United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

The Honorable Tom Davis
Chairman
Committee on Government Reform
United States House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Mr. Chairman:

Thank you for your letter dated July 10, 2006 regarding the Department of Agriculture's (USDA) incidents involving the loss or compromise of any sensitive personal information since January 1, 2003. I am providing the attached information in response to your request.

Since January 1, 2003, USDA has had eight incidents. If you have any additional questions, please do not hesitate to contact me at (202) 720-8833 or by email, dave.combs@usda.gov. An identical letter is being sent to Representative Henry A. Waxman, Ranking Member.

Sincerely,

David M. Combs
Chief Information Officer

Attachment

cc: OMB EOP
OIG

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

September 22, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter regarding the loss or compromise of sensitive personal information. In response to your request, the Department is undertaking a comprehensive survey of all operating units comprising 15 program offices within the Commerce Department to provide an up-to-date status of all incidents involving the loss or compromise of sensitive personal information held by the Department since January 1, 2003. We have no reason to believe that information lost or compromised has been used in any illegal or improper manner.

In response to your request, we have attached a summary of incidents involving the loss or compromise of data including pertinent facts, types of information lost or compromised, the number of individuals that may have been impacted and the dates where known. In summary, as displayed in the table below, Commerce has experienced 297 incidents in which sensitive personal information has been lost, potentially compromised or potentially breached. Although the largest category of these involve 217 laptops that were stolen, lost, or misplaced, this is out of an estimated inventory of over 30,000 laptops owned by the Department during the review period.

Reporting timeframe 2003 - 2006

Bureau	Laptops	Paper	Website	Thumb-Drives[2]	Other[3]
NOAA	3		1		1
OS		1			
CENSUS	214 [1]	16		46	**15**
TOTAL	**217**	**17**	**1**	**46**	**16**

[1] All 214 laptops were password protected, with 106 fully encrypted, 50 partially encrypted, 58 no encryption.
[2] All thumbdrives were fully encrypted.
[3] Includes: 1 email incident, and 15 handheld computer incidents.

As you can see, the overwhelming majority of these losses involved laptops within one agency at Commerce, the Census Bureau. The Census Bureau has a unique mission. Every year, thousands of Census field representatives fan out around the country to compile survey data, using laptops in their work. Much of the field workforce is comprised of temporary, hourly employees paid to gather data door-to-door.

Given the unique nature of the Census workforce and method of data collection, the Bureau has long had technological and procedural mechanisms in place that limit any potential breach of information. The Bureau indicated that the laptops contained the following:

- Technological Protections:
    - Every Census laptop from 2001 on requires a password to access;
    - Systemic safeguards ensure that once a survey is completed, the data is automatically stored on a laptop and cannot be retrieved or accessed in the field, even by the Census field representative; and
    - Each laptop contains information on an estimated 20-30 households, and rarely more than 100; field offices report that typical laptops would contain zero-to-two incomplete surveys.
- Procedural Protections:
    - The survey data is contained in complex database formats requiring specialized applications to access;
    - Each laptop contains survey data that is regularly transmitted at the end of each day, and such data is fully removed from the laptops at the end of each survey period; and
    - Since 2001, the Census Bureau has been adding encryption technology on a rolling basis for extra protection, and today, all new laptops have encryption protection.

In the last five years, the Census Bureau has been issued approximately 20,000 laptops for field data collection operations. Of the 246 missing Census laptops over that period, 104 were stolen, often from the employees' vehicles or while they were working, and another 113 were not returned by former employees.

In addition to laptops, Census began evaluating the use of handheld devices to record survey data for testing processes in preparation for the 2010 Census. Of the approximately 2,400 in use since 2004, 15 have been lost, stolen or are missing with personally identifiable information on them. All of these had encryption and required an initial password to operate the unit, and a second password to access the data that was only available to employees at Census headquarters. Unlike the laptops, it is possible for us to determine the potentially affected households, and we are in the process of contacting those 558 households even though the risk of misuse of data is extremely low.

In addition to those instances of potential breaches, the Census Bureau also reported 16 instances of non-electronic potential breaches of personal information, ranging from employee time and attendance records being lost in an office move to retirement

information packages sent to the National Finance Center during Hurricane Katrina not being received. Where these potentially affected people can be identified, we are also in the process of contacting them.

We at the Department of Commerce fully share your concern about the possible release and compromise of data and will continue efforts within the Department to employ protective technologies and implement more stringent rules and procedures to better protect personal information. While the vast majority of missing laptops don't contain any personal data, and all are protected by combinations of passwords, complex database software, systemic safeguards and/or encryption tools, there clearly is an unacceptably high degree of missing laptops.

