulnerabilities in the passport issuance process do include the problems with the Social Security Administration (SSA) database checks and counterfeit document detection discussed by the GAO in their March 16, 2009 report and their April 13, 2009 follow-up letter to Senator Kyl and Senator Feinstein, but the vulnerabilities run much deeper than that. As the GAO reported in 2005, most fraud is committed by persons using genuine citizenship and identity documents that were fraudulently obtained. While the problems identified by the GAO must be addressed, it is also important to keep in mind that they are just the tip of the iceberg.

The vulnerabilities in the passport issuance process include the following:

- Too little focus on fraud prevention in the passport specialists' performance elements, awards, and overall work culture
- Insufficient fraud detection training, information, and tools
- Insufficient permanent fraud prevention staffing

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.021

- Organizational and interagency information sharing roadblocks
- Insufficient oversight and restrictions on the passport acceptance function
- Failing to adequately seek out and consider employee input, through their union, when making changes to systems, applications, processes, and procedures

Too Little Focus on Fraud Prevention in Job Elements, Awards, and Work Culture

With millions of passport applications submitted each year, and with many citizens often needing their passports on an urgent basis, processing passport applications in a timely manner is a goal shared by employees, the union, supervisors, and managers. However, the focus on production should not come at the expense of making sure the job is done right. After all, the passport fee is intended to pay for a rigorous adjudication process. Yet, passport specialists repeatedly indicated to NFFE that there is too much focus on the quantity of the work at the expense of quality, and that the production quotas (24/hour for the GS-9 and GS-11 levels, for an average of 2.5 minutes per application) required them to rush through applications without enough scrutiny of the evidence and information. In a February 2009 survey, 95% of specialists responding stated that it was necessary to lower the production quotas in order to improve fraud prevention efforts. In a March 2007 petition, 85% of non-probationary specialists signed a statement stating that the "current numerical standards make our process too vulnerable to being exploited by frauds" and that "it is all too easy for someone to fraudulently obtain a passport…." In a January 2006 survey, 97% of specialists stated that the focus in adjudication is on the quantity of work instead of the quality, and 96% stated that the numerical standards do not provide enough time for diligent adjudication. In a smaller July 2005 survey, 96% of specialists stated that the quotas did not give them enough time to catch passport fraud and 94% expressed concern that we would issue a passport to a terrorist or criminal. The work culture focuses overwhelmingly on production and the job elements and performance awards system are skewed in that direction as well, with some troubling instances of disincentives to spend additional time examining evidence, or to refer them for additional investigatory steps. Simply put, because of the production quotas, the passport specialists do not have enough time to consistently detect indicators of passport fraud.

In the past, management at PPT has responded to this with the argument that almost every passport specialist meets the numerical quotas, so they must therefore be adequate. Yet, those very same

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.022

employees who are meeting the quotas have repeatedly rejected this circular reasoning, most explicitly in the March 2007 petition and in the July 2005 survey, in which 98% of employees stated that just because they work at the rate required by the quota does not mean that it gives them sufficient time to diligently adjudicate. The quotas measure how fast the work is produced, not how well it is done. The employees who approved the 4 GAO test applications – along with the employees who approved the over 100 applications from criminals using deceased identities referenced in that GAO's March 2009 report – were virtually all meeting or exceeding the quota. NFFE is hopeful that the welcome decision by Deputy Assistant Secretary Brenda Sprague to suspend the production quotas for 2009 signals a permanent new approach by management.

Insufficient Fraud Prevention Training, Information, and Tools

In its 2005 report, the GAO recommended that DOS "[e]stablish and maintain a centralized and up-to-date electronic fraud prevention library that would enable passport agency personnel at different locations across the United States to efficiently access and share fraud prevention information and tools." PPT has complied with the recommendation to establish a centralized online library, but has not consistently maintained it. For example, a counterfeit New York birth certificate was used in all 4 GAO test applications. While New York is the third most populous state in the U.S., there was no exemplar of the genuine New York state birth certificate in the library upon which the counterfeit GAO certificate was modeled and against which it could have been compared.

