



One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 10, 2007

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, DC 20528

Dear Secretary Chertoff:

According to a May 5, 2007 report in the Washington Post (“TSA Hard Drive With Employee Data Is Reported Stolen”), the FBI and the Secret Service have initiated a criminal investigation into the apparent theft of a computer hard drive that contains personal, payroll and bank information of 100,000 current and former Transportation Security Administration (TSA) employees, including airport security officers and federal air marshals. This incident, coupled with TSA’s failure to secure a website designed to help travelers resolve potential cases of mistaken identity, suggests that TSA is inadequately and improperly securing sensitive information.

These data security lapses are unacceptable, and they reflect the Department’s dismal record in data privacy and information security. We are troubled by these two incidents and concerned that additional breaches may occur in the future. Therefore, pursuant to the Committee on Homeland Security’s oversight responsibilities as set forth in House Rule X, we request that the Department provide the Committee with the following information:

Theft of TSA Hard Drive

- (1) Was the information contained on the TSA laptop that is presumed stolen protected using encryption or alternative methodologies or technologies that render data in electronic form unreadable or indecipherable by unauthorized users? If not, why not?
- (2) What specific personal information did the missing hard drive contain?
- (3) How long does TSA maintain personal information belonging to former TSA employees?
- (4) Does TSA have a data retention policy for handling the personal information of its former employees? If not, why not? If it does, please provide the Committee with a copy of this policy.

Security Weaknesses on TSA's Watchlist Redress Web Site

- (1) From October 6, 2006 through February 14, 2007, the TSA watchlist redress website contained an insecure link. During that time, an estimated 200 users accessed the system through this link. Did the individuals whose information may have been compromised during this time period receive notification from TSA alerting them of the potential risk to their personal information? If yes, describe the method of notification.
- (2) Please provide the exact number of individuals that accessed the site during the time period in (1) above.
- (3) Please provide the number of individuals that received notification and the number of people whom TSA was unable to notify, if any. For those individuals for whom notification was not effective, please describe any and all additional means of notification employed by TSA.
- (4) If the method of notification was in writing, please provide a copy of the notification letter.
- (5) Please provide a listing of remedies (e.g., credit monitoring service) that TSA is offering to individuals who clicked on the insecure link.
- (6) Does the Department utilize a policy that prescribes the frequency of audits for its Web sites to ensure their security and accuracy? If yes, please provide a copy of this policy.
- (7) Was such a policy utilized prior to the detection of the security weakness at TSA's watchlist redress site?
- (8) How often are the Department's Web sites monitored for security and accuracy, and how is such monitoring performed? Please indicate whether this monitoring is achieved through automated tools solely or whether the process also includes human monitoring.
- (9) We understand that the development of the site was performed by a contractor, Desyne Web Services, Inc. Does TSA continue to contract the services of Desyne Web Services, Inc. for this website or any other TSA website?
- (10) If the contract with DeSyne is no longer in effect, please indicate when the contract became inactive and whether the conclusion of the contract was prompted by TSA. If the contract was concluded by TSA prior to the expiration of its term, please indicate the rationale for the termination.
- (11) Does the Department or any of its components utilize the services of Desyne Web Services? If yes, please provide the contract numbers and dollar values of those contracts.
- (12) TSA, through its online watchlist redress site, is collecting personally-identifiable information on a significant number of individuals. What data safeguards are in place to ensure that this information is secure? Is this information encrypted in transit and in storage? Is this information retained after an individual's case has been resolved? If yes, why, how long is the retention period and how is this information ultimately disposed of?

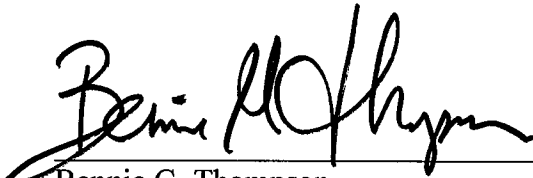
DHS Data Security Policies

- (1) Please provide a copy of the Department's data security policy with respect to the collection, use, dissemination, and maintenance of personal information (e.g., Social Security Numbers, first and last names, addresses, etc.)
- (2) Does the Department utilize a process for the disposal of obsolete data in electronic form containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable? If so, please provide a narrative describing this process. If not, why not?

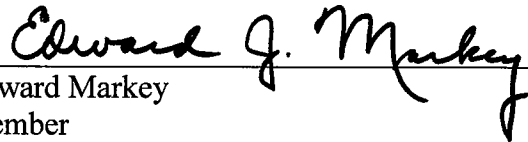
- (3) For the period from May 1, 2005 to May 1, 2007, please provide the following information:
- a. How many instances have occurred in which electronic data containing personally identifiable information maintained or collected by the Department was accessed by an unauthorized individual or individuals? For each instance, please provide the date of the breach and the actions taken by the Department to notify affected individuals and prevent a recurrence.
 - b. How many instances have occurred in which electronic data containing personally identifiable information maintained by the Department was lost or stolen? For each instance, please provide the date of the breach and the actions taken by the Department to notify affected individuals and prevent a recurrence.
 - c. In (a) and (b) above, how many of the individuals affected were Department employees?
 - d. What efforts did the Department undertake to notify the employees in question (c)? How and when were these individuals notified? If they were not notified, why not?

We appreciate your prompt attention to this matter. If you have questions, please have a member of your staff contact Cherri Branson, Chief Oversight Counsel on the Majority Committee staff at (202) 226-2616 or Mark Bayer, Deputy Chief of Staff, on Representative Markey's staff at (202) 225-2836.

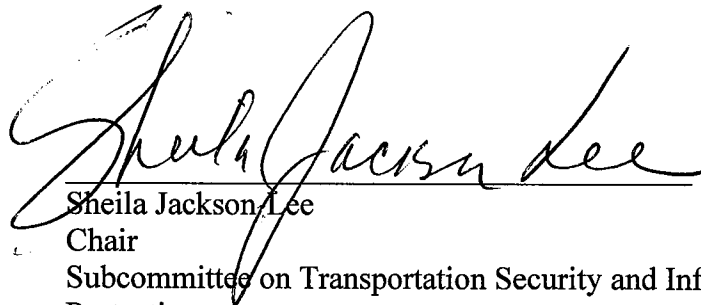
Sincerely,



Bennie G. Thompson
Chairman
Committee on Homeland Security



Edward Markey
Member
Committee on Homeland Security



Sheila Jackson Lee
Chair
Subcommittee on Transportation Security and Infrastructure
Protection
Committee on Homeland Security