As we go forward, the Department is:

- Asking the Inspector General to perform an investigation at the request of the Secretary;
- Directing an onsite senior Department of Commerce management team review at Census;
- Instituting inventory reforms, including the creation of one comprehensive database for all departmental property;
- Raising employee accountability standards;
- Expanding training to raise user awareness;
- Reviewing Department remote access and teleworking policies;
- Where warranted, imposing disciplinary action;
- Strengthening password protection policies; and
- Ensuring the recommendations included in the recent Administration policies are being implemented to include:
    - 100% encryption for all Department laptops;
    - Two-factor authentication for remote access and laptop use; and
    - The reporting process for personally identifiable information.

The Department takes very seriously these high instances of missing laptops, as well as potential breaches of personal identity data. This review process has clearly pointed out the flaws in the Department's inventory and accountability efforts going back many years. We are viewing this process with the spirit of actively rooting out the problems and addressing them immediately, and I look forward to working with the Committee on these matters. If you have any questions, or need additional information, please feel free to contact me at (202) 482-2112.

Sincerely,

Carlos M. Gutierrez

Enclosures

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

The Honorable Tom Davis
Chairman, Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515-6143

Dear Mr. Chairman:

This is in response to your letter requesting a summary of incidents involving the loss or compromise of personal information held by the Department of Defense (DoD) or a contractor on its behalf. Currently, the Department does not maintain data on the loss of personal information in a centralized location. Consequently, a preliminary survey of the DoD Component Privacy Offices was conducted to gauge the magnitude of the problem. Enclosed are the 43 incidents reported by the DoD Components, along with the associated corrective actions.

The Department is taking steps to secure and provide better protection for personal and sensitive data maintained internally or by contractors on individuals. On April 18, 2006, the DoD Chief Information Officer issued guidance regarding the protection of sensitive DoD data, and policies are being revised to include more stringent controls regarding the handling of sensitive information, mechanisms are being established to report such information to a centralized location, and individuals are being better trained on the proper handling of such information. These and other efforts will improve oversight of the management and handling of personal information, as well as strengthen the Department's ability to identify incidents in a timely manner to take corrective action.

Enclosure

cc:
The Honorable Henry A. Waxman
Ranking Member

UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, D.C, 20202-_____

JUL 2 8 2006

Honorable Henry A. Waxman
Ranking Member, Committee on Government Reform
2154 Rayburn House Office Building
United States House of Representatives
Washington, DC 20515

Dear Representative Waxman:

The U.S. Department of Education (the Department) is pleased to respond to your letter dated July 10, 2006, requesting information on lost or compromised personal information since January 1, 2003.

The Department implemented a data security incident response, tracking, and reporting program in February, 2004, and continues to work to ensure that all data security incidents are promptly identified and reported. This program has resulted in improved management of such incidents and an improved record of such events. The incidents reported herein represent our best understanding of the incidents that have occurred, and may not be complete.

The identified incidents include events where personally identifiable information (PII) was compromised under the Federal Student Aid program, as part of national research programs, conducted by the National Center for Education Statistics, and in other offices of the Department. This letter also notes reported incidents where it was later determined that no PII was compromised.

Incidents Related to Federal Student Aid
Four (4) incidents involve the Department's Federal Student Aid programs.

- **April 21, 2004.** Students attempting to access their student aid records online were instead presented information for another applicant. Federal Student Aid received notice of three such occurrences. Upon learning of the error, Federal Student Aid immediately took the system off-line until the application was corrected.

- **November 3, 2004**. ACS, a contractor to Federal Student Aid, used the commercial shipping company Federal Express to send a package to its facility in Utica, NY. The package, containing a paper roster with the names, social security numbers, and account numbers of 8,290 borrowers of federal student aid, was lost in transit by Federal Express. ACS has discontinued the use of DHL for Utica shipments.

- **February 11, 2005**. One postsecondary institution discovered an error within a Federal Student Aid database that allowed it to view the PII of up to 500 students at a different postsecondary institution. Upon notification of the incident, Federal Student Aid corrected the software code.

- **November 5, 2005**. An unencrypted magnetic media tape from the Connecticut Student Loan Foundation, with the PII of 11,329 Federal Student Aid borrowers, was lost after it arrived at Federal Student Aid's Virtual Data Center (VDC) in Meriden, CT. Staff conducted a thorough search for the missing tape and the Department's Office of the Inspector General (OIG) provided additional assistance. OIG subsequently conducted a thorough investigation that concluded that the incident was void of criminal misconduct and closed the case. The VDC enacted new shipping and receiving procedures as part of the remediation plan.

Based on assessments of each of these incidents, the Department concluded that notifications to potentially impacted individuals were not required.

Incidents Related to Research Activities
Thirty-four incidents involve the Department's National Center for Education Statistics (NCES). All involve a single contractor, the Research Triangle Institute (RTI), and none involve data in the possession of Department staff. Upon notification of these incidents, NCES has taken action to prevent similar incidents in the future, and, at the direction of NCES, the contractor has incurred substantial costs to correct its procedures for handling PII, replace lost information, and notify the impacted individuals.