In its 2005 report, the GAO recommended that DOS "[e]stablish a core curriculum and ongoing fraud prevention training requirements for all passport examiners, and program adequate time for such training into the staffing and assignment processes at passport issuing offices." PPT has made great strides in its introductory training for beginner passport specialists, specifically the two-week long National Training Program (NTP) for new hires. However, there are now areas where those who went through the NTP adjudicate differently than those who did not. Also, there is still no established fraud prevention training curriculum for employees advancing through the GS-5/7/9/11 career ladder. In addition, the amount of fraud prevention training varies from one office to another and is not consistently provided, especially when workload levels are high.

PPT also relies too heavily on training constructed and taught by the DOS Foreign Service Institute. The quality of the courses and the caliber of the instructors are both excellent, but the problem is

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.023

that they are designed by and for those who adjudicate passport applications overseas (Foreign Service Officers) as opposed to focusing on domestic passport adjudication – despite the fact that approximately 95% of passport applications are submitted in the U.S.

When a traveler goes through security at the airport, a Transportation Security Administration (TSA) employee scans the identification of the traveler, usually using an ultra violet light (black light) to help view the security features in order to verify its authenticity. Over three years ago, NFFE requested that PPT provide black lights for all passport specialists. For three of its four tests, the GAO used a counterfeit identification document. UV lights would help prevent fraud by confirming whether a document is bona fide. NFFE understands that PPT is obtaining these tools now.

Implementing effective facial recognition technology would help to detect some forms of passport fraud, but to be truly effective that technology would have to be able to confirm that the person applying for a renewal is the same as the person pictured in a passport from years' earlier and not a look-alike. Facial recognition programs could possibly have detected the fact that the same GAO investigator applied for all four test applications.

Insufficient Permanent Fraud Prevention Staffing

The number of permanent fraud prevention program staffing positions is critical to detecting fraud. These personnel handle fraud referral casework from passport specialists and provide guidance and training. NFFE argued unsuccessfully against the decision by PPT to cut permanent fraud staffing positions effective in January 2004. The need for additional staffing was supported by the GAO, the DOS Office of Inspector General (OIG), and testimony provided at the 2005 HSGAC hearing.

In its 2005 report, the GAO recommended that PPT "[c]onsider designating additional positions for fraud prevention coordination and training in some domestic passport-issuing offices." In addition, the OIG recommended in November 2004, "[t]he Bureau of Consular Affairs should reestablish assistant fraud prevention manager positions in all large passport agencies and centers and determine whether such positions are needed at smaller agencies." Despite these recommendations, the permanent fraud prevention staffing in the Passport Agencies and Centers has fallen both in gross numbers and even more so in relative numbers. From 2002 to 2004, there were 28 permanent

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.024

fraud staffing positions to provide guidance and training to 450 passport specialists adjudicating a little over 7 million passport applications each year. In 2007-2009, there were only 26 permanent fraud staffing positions to go along with 1,300 passport specialists handling between 12 million and 18 millions passport applications. This limits the guidance provided to specialists, hampers fraud casework processing, and contributes to the problem of insufficient training and information.

Organizational and Interagency Information Sharing Roadblocks

The most obvious vulnerability confirmed by the GAO's test is the insufficient database check between PPT and SSA. The PPT check against the SSA database was not done on a streaming basis. The policy was to not wait for that check before issuance. When the check was done, it was not a comprehensive check against all SSA information (including the death database).

There are additional organizational impediments to closing the door on passport fraud. For example, PPT is but one part of the Bureau of Consular Affairs (CA), even though PPT is nearly three times the size it was less than a decade ago. The Foreign Affairs Manual (FAM) contains DOS policies. Volume 8 is now empty – it once held the passport policies promulgated by PPT, but now those policies are subsumed into the 7th volume, with changes cleared through extra levels of bureaucracy. The headquarters office in charge of leading the effort against passport fraud has transferred from PPT to CA to PPT and now back to CA again, and the office where it is now has a mixed mission of combating visa fraud and passport fraud. The Forensic Document Laboratory (FDL), which provides expert analysis of citizenship and identity documents, was part of the old Immigration and Naturalization Service (INS), which is now part of the Department of Homeland Security (DHS). At that time made sense, because INS employees were charged with examining thousands of varieties of citizenship documents (e.g., birth certificates from states, counties, and cities) for authenticity for travelers entering the U.S. With the advent of the Western Hemisphere Travel Initiative (WHTI), just a small handful of documents will be accepted as proof of citizenship upon entry into the U.S. (e.g., the U.S. passport book, passport card, etc.). PPT employees still view those thousands of varieties of citizenship documents while adjudicating passport applications, while the DHS employees at points of entry will look at less than a dozen.

