



**U.S. Department of
Transportation**

Office of the Secretary
of Transportation

Office of Inspector General

August 9, 2006

Dear Member of the Florida Congressional Delegation and Chairs and Ranking Members of Department of Transportation Oversight Committees and Subcommittees:

I am writing to inform you of a recent incident involving the theft of a password-protected laptop computer containing personally identifiable information (PII). The laptop, assigned to a special agent in the Miami office of the U.S. Department of Transportation Office of Inspector General (OIG), was stolen from a government-owned vehicle on July 27, 2006, in Doral, FL.

The theft of the laptop was reported to me on July 31, 2006 and I learned of the presence of databases containing PII on this laptop on August 5, 2006. Since then, we have been conducting an intensive investigation to determine what information was contained on the laptop and to recover it as expeditiously as possible.

We have dispatched a team of special agents to the Miami area to work with the Miami-Dade Police Department in a full-scale effort to recover the stolen laptop. We also intend to establish a reward for information leading to its recovery.

Based on our review so far, the stolen laptop, which is password protected, contained at least four databases with PII information (such as names, social security numbers, dates of birth, or addresses) pertaining to: approximately 42,792 Florida residents holding airman certificates; approximately 80,667 Miami-Dade County area commercial driver's license (CDL) holders; approximately 9,005 individuals who obtained their personal driver's license information from the Largo licensing examining facility near Tampa; and, approximately 491 drivers who obtained their CDLs from the same Largo licensing examining facility.

For these individuals, there is no financial or medical information. Also, these databases were not lists of individuals under investigation but instead were general lists of license and airman certificate holders in the State of Florida.

Miami-Dade CDL holders who obtained their licenses after April, 2003, Florida pilots who obtained their airmen certificates after March, 2003, and drivers who obtained their personal driver's licenses or CDLs from the Largo facility after July, 2005, are not affected.

We are continuing to analyze a back-up of the laptop's hard drive that was made several months ago. As we determine if other PII information is contained we will make additional notifications.

OIG's Miami office was using the Miami-Dade CDL information and the Florida airman certificate information in connection with multi-agency task forces focusing on the use of fraudulent information to obtain CDLs or airman certificates. Past reviews have identified people ineligible to hold these certificates and licenses due to disqualifying criminal histories or the use of fraudulent social security numbers. The Tampa-area driver's licensing data was used as part of an ongoing investigation involving fraud at the licensing facility, which resulted in a guilty plea.

While we do not have reason to believe that the perpetrators targeted the laptop based on any knowledge of its data contents, we are nonetheless taking all possible steps to inform Florida residents. We will make every attempt to ensure that all affected persons are notified. We will be working with Members of Congress, Federal agencies, State and local agencies, the news media, and trucking and aviation organizations to further ensure that the individuals are aware of the situation and of the steps they may take to protect themselves from misuse of their personal information.

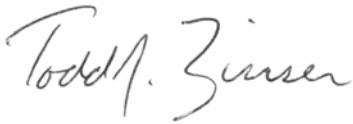
I have notified the Acting Secretary of Transportation, Maria Cino, and other senior Departmental officials, including the DOT Chief Information Officer, Daniel Mintz. We also made appropriate notifications to the Department of Transportation's Computer Incident Response Center, which, in turn, notified the Computer Emergency Readiness Team at the Department of Homeland Security (DHS). DHS, which is the lead Federal organization for Computer Security and Incident Response, is assisting DOT's efforts to minimize the impact of this incident. The Office of Management and Budget and the President's Identity Theft Task Force have also been notified.

We have taken steps to ensure that no other OIG laptops or portable media devices assigned to our field offices and headquarters employees contain such PII databases.

In order to further communicate with those who may be affected, we are maintaining a hotline at 1-800-424-9071 and providing information on our website at: www.oig.dot.gov. Our hotline is staffed 24 hours per day, seven days a week.

We regret this matter and take our responsibilities seriously. We have taken action and will continue to take steps necessary to prevent this from happening again. We will be providing you with updated information as we know more. If you have any questions concerning this matter, please feel free to contact me at 202-366-1959, or Charles H. Lee, Jr., Assistant Inspector General for Investigations, at 202-366-1967.

Sincerely,

A handwritten signature in cursive script that reads "Todd J. Zinser". The signature is written in black ink and is positioned above the typed name.

Todd J. Zinser
Acting Inspector General