- **November 14, 2005 through July 7, 2006.** RTI staff, conducting interviews of families across the United States, report 33 incidents where the PII of 182 study participants has been stolen or lost. One hundred and sixty-four of the impacted individuals have been notified, and attempts are continuing to notify the remaining 18.

- **June 19, 2006.** A commercial shipping company lost a package containing a CD-ROM with a password protected zip file containing PII for 13,700 study respondents shipped by RTI to the NCES. RTI notified the NCES of this incident on July 11, 2006, and on July 14, 2006, NCES issued guidance to cease all mail or courier shipments of PII of survey respondents and all other human subjects participating in any and all NCES data collection activities. NCES is in the process of implementing a secure server that will allow the transfer of sensitive information as required. None of these individuals have been notified.

Incidents Related to Other Department Offices
Three incidents have occurred in other offices within the Department. One occurred in the Department's Office of the Inspector General (OIG) and two in the Department's Office of Management (OM).

- **March 17, 2005.** An unencrypted laptop that may have contained PII of four subjects under investigation by a Special Agent of the OIG was stolen from the investigator's government vehicle parked inside the garage of a government facility in Atlanta, GA. Because the information that may have been lost belonged to subjects who were under criminal

investigation, no notification was given to the affected individuals. As part of the remediation effort, the OIG immediately began to research and test possible encryption solutions and has since implemented encryption software on all OIG laptops, enacted disciplinary action against the Special Agent and advised the US Assistant Attorney of the incident.

- **February 27, 2006 through March 9, 2006.** During this two-week period, OM staff mailed documents including the PII of five contractors to the wrong individuals. The forms contained names, dates of birth, social security numbers, address, work history and criminal history as well as family and reference contact data. OM learned of the error from a recipient who received a document in error. OM immediately contacted all addresses to which documents were sent and recovered the five misdirected documents. All five impacted individuals were notified.

- **November 2005 - present.** In November 2005, the Department identified potential issues with computer equipment inventory records and asked the Office of Inspector General (OIG) to review the matter. On July 28, 2006, the Department received an interim audit memorandum from OIG confirming weaknesses in the Department's procedures and controls in this area, potentially impacting a significant amount of computer equipment. The Department has begun its review of the interim audit memorandum and related information, and, at this time, cannot conclude whether any computer equipment has been lost or compromised or whether any such equipment contained PII. The Department will communicate to you the results of this review when it is completed.

Incidents Where Potentially Compromised Data Was Recovered Intact

Three incidents have occurred where PII was reported as lost or comprised but later recovered and/or determined to not have been lost or compromised. Each incident involves the physical transmission of data related to the Department's Federal Student Aid programs. Federal Student Aid has initiated new procedures and polices to reduce and eliminate the physical transmission of data.

- **June 10, 2006**. The commercial shipping company DHL lost a tape with PII during its transit to the Federal Student Aid Virtual Data Center in Meriden, CT from Premier Credit. An investigation by DHL found that the tape had fallen out of the package and was successfully delivered to the Federal Student Aid Virtual Data Center on June 13, 2006. The information on the tapes was not considered to be compromised.

- **July 7, 2006.** The commercial shipping company UPS delivered to Federal Student Aid's Virtual Data Center in Meriden, CT a damaged package containing tapes with PII from the Texas Guaranteed Student Loan (TG) Agency on July 3, 2006. The damaged package was rejected by the Virtual Data Center and returned to the sender for resubmission. The information on the tapes was not considered to be compromised.

- **July 11, 2006**. The commercial shipping company UPS lost one individual's application in transit to the Federal Student Aid Processing Center in Greenville, TX. A subsequent search found the document. The information on the application was not considered compromised.

Based on assessments of each of these incidents, the Department concluded that no notifications were required to potentially impacted individuals.

The Department's Focus on Protecting PII

As part of our ongoing review of the Department's overall data security, including security of PII, the Department and the Department's Office of the Inspector General, have identified weaknesses in critical IT security controls which could allow the loss or compromise of PII. The Department recognizes the need to strengthen its current policies and procedures and to develop and implement new strategies to protect PII in the future. The Department is working to ensure that all employees and contractors adhere to federally mandated standards for protecting sensitive personal information and associated information technologies.

To this end, the Department has taken prompt steps to ensure compliance with all statutory guidance and Presidential direction. This includes steps supporting the implementation of the Federal Property and Administrative Services Act of 1949; Privacy Act of 1974 (5 U.S.C. § 522a); chapter 35 of title 44, U.S.C.; The E-Government Act of 2002; subtitle III of title 40, U.S.C.; the Government Paperwork Elimination Act (44 U.S.C. 3504 note); and the Federal Information Security Management Act of 2002 (FISMA). Further, the Department works with the Office of Management and Budget (OMB) to identify specific mitigation strategies for improving our security posture as required by additional implementing regulations and guidance.