Another organizational problem is the question of where applications are adjudicated. A decade ago, PPT relied on a regional system whereby applications, for example, from the eleven states in

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.025

the northwest would be handled by the Seattle Passport Agency (that was the largest region) – effectively, employees would be responsible for and experts on applications and fraud indicators from that region. DOS switched to a system of "megacenters" and workload transferred applications. So, an application from one region could be processed by an agency or center outside of that region – effectively, employees would be responsible for, but not experts on, applications and fraud indicators from all 50 states. The employees we represent are dedicated and hard working, but when one attempts to become a jack of all trades one often ends up as a master of none. This policy of workload transfers helped boost PPT's productivity but had a negative impact on fraud prevention rates, which NFFE documented anecdotally at first and then with hard statistics. The GAO confirmed this problem in its 2005 report, and recommended that DOS "[a]ssess the extent to which and reasons why workload transfers from one domestic passport-issuing office to another were, in some cases, associated with fewer fraud referrals, and take any corrective action that may be necessary."

There are also some federal/state information sharing problems that impede fraud detection efforts. The GAO submitted four counterfeit birth certificates with the test applications. How can PPT verify their authenticity? Only a state's vital statistics office can do that and while most work with PPT, not all do. Another concern is birth abstracts issued by California, which are no longer accepted by PPT because they show the place where the birth was filed as the place of birth: someone born overseas that registers the birth in California can receive an abstract showing birth in the U.S.

When passport fraud is detected by PPT, it is referred to Diplomatic Security (DS) for investigation. The DS agents do a great job of investigating passport fraud, but they have other missions, such as protecting foreign dignitaries visiting the U.S. Also, they must rotate through their duty locations every two years, which hurts continuity. When a passport fraud case is confirmed, it is not always prosecuted because federal prosecutors are understaffed and have to prioritize what cases to bring to trial. Those convicted of passport fraud too often receive minimal sentences.

Insufficient Oversight and Restrictions on the Passport Acceptance Function

The function of accepting and executing a passport application is critical – the employee performing this job is the first line of defense against passport fraud, and the only person who meets the

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.026

applicant face-to-face. NFFE believes this is an inherently governmental function, as the acceptance agent is determining and verifying the identity of the applicant. This view was shared by DOS up until the workload crisis of 2007, when DOS contracted out this function. The DOS then changed Volume 22, Chapter 51 of the Code of Federal Regulations to allow the use of contractors at DOS for this function, but without first providing notice in the Federal Register as required by the Administrative Procedures Act.

The overwhelming majority of passport applications are submitted through passport acceptance facilities, which are government offices such as post offices, clerks of court, or other state, county, or municipal government entities. The GAO submitted three of the four passport applications at acceptance facilities, which did not detect the counterfeit driver's licenses that were presented to them. Back in 2005, when there were about 7000 acceptance facilities, the GAO recommended that DOS "[s]trengthen fraud prevention training efforts and oversight of passport acceptance agents."

The number of acceptance facilities has since grown to approximately 9500 (employing tens of thousands of acceptance agents). We have heard that PPT is considering adding new auditing positions to increase oversight of the acceptance facilities, but four years after the GAO made its recommendation this has still not been realized. During the workload crisis of 2007, numerous training trips to acceptance facilities were cancelled. Some improvements have been made, including better quality control in certifying agents. However, at some point the question has to be asked: are there too many acceptance facilities to properly oversee?

NFFE has previously called for PPT to restrict or eliminate the use of "hand-carried" applications, which are applications executed at an acceptance facility and then transmitted to PPT by another person, often a private courier company that charges a fee to the applicant. The applications are of concern because they exit the internal controls employed by PPT, and the security measures in place are not sufficient. This vulnerability has been exploited by some fraudulent applicants.

