Testimony of

Mark Duda

July 10, 2008

REMARKS OF MARK W. DUDA

ASSISTANT INSPECTOR GENERAL

FOR AUDITS

U.S. DEPARTMENT OF STATE AND BROADCASTING

BOARD OF GOVERNORS

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

ON

CONTROLS AND NOTIFICATION FOR ACCESS TO PASSPORT RECORDS IN THE DEPARTMENT OF STATE'S PASSPORT INFORMATION ELECTRONIC RECORDS SYSTEM

JULY 10, 2008

Chairman Leahy, Ranking Member Specter, members of the Committee, thank you for the opportunity to discuss the results of our review of controls over access to passport records in the Department of State's Passport Information Electronic Records System, which is known as the PIERS system.

On March 21, 2008, following the first reported breach of a presidential candidate's passport records and at the direction of the former Acting Inspector General, the Office of Inspector General, Office of Audits, initiated this limited review of Bureau of Consular Affairs controls over access to passport records in PIERS. Specifically, this review focused on determining whether the Department:

(1) adequately protects passport records and data contained in PIERS from unauthorized access and

(2) responds effectively when incidents of unauthorized access occur.

During Fiscal Year 2007, the Department issued almost 18.4 million passports domestically and participated or assisted in the issuance of about 365,000 passports overseas.

According to Consular Affairs officials, there were about 20,500 users with active PIERS accounts as of May 2008, and about 12,200 of these users were employees or contractors of the Department. PIERS is also accessed by users at other federal departments and agencies, including the Department of Homeland Security, the Federal Bureau of Investigation, and the Office of Personnel Management, to assist in conducting investigations, security assessments, and analyses.

In our review, OIG found many control weaknesses--including a general lack of policies, procedures, guidance, and training--relating to the prevention and detection of unauthorized access to passport and applicant information and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

In some cases, Department officials stated that the lack of resources contributed to the lack of controls and to the Department's ability to assess vulnerabilities and risk. OIG described some security and management practices utilized by the Internal Revenue Service and the Social Security Administration as examples where similar improvements can be made by the Department.

OIG made 22 recommendations to address the control weaknesses found with safeguarding passport records. We did not verify instances of unauthorized access, but it did conduct a judgmentally determined study at the initiation of this review to identify the frequency with which the records for 150 high-profile individuals were accessed in PIERS between September 2002 and March 2008. Our results revealed several patterns that raised serious concerns about the potential for undetected unauthorized access to passport records. Of the 150 names included in the study, OIG found that the records of 127 individuals, or 85 percent, had been accessed at least one time. The query results showed a total of

4,148 hits to the passport information for these individuals. OIG made no determination as to whether the hits represented authorized or unauthorized access. Further, although an 85 percent hit rate appears to be excessive, the Department currently lacks criteria to determine whether this is actually an inordinately high rate.

As stated by the Acting Inspector General, following the publicized passport record breaches, the Department implemented a number of corrective actions and has other efforts planned, as detailed in the report.

Of the 22 recommendations made OIG considers 19 recommendations resolved and three recommendations unresolved based on the responses by Department officials. To ensure that adequate and timely progress is achieved, we will conduct a follow-up compliance review of the Department's implementation of the recommendations in this report, as well as Consular Affairs' process for reviewing possible unauthorized accesses by users as identified in our study.

Thank you for the opportunity to appear before you today. I would gladly answer any questions you may have.