Examples of this include the designation of Michell Clark, Assistant Secretary for Management, as the Designated Senior Official for Privacy Policy, as well the recent appointment of Mr. Bill Vajda as the Departmental Chief Information Officer (CIO). As these roles are defined by statute, they work with all other Senior Departmental Officials to establish, review, test, evaluate, assess, and improve Information Records Management systems and safeguards used for handling sensitive personal information. In addition, several new policies have been established that improve record and data security. As required by FISMA and associated guidance (FIPS 199 and NIST Special Publication 800-60), Certification and Accreditation (C&A) activities have been completed for all Major Agency Information Systems. Mandatory information security awareness training has been revised and implemented throughout the Department with a specific emphasis on handling sensitive personal information. The Department has implemented and published incident response procedures per guidance from OMB that support the one-hour reporting requirement to the US CERT for the loss, exposure, or compromise of personal information.

The Department has initiated data minimization actions necessary to protect sensitive personal information while ensuring appropriate use for our business missions. We have initiated reviews of all Departmental data and information in accordance with FIPS 199. This will provide the framework for a comprehensive risk assessment, and basis for evaluating potential data loss impacts and appropriate mitigation techniques. These reviews includes evaluations of a systemic or technical nature; i.e., physical transportation and encryption of electronic media, hard-copy records retention and destruction, audit logs, etc.; as well as evaluation or our standard operating procedures for managing individual personal record requirements, such as those mandated by the

Children's On-line Privacy Protection Act (COPPA). As a result, the Department is heavily engaged with the OMB, the Federal CIO Council, and other Federal Departments to ensure that in the event of a security breach, our individual notification procedures and mitigation support are implemented consistent with established government policy and precedent.

The Department takes its role as caretaker of sensitive information seriously and will continue to pursue, implement and monitor security controls necessary to protect critical assets and the sensitive information entrusted to us by our constituents.

Sincerely,

William Vajda
Chief Information Officer
U.S. Department of Education

Enclosures
Suspicious Event Reports
Remediation Artifacts
Draft Policies for Handling PII

cc: Hon. Tom Davis

Department of Energy
Washington, DC 20585

August 28, 2006

The Honorable Thomas Davis
Chairman
Committee on Government Reform
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Secretary Bodman has requested that I respond to your July 10, 2006, letter requesting details about incidents involving the loss or compromise of sensitive personal information since January 1, 2003. Confirmed incidents that we are aware of as of today are described in the enclosure.

If you have any further questions, please contact me or Mr. Dirk A. Bartlett, Associate Deputy Assistant Secretary for Congressional and Intergovernmental Affairs, at (202)586-2701.

Sincerely,

Thomas N. Pyke, Jr.
Chief Information Officer

Enclosure

Enclosure to letter from Department of Energy (DOE), Chief Information Officer (CIO), Tom Pyke concerning loss of personal information

1. On June 10, 2003, the Pantex Plant, a component of the National Nuclear Security Administration (NNSA), reported a compromise of its Pantex PeopleSoft database. The compromise involved misuse of system administrator privileges by an individual who was a consultant at Pantex and who was operating inside the facility at the time of the incident. The individual's consulting agreement was immediately terminated and the consultant's access to the database was terminated. Personal information was exposed only to this consultant. The consultant was instructed to not disclose any sensitive information as part of the termination process.

2. In the Fall of 2004, a hard drive from the Idaho National Laboratory was sold to the public. The hard drive was returned to DOE on June 20, 2006, and it was discovered that it still had DOE information on it, some of which is personal information. To date, the Department has identified personal information on 34 individuals whose data was on this hard disk. These 34 individuals have been notified by the Department.

3. During July 2005, malicious software implanted through a sophisticated cyber attack was detected on a system at the NNSA Albuquerque Service Center. The malicious software caused transfer of a number of files through the Internet. These files contained personal information on 1,717 NNSA employees and contractors. Analysis of the intrusion techniques provided details that have been used to improve DOE defenses against a repeat of this attack. Each of the individuals whose sensitive personal information was involved has received notification of the loss of their personal information.

4. On June 8, 2006, 29 NNSA PC users were the object of a sophisticated cyber attack via electronic mail which used what looked like a valid email address of an NNSA senior manager. Two of the systems were compromised when the users clicked on the attachment of the email. The malicious software transferred several files through the Internet. One of these files contained the personal information of an NNSA employee. This individual has received notification of the loss of their personal information.

5. On June 9, 2006, there was a break in at the Cloverleaf DOE headquarters facility located in Germantown, MD. Ten laptops were stolen from DOE offices. Personal information on four individuals resided on these laptops. All of the individuals whose information was compromised have been notified.

6. On July 28, 2006, a senior Sandia National Laboratories official left his laptop on a domestic airline while on travel. The Department is still investigating this issue. To date, personal information on 249 individuals has been identified as present on the laptop at the time of loss. The individuals believed to be affected by this loss of data have been notified.

