Testimony of

Harold Geisel

July 10, 2008

REMARKS OF HAROLD W. GEISEL

INSPECTOR GENERAL (ACTING)

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 inviting me to discuss with you the privacy concerns reported in the results of our review of controls over access to passport records in the Department of State's Passport Information Electronic Records System or PIERS system. The full report has been provided to the Committee.

In March 2008, media reports surfaced that the passport files maintained by the Department of State (Department) of three U.S. Senators, who were also presidential candidates, had been improperly accessed by Department employees and contract staff. On March 21, 2008, the Office of Inspector General, Office of Audits, initiated a limited review of Bureau of Consular Affairs controls over access to passport records, and issued the final report one week ago, on July 2, 2008. The OIG made 22 recommendations to address the control weaknesses and the Department concurred with 19 of them, partially agreed with one and did not agree with two recommendations.

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.

As of April 2008, PIERS contained records on about 192 million passports for about 127 million passport holders. These records include personally identifiable information or P-I-I , as it is known, such as the applicant's name, gender, social security number, date and place of birth, and passport number. PIERS also contains additional information, such as previous names used by the applicant, citizenship status of the applicant's parents or spouse, and scanned images of passport photos. PIERS offers users the ability to query information pertaining to passports and vital records, as well as to view and print original copies of the associated documents. As a result, PIERS records are protected from release by the Privacy Act of 1974. Unauthorized access to PIERS records may also constitute a violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

At the time of the publicized breaches, neither Consular Affairs nor the Department had implemented breach notification policies, procedures, or other criteria for reporting incidents of unauthorized access of passport records when they were detected. However, between March and May 2008, Consular Affairs and the Bureau of Administration took a number of corrective actions, including issuing interim guidance on the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to passport records and applicant personally identifiable information, and a Department-wide

P-I-I breach response policy.

While these immediate actions taken are commendable, OIG has recommended that the Department conduct the necessary vulnerability and risk assessments of all passport systems given the weaknesses and data vulnerabilities identified in this limited review of PIERS. Accordingly, OIG believes that the Department should make resources available to conduct the assessments as quickly as possible.

OIG also recommended that CA ensure the accuracy of its Privacy Impact Assessments for PIERS and for all other passport systems to accurately reflect security controls for and risks to personally identifiable information.

I would like to introduce Mr. Mark W. Duda, Assistant Inspector General for Audits, who led this review and will provide a summary of the findings.

Thank you for the opportunity to present this timely information to you today. Following Mr. Duda's remarks, we would be happy to answer any questions you may have.