U.S. Department of Transportation

Office of the Secretary of Transportation

Office of Inspector General
Washington, DC 20590

Wednesday, August 9, 2006

Contact: David Barnes
Phone: (202) 366-6312
david.barnes@oig.dot.gov

DOT Inspector General Alerts Florida Residents Regarding Stolen Laptop Containing Personal Information

The Office of Inspector General (OIG) at the U.S. Department of Transportation today announced that a laptop computer containing personal identification information of approximately 133,000 Florida residents was stolen from a government-owned vehicle on July 27, 2006 in the Miami, FL, area.

Based on OIG's review so far, the laptop, which is password protected, contains four databases with personal identifiable information (such as names, Social Security numbers, dates of birth, and addresses) of approximately 42,792 Florida pilots, approximately 80,667 Miami-Dade County CDL holders, and approximately 9,005 individuals who obtained their personal driver's licenses and approximately 491 drivers who obtained their CDLs from the Largo licensing examining facility near Tampa.

For these individuals, there is no financial or medical information on the laptop. 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.

Special Agents in OIG's Miami office were 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 prior criminal history 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 recently resulted in a guilty plea.

-more-

OIG special agents and the Miami-Dade Police Department are engaged in a full-scale effort to recover the laptop. While OIG does not have reason to believe that the perpetrator or perpetrators targeted the laptop because of any knowledge of the data contents, OIG is taking all possible steps to protect and inform Florida residents. People who believe their data might be at risk can call OIG's Hotline Complaint Center at 1-800-424-9071 or visit OIG's website at www.oig.dot.gov. OIG also intends to establish a reward for information leading to the laptop's recovery.

"We are making every effort to recover the stolen laptop and resecure the data it contains," said Acting Inspector General Todd J. Zinser. "We seriously 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."

OIG is working with members of Congress, Federal, State, and local agencies, and the news media to help ensure that at-risk parties are aware of the situation and the steps they may take to protect themselves from misuse of their personal information. Individual notification letters are being sent to at-risk Floridians to every extent possible.

All appropriate notifications have been made, including Acting Transportation Secretary Maria Cino and DOT Chief Information Officer Daniel Mintz. OIG has also made appropriate notifications to the Department'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.

OIG has taken steps to ensure that no other OIG laptops or portable media devices assigned to field offices and headquarters employees contain such data. The agency is strengthening its polices regarding laptop computers.

In order to further communicate with those who may be affected, OIG is maintaining a 24 hour-a-day hotline at 1-800-424-9071, which can also be accessed on the Internet at: www.oig.dot.gov.

###