Failing to Adequately Seek Out and Consider Employee Input Through Their Union

Most of the senior managers at PPT have either never adjudicated a passport application or have not done so in many years. The employees who do the job of adjudication are intimately familiar with the vulnerabilities in the passport issuance process. They knew about a number of problems with

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.027

CLASS, they knew about the problems caused by the policy of not waiting for the SSA match check to be completed, they knew about the insufficient training and information, and they knew about the lack of focus on quality. NFFE has communicated all these concerns to PPT.

Employee representatives have been included in some efforts by PPT management, including a reshuffling of performance elements in 2008, opportunities to comment on draft changes to the 7 FAM, and an ongoing effort to redesign the passport application form, all with positive effect. On the other hand, the computer programs and displays used by passport specialists, the passport application, passport policies, and even the passport design itself have all been changed without "user" input, to their detriment. There have been too many instances where the left hand of PPT doesn't know what the right hand is doing, but the employees do, and addressing their concerns years ago would have caused some (and perhaps all) of the GAO test applications to have been caught. More importantly, working with the employee representatives to address passport vulnerabilities would have prevented real passport fraud attempts from succeeding.

How to Close the Door to Passport Fraud

In order to effectively close the door on passport fraud, NFFE believes the following steps are necessary:

1. Change the process: involve employee representatives in the process of crafting solutions to vulnerabilities, and making changes to applications, systems, and policies. This does not require a role reversal; management would still be management. NFFE is seeking a seat at the table, not the seat at the head of the table.
2. Change the performance elements to put more focus on quality work and fraud prevention. This would help close the door on passport fraud by giving passport specialists the time they need to scrutinize applications and evidence for fraud indicators.
    a. Provide more time for adjudication by lowering production quotas
    b. Lower them again as additional checks and tools are added and required
    c. Eliminate senseless incentives to not refer applications to the fraud office
    d. Eliminate higher rating levels for spending less time on each application
3. Change the work culture to recognize and reward quality work and fraud prevention. This would help close the door on passport fraud by communicating to employees in very concrete terms that fraud prevention is a priority.

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.028

   a. Mandate minimum of 15% of awards dollars go to fraud prevention efforts
   b. Mandate minimum of 15% of awards dollars go to other quality work efforts
4. Fully implement the GAO's recommendations from June 2005 and the OIG's recommendations from November 2004. This would help close the door to passport fraud by improving training and information, and increasing permanent fraud staffing.
   a. Create a fraud detection training curriculum for the entire career ladder. Do not postpone training during busy seasons. Design training for domestic passport adjudication. Work with other government agencies to conduct cross-training. Analyze all applications issued in error and address those mistakes in training.
   b. Update the online fraud prevention library.
   c. Hire additional permanent fraud prevention staffing.
   d. Study the workload transfer issue and craft effective solutions.
5. Establish connection with SSA so that all passport applicants' names and SSN's are checked against the database for a match and for death status.
6. Establish better interagency communication between PPT and other government entities.
7. Obtain UV lights (and replacement batteries), and provide training on how to use them.
8. Consider legislation to declare the passport acceptance function inherently governmental. Bring 22 CFR 51.22(a)(4) into compliance with the APA by eliminating "and contractors."
9. Consideration should be given to making PPT its own bureau within DOS – and include the FDL within PPT – with control over training, policy (8 FAM), and fraud prevention.
10. Consider hiring additional DS agents, and additional Assistant United States Attorneys. Consider strengthening penalties for passport fraud.

Conclusion

The vulnerabilities in the passport issuance process have been known for years. The GAO reported on this issue in 2005. The GAO is again reporting on this issue in 2009. DOS and PPT should wait no longer. Action needs to taken, by DOS or by Congress, to address these concerns now. Implementing the steps outlined in this testimony will go a long ways toward closing the door on passport fraud.

VerDate Nov 24 2008 11:38 Jan 19, 2010 Jkt 054246 PO 00000 Frm 00059 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\54246.TXT SJUD1 PsN: CMORC

54246.029