7. On August 2, 2006, a number of emails masquerading as being from the Argonne Credit Union were sent to some employees of Fermi National Accelerator Laboratory (FNAL) and Argonne National Laboratory (ANL). However, three employees (2 ANL and 1 FNAL) supplied personal information to a falsified Argonne Credit Union website. The three employees affected were notified.

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C 20201

SEP 2 7 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

As requested, enclosed is documentation on computer security incidents in response to your request dated July 10, 2006. As requested, this includes incidents involving the loss or compromise of sensitive personal information held by the Department of Health and Human Services (HHS) since January 1, 2003, as reported by each HHS Operating Division (OPDIV).

The incidents documented in the enclosed report include 16 instances of exposure of Centers for Medicare and Medicaid Services (CMS) data, three of Indian Health Service (IHS) data, one of Centers for Disease Control and Prevention (CDC) data, one of Office of the Inspector General (OIG) data, two of Program Support Center (PSC) data, and one of Administration for Children and Families (ACF) data. Four additional incidents are excluded from the report because they are related to pending investigations; information on these four incidents will be provided as the investigations are completed. One additional incident, involving a CMS contractor, is excluded because it was only recently reported, on September 25, 2006 and we are still gathering information; information on this incident will be provided as that information becomes available. Where appropriate, disciplinary action was taken. In order to provide as much information as possible, we have also included incidents of potential breaches of personal sensitive information by contractors of CMS, in which federal personnel and federally-owned systems are not involved. We note that HHS provides funding for many programs administered by states and other entities that utilize personally identifiable information. However, our reporting and management systems do not provide us with information on possible computer security incidents in those programs administered by states and other entities.

HHS centralized its incident reporting capability in mid-2004, to better comply with the Federal Information Security Management Act (FISMA) and, Office of Management and Budget Circular A-130. This reform, coupled with heightened awareness and attention to potential problems, has greatly increased the volume of reported incidents in FY 2006. HHS continues to strengthen our reporting processes and systems in support of protection of personally identifiable information.

HHS is cognizant of the importance of safeguarding the public trust by continuing to seek the most effective ways to protect that public's personal sensitive information. To that end, we have embarked on a broad review of HHS policy, guidance, and processes to verify that HHS is protecting personal sensitive information, mitigating the risk of exposure of personal sensitive information, and leveraging technology to monitor the effectiveness of those safeguards. Please call me if you have any further thoughts or questions.

Sincerely,

Charles E. Johnson
Assistant Secretary for Resources
and Technology

Enclosure

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 14, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
US House of Representatives
Washington, DC 20515-6143

Dear Mr. Chairman:

On behalf of Secretary Chertoff, I am responding to your July 10, 2006 letter regarding privacy data breaches committed by the Department. This letter is in response to your request for information regarding sensitive personal information lapses at the Department of Homeland Security (DHS).

The attachment to this letter details the sensitive personal information lapses in DHS since January 1, 2003.

Should you or your staff have any questions, please contact the Chief of Staff for the Office of the Chief Information Officer, Mr. Michael Butcher at (202) 447-3400.

Sincerely,

Scott Charbo
Acting Under Secretary for Management

Enclosure

August 2006 - Transportation Security Agency (TSA)

- Letters were sent to former TSA employees that contained SSN and birth dates, however, there was an error in the addresses used. The letters were sent to incorrect addresses and not the intended recipients.
- All of the intended recipients were notified of the incident and given guidance on additional measures to protect themselves.

August 2, 2006 – Customs and Border Protection (CBP)

- An email was sent to 43 recipients containing SSN's of the recipients. The recipients included DHS and other government organizations.
- An email was sent to all recipients explaining what had occurred and directed all the users to delete the subject file.

July 31, 2006 – Citizenship and Immigration Services (CIS)

- The incident involved an employer named "Staff Force," who left several boxes of documents by a dumpster. The documents included a user password for the USCIS Basic Pilot program. The documents by the dumpster also included copies of completed I-9 forms, as well as names, social security numbers and other sensitive information about individuals such as copies of driver's licenses.
- The account was disabled as a precautionary measure.

July 21, 2006 - Citizenship and Immigration Services (CIS)

- A document containing PII information on DHS employees and contractors was placed on an internal web site (DHS Online) and was accessible to anyone internal to DHS.
- A department wide effort focused on finding all occurrences of this document. These efforts included the scanning of all workstations, servers, email servers, and deploying IDS signatures to detect the transferring of the subject document.

June 14, 2005 - Citizenship and Immigration Services (CIS)

- A CIS user provided payroll information to the soon to be X-wife of an ICE employee. The CIS user used her every day access to the system to obtain the payroll information without prior or proper authorization. Apparently the CIS user is friends with the soon to be X-wife.
- This incident was sent over to the ICE Joint Intake office of OPR for further investigation.

