

OIG Status Report

August 14, 2006

We are providing the following update on the Department of Transportation's Office of Inspector General activities regarding the reported theft of a laptop computer belonging to an OIG special agent in Miami, FL on July 27, 2006.

Response to Florida Members of Congress **Letter to Acting Inspector General**

On August 11, 2006, 16 Members of the Florida congressional delegation sent a letter to the Acting Inspector General, expressing their concerns about the loss of personally identifiable information of Florida residents, especially in light of other recent data thefts at other Federal Agencies. The Members requested a "detailed description of current procedures and protocol in handling this type of information and what steps and specific protocols are being implemented to ensure a massive breach does not occur again".

In response, the OIG is drafting a letter that will assure the Members that we will report to them the results of (1) our investigation of the incident, (2) our review of the adequacy of policies compared to existing requirements and whether our policies were appropriately followed, and (3) actions taken to strengthen our policies and controls to ensure that no similar incident can occur in the future. We plan to enlist the help of an outside contractor with expertise in computer security and privacy requirements to assist in the review of our policies and the development of new policies, as appropriate. We will also provide periodic progress updates to the Department and interested congressional staff.

Our current efforts are focused on:

Recovery Efforts

- We have a team of approximately 15 investigators on the ground in Miami. They are working with the Miami/Dade County police and other law enforcement agencies, which have provided important assistance in efforts to recover the stolen laptop.
- OIG investigators and local police have conducted more than 500 field interviews.

- We have handed out over 600 fliers announcing the reward for and providing a description of the laptop (including its serial number) to police stations, pawnshops, and used computer stores in the Miami area.
- OIG investigators and local police have visited more than 350 pawnshops in the Dade County area.
- OIG investigators and local police visited 12 flea markets on Saturday, August 12th.
- We reviewed the stolen/recovered property inventories for 8 local police agencies in the area and the Florida Highway Patrol.
- Via our website, we have directed victims to call our hotline to receive tips and advice on how to check their credit. As of Monday morning, we had received a total of 311 calls. Several calls provided tips which we have actively followed up on.
- We have offered a \$10,000 reward for information leading to the laptop's recovery and posted this on our website along with a description of the laptop and contact information.

Public Outreach

- OIG has posted open letters on our website for Florida residents who had certain PII information contained on the laptop. The letters are written in both English and Spanish.
- We are mailing out personal letters to individuals beginning August 15th to notify them of this situation and provide information on actions that they can take to prevent identity theft.
- We have recommended that affected individuals: contact one of the three major credit reporting bureaus to request that an initial fraud alert be placed on their credit record (which entitles them to one free credit report from each company); monitor bank and credit card statements and contact financial institutions to check for any suspicious activity on their accounts; be vigilant to any phone calls, e-mails, and other communications from individuals purporting to be government officials and “phishing” for or asking to verify personal information.
- We are encouraging anyone who suspects they may be the victim of identity theft to contact our hotline (1-800-424-9071), 24 hours a day.
- We are working with the General Services Administration and Department of Veterans Affairs to obtain information on credit monitoring services.

OIG Actions

- Once we obtained confirmation that the stolen Miami laptop contained PII information, we began to undertake our own investigation to determine the facts and circumstances surrounding the loss of this laptop as well as what follow-up actions were taken. We have two agents assigned full-time to this investigation.
- On August 3, OIG investigators and agents were instructed not to leave government laptops unattended in their vehicles, even if the vehicle is locked. All electronic storage media must be kept out of site. Any loss of computers or electronic storage media must immediately be reported to OIG HQ management and information security staff.
- On August 7, all OIG employees were instructed to remove all PII data from laptops and to ensure that all sensitive data is stored in encrypted folders. OIG managers are being directed to review the content of their employees' laptops and obtain a certification from each employee that their laptop does not contain PII.
- On August 14, the Acting IG held an all employee web cast to reinforce these safeguards.
- All OIG employees must also re-certify that they have read and understand Departmental and OIG guidance on computer security.
- Additional training for employees on Privacy Act requirements and computer security is being required for all OIG employees.
- Specific policies on PII are being established consistent with new DOT policies being issued in response to OMB's July 12, 2006, memorandum (M-06-19) directing Chief Information Officers to strengthen controls over PII data.