August 20, 2004 - Immigration and Customs Enforcement (ICE)

- User's laptop was stolen while on travel in Rome, Italy. The information that was lost was reported to include only personal information for the one individual that included passport and additional ID's.
- Items reported as stolen:
  - Laptop (hard drive was encrypted)
  - Secure ID Token

  - Government cell phone
  - Deportation Officer Badge
  - Deportation Officer Credentials
  - Official Passport
  - Krome Detention Center ID
  - Miami District Office ID
  - Miami Airport ID (expired)
- Remote access was disabled for this users account and the Embassy Security Officer was notified of incident in addition to filing the appropriate police report.

452032

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-1000

OFFICE OF CONGRESSIONAL AND
INTERGOVERNMENTAL RELATIONS

JUL 24 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515-6143

Dear Mr. Chairman:

On behalf of Secretary Jackson, thank you for your letter of July 10, 2006. I am pleased to have this opportunity to highlight what the Department of Housing and Urban Development is doing to ensure the protection of personally identifiable information. HUD is deeply committed to protecting the confidentiality of data pertaining to its customers, business partners, program participants, and employees. In light of the losses and compromises of personal data reported elsewhere in the federal government, the Department has taken action to review and strengthen security controls to protect sensitive information. Additionally, as described in the enclosed incident summary table, HUD has also taken appropriate action in responding to the single case of potential loss or compromise of personal data that the Department has experienced.

As reflected in the enclosure, HUD employees have been provided instruction on what is required to secure sensitive data, and executive management has emphasized the importance of protecting personally identifiable information. HUD remains vigilant of the potential for loss or compromise of sensitive data and has implemented processes for continual review and monitoring of its policies and procedures to ensure that the necessary controls are in place.

Should you have questions regarding this report, please do not hesitate to contact the Department.

Sincerely,

L. Carter Cornick III
General Deputy Assistant Secretary
for Congressional and
Intergovernmental Relations

Enclosures

350768

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

TAKE PRIDE IN AMERICA

JUL 25 2006

The Honorable Thomas M. Davis III
Chairman, Committee on Government Reform
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This is in response to the Committee's letter to Secretary Kempthorne dated July 10, 2006, seeking certain information on data breaches at Federal agencies.

Pursuant to the request, the Department of the Interior conducted an internal data call to capture details about reported incidents involving the loss or compromise of any sensitive personal information since January 1, 2003. The enclosed spreadsheet outlines seven (7) incidents reported for Interior and one (1) incident resulting from Interior's charge card issuer, Bank of America under GSA's SmartPay program, for which we have credible information. Should we identify any additional incidents we will promptly report them.

We are providing an original letter with enclosure to the Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform, House of Representatives.

Sincerely,

W. Hord Tipton
Chief Information Officer

Enclosure

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 22, 2006

The Honorable Tom M. Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This responds to your letter, dated July 10, 2006, to the Attorney General, which requested "details about incidents involving the loss or compromise of any sensitive personal information held by the federal government or a contractor that occurred in your Department since January 1, 2003." We are sending a similar response to Ranking Member Waxman, who joined in your letter to us.

Since 2003, the Department has tracked computer security incidents, instructing Departmental components to promptly report such incidents to the Department's Computer Emergency Response Team ("DOJCERT"). Prior to May 2006, however, when the sensitive personal information of millions of veterans and active duty military was lost on a burglarized Veterans Administration laptop, the Department did not specifically track the content of lost, stolen or otherwise compromised devices. After we learned of the VA laptop loss, the Department's Chief Privacy & Civil Liberties Officer, Jane C. Horvath, promptly instructed the senior information technology and security managers to begin specifically tracking whether personally identifiable information was present on any lost, stolen or compromised device. Accordingly, DOJCERT now does so.

We are aware of two recent incidents that are responsive to your request. On July 7, 2006, a tourist visiting Washington found an envelope lying on the street, and turned it over to a U.S. Capitol police officer. Its contents included two forms, each of which contained the social security number of an FBI employee. The officer contacted the employee personally. It was determined that the envelope had been lost by a contract employee; the contractor was terminated. To date, there is no indication of compromise of this information.

On July 26, 2006, the Department's Management Division reported that an online training module for the Department's time-and-attendance reporting program had included actual time-and-attendance reports submitted by six employees, albeit with social security numbers blacked out. Notwithstanding the efforts to conceal them, the social security numbers could be made out. Upon discovery of this, the reports were removed from online access. In the meantime, however, the file containing them was downloaded 220 times, and viewed 7,772 times. The affected employees have been notified, and the downloaded files removed from the Department's computer system. To date there is no indication of compromise. Investigation of this incident is ongoing.

If we can be of further assistance regarding this or any other matter, please do not hesitate to contact this Office.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

JUL 24 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Davis:

As the Department of Labor's Chief Information Officer, I am writing to respond to your July 10, 2006 inquiry regarding security incidents related to the loss or compromise of sensitive personal information.

The Department of Labor takes seriously its responsibility to ensure the security of its computer systems, web-based resources and collection points for sensitive personal data. We appreciate the leadership your Committee has demonstrated in promoting stronger electronic security in the Federal Government. As outlined in your inquiry, the compromise of personal information of 26.5 million veterans resulting from the theft of a Department of Veterans Affairs laptop computer has revealed the continuing, urgent need for Federal Agencies to constantly evaluate their security protections and elevate them to acceptable industry standards. As evidenced by the high marks your Committee has given our Department in the past on computer security, we are committed to identifying security concerns throughout the agency and addressing them with tested "best practices" from industry and government.

In addition to protecting the Department of Labor's systems from unauthorized access and disabling viruses, we view the security of personally identifiable information (PII) as one of our highest priorities. Because the loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information, we take our responsibility to protect that information very seriously. To that end, we have adopted a comprehensive strategy to assess the Department's current privacy policies, procedures and practices to ensure compliance with all applicable Federal mandates and to identify areas where our current procedures can be strengthened. As recently as May 26, 2006, the Office of the Chief Information Officer distributed the enclosed e-mail to the more than 16,000 DOL employees and contractors reminding them of their critical responsibility to safeguard PII and referring them to Departmental security and privacy policies.

The Department maintains a fully centralized Computer Security Incident Response Capability (CSIRC) where all DOL agencies are required to report security incidents, according to risk category. As of July 14, 2006, in accordance with Office of Management and Budget guidance, all incidents involving PII must be reported to the

CSIRC within one hour of detection. The CSIRC then conducts an analysis of the information provided and reports to the DOL Office of the Inspector General (OIG) and the United States Computer Emergency Response Team (US-CERT) as appropriate.

In response to your inquiry, we have reviewed all responsive incidents reported since January 1, 2003 and provide the following information:

Laptop Computer Stolen Containing Personally Identifiable Information
On March 3, 2005 a DOL laptop containing PII on 91 members of the public was stolen from a DOL employee's office in Dallas, Texas. The laptop computer has not been recovered. Information contained on the password-protected laptop includes these individuals' names, addresses and social security numbers.

On March 3, 2005, a police report for the stolen laptop was filed with the Department of Homeland Security Federal Protective Service and the incident has since been reported to US-CERT and to the DOL OIG. To prevent further access to other DOL information resources, on March 4, 2005 the laptop was removed from the Active Directory environment of the associated general support system. The Department is currently in the process of notifying the affected individuals.

Laptop Computer Stolen Containing Encrypted Personally Identifiable Information
On November 23, 2005, a DOL laptop containing PII on 203 members of the public was stolen during an office renovation in Glendale, California. The laptop has not been recovered. Information contained on the password-protected laptop includes these individuals' names, social security numbers, and employer tax identification numbers. The information on the laptop was also encrypted.

On December 5, 2005, to prevent further access to any other DOL information resources, the laptop was removed from the Active Directory environment of the associated general support system. The Department is currently in the process of notifying the affected individuals.

Lost Laptop Computer Containing Personally Identifiable Information
On February 28, 2006, a DOL laptop containing PII on 510 individuals was lost in Houston, Texas. The laptop was lost by a DOL employee conducting an investigation of potential civil and criminal violations. At this time, the laptop has not been found. The password-protected laptop contained case records including the following attributes: name, date of birth, social security number, home and work addresses.

On March 6, 2006, the user was issued another laptop computer, and the user's password was reset to prevent the missing laptop from being used to access other DOL information resources. This incident has since been reported to US-CERT and to the DOL OIG. The Department is currently in the process of notifying the affected individuals.

Computer security is taken seriously at the Department of Labor. DOL senior managers and IT professionals are committed to fulfilling and enhancing the Department's Computer Security Program, to ensure the highest level of data security and system protection possible. We welcome the continued leadership and guidance of your Committee as we work to implement our comprehensive strategy mentioned above to strengthen the protective measures for safeguarding the PII entrusted to the Department.

Please feel free to contact me with any future inquiries at Pizzella.Patrick@dol.gov, or 202-693-4040.

Sincerely,

Patrick Pizzella
Assistant Secretary for Administration and Management,
Chief Information Officer

Enclosure

United States Department of State
Washington, D.C. 20520

Dear Mr. Chairman:

Thank you for your letter of July 10 regarding incidents involving the loss or compromise of any sensitive personal information held by the Department of State or a contractor that occurred since January 1, 2003.

Since January 1, 2003, we have had only one confirmed loss of sensitive personal information. The loss occurred on May 11, 2005. Analysis of network traffic revealed that a Department user's personal online banking password, which had been stored on the employee's Government computer, was compromised. The user was contacted and informed that he should change the password and check the account for fraudulent use. The user later reported no unauthorized access to the account.

We hope this information is helpful in addressing your concerns. Please feel free to contact us further on this or any matter of concern to you.

Sincerely,

Jeffrey T. Bergner

Jeffrey T. Bergner
Assistant Secretary
Legislative Affairs

The Honorable
Tom Davis, Chairman,
Committee on Government Reform,
House of Representatives.

THE SECRETARY OF TRANSPORTATION
WASHINGTON, D.C. 20590

July 31, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman: CHAIRMAN,

Thank you for your letter of July 10, cosigned by Ranking Member Waxman, requesting information regarding the U.S. Department of Transportation's (DOT) incidents involving the loss or compromise of sensitive personal information. The DOT takes seriously the need to protect sensitive personal information. The DOT has established a variety of security and privacy policies and has reexamined these policies in light of recent events. New policies are presently being developed in response to the Office of Management and Budget's (OMB) recent issuances, Memorandums 06-15, 06-16, and 06-19.

To answer the questions raised in your letter, to date, the DOT has no knowledge of any DOT system that was ever breached that resulted in any cases of identity theft. However, DOT does have knowledge of one incident of unauthorized access of employee personal information by another employee. As requested in your letter, the following is a short narrative of the event, as well as the corrective actions taken.

- On July 11, a Federal Aviation Administration (FAA) employee reported that he had acquired access to other Federal employees' personal information located on travel vouchers in the FAA's Travel Management System. When the employee printed a copy of his own travel voucher, he had the capability to print the last five vouchers that were printed by other employees. The vouchers included personally identifiable information (PII), including social security number and home address. The employee stated that he never actually accessed these vouchers and merely took note of the ability to do so in order to report it.

- Through a review of the incident, it was determined that no PII was ever available to the public. Previously printed travel vouchers were only available until the system maintenance processes were run each night, at which point the files were deleted.

- The employee reported this incident through established management channels and the FAA and DOT information technology functions were made aware of this incident on July 17. Since the files were deleted every 24 hours, and 6 days had passed since the

incident, DOT was unable to determine which employees' information was available through the incident and notify those employees.

- The FAA immediately remediated the issue by increasing the frequency of file deletions to every 5 minutes. Previously, the files were deleted every night. It should be noted that FAA's Travel Management System is to be retired within the next month and replaced by a Government-wide solution, GovTrip.

- This is the only reported case of PII data access by an unauthorized individual. The details of this incident were reported by the DOT Transportation Computer Incident Response Center to the Department of Homeland Security in compliance with the recently issued OMB Memorandum 06-19.

Recognizing the consequences of data breaches and to safeguard against these risks, DOT assumes responsibility for mitigating risks to an acceptable level and holds each DOT employee and contractor accountable for protecting any PII they come in contact with in performing their job duties.

If I can provide further information or assistance, please feel free to call me. An identical letter has been sent to Ranking Member Waxman.

Sincerely yours,

Maria Cino

Maria Cino
Acting Secretary

DEPARTMENT OF THE TREASURY
WASHINGTON

ASSISTANT SECRETARY

SEP 2 7 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Davis:

Treasury shares your deep concern for incidents within the federal government involving the potential loss or compromise of sensitive personal information. We appreciate your efforts to elevate awareness of this issue on a government–wide level.

The enclosed spreadsheet provides details on the 340 total incidents that have occurred in the Department of the Treasury from January 1, 2003. Each entry includes a brief summary of the incident, including the date, incident circumstances, information that may have been lost, and the number of potentially affected individuals. In a number of incidents we have been able to confirm that no compromise of sensitive personally identifiable information occurred. However, many incidents are still being investigated as to whether or not sensitive personal information was lost or compromised.

Treasury has policies and practices in place to safeguard sensitive personal information, such as requiring encryption of sensitive data. All matters involving sensitive data loss must concurrently be reported within one hour to Treasury officials and the Inspector General so that the powers of law enforcement can be brought to bear on recovery. In the case of the IRS, additional safeguards are in place and taxpayer case file data is required to be encrypted; this provides additional security above and beyond password protection.

Yet, clearly, more must be done. That is why Treasury is taking aggressive action to do everything possible to protect data. The Department currently is in the process of implementing additional protections and actions, including but not limited to automatic encryption solutions on all mobile media, and mandating additional training to re–emphasize awareness of user security responsibilities. In addition, we have underscored to all Treasury bureau heads the seriousness of any loss of sensitive personal information and charged them to further strengthen their efforts to enhance physical and cyber security as necessary.

With regard to aforementioned incidents, most of which involve Treasury bureaus, please know all bureau heads have been instructed to forward additional information directly to you and your staff and are available should there be need for further information or discussion.

Again, thank you for your efforts to elevate awareness of this issue on a government–wide level. If there is anything we can do to be of further assistance, I encourage you to contact me personally anytime.

Sincerely,

Sandra L. Pack

Sandra L. Pack
Assistant Secretary for Management
and Chief Financial Officer

Enclosure