STAFF REPORT
AGENCY DATA BREACHES SINCE JANUARY 1, 2003
COMMITTEE ON GOVERNMENT REFORM
TOM DAVIS, CHAIRMAN
HENRY A. WAXMAN, RANKING MEMBER
U.S. HOUSE OF REPRESENTATIVES
109th CONGRESS
OCTOBER 13, 2006

SUMMARY

The federal government compiles and holds sensitive personal information on every citizen, including health records, tax returns, and military records.

In May 2006, the Department of Veterans Affairs announced that computer equipment containing the personal information of approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Since that time, several other agencies – including the Social Security Administration, the IRS, and the Department of Health and Human Services – have revealed security breaches that affected thousands more individuals.

Given the VA incident, and in order to develop a full picture of the risks posed by data breaches at federal agencies, the Government Reform Committee asked agencies to provide details about incidents involving the loss or compromise of any sensitive personal information held by an agency or a contractor since January 1, 2003. The Committee issued the request, dated July 10, 2006, to all cabinet agencies, as well as the Office of Personnel Management and the Social Security Administration.

Specifically, the Committee requested a brief summary of each incident, including the date, circumstances of the breach, information that was lost or compromised, and the number of individuals affected. In addition, the Committee requested, for each instance, documentation regarding the Department's remedial efforts, including any notification made to the individuals whose information was compromised. The Committee requested a response by July 24, 2006.

The agency responses show a wide range of incidents involving data loss or theft, privacy breaches, and security incidents. Agency responses to data losses appear to vary as well, with some notifying all potentially affected individuals, and others not performing such notifications. Despite the volume of sensitive information held by agencies, there is no requirement that the public be notified if their sensitive personal information is compromised. Legislation authored by Committee Chairman Tom Davis and included in the House passed Veterans Identity and Credit Security Act of 2006 would change that.

Agency reports to the Committee varied in the level of detail provided about data loses. Thus, this report, which provides highlights from agency responses, cannot be seen as a comprehensive review of data loss by federal agencies. Despite this limitation, some conclusions can be drawn:

1. Data loss is a government-wide occurrence.

All 19 Departments and agencies reported at least one loss of personally identifiable information since January 2003. This is not a problem that is restricted to the Department of Veterans Affairs or any other single agency.

2. Agencies do not always know what has been lost.

The letters received by the Committee demonstrate that, in many cases, agencies do not know what information has been lost or how many individuals could be impacted by a particular data loss. Similarly, agencies do not appear to be tracking all possible losses of personal information, making it likely that their reports to the committee are incomplete. For example, the Department of Justice reports that, prior to the May 2006 Veterans Administration data breach, "the Department did not track the content of lost, stolen, or otherwise compromised devices."

3. Physical security of data is essential.

Only a small number of the data breaches reported to the Committee were caused by hackers breaking into computer systems online. The vast majority of data losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees.

4. Contractors are responsible for many of the reported breaches.

Federal agencies rely heavily on private sector contractors for information technology management services. Thus, many of the reported data breaches were the responsibility of contractors.

Department of Agriculture

The Department of Agriculture reported to the Committee on July 25, 2006 that it has confirmed eight incidents involving the loss or compromise of any sensitive personal information since January 1, 2003.[1] The details of four incidents are as follows:

- On December 17, 2004, an email was sent to 1,537 individuals that included as an attachment, a database containing the 1,537 individuals' social security numbers and other personal information. In response to the event, a letter of apology was sent to all 1,537 individuals, and training on appropriate security measures was developed.

- On February 24, 2005, a system containing research data was compromised by someone cracking a password or a user account and installing hacking software. The Agency reports that no information was compromised, but the intruder had read/write access to the server and was able to open access points. In response to the event, the login account that was cracked was disabled and the agency prevented certain types of inbound traffic from outside the building.

[1] Letters from David M. Combs, Chief Information Officer, Department of Agriculture, to Reps. Thomas M. Davis and Henry A. Waxman (July 25, 2006).

- On July 15, 2006, a computer was stolen which contained the listing of an unknown number of individuals' personal information. In response to the event, local law enforcement and the FBI were contacted.

- On June 3, 2006, three systems were compromised, potentially making available the names, social security numbers, and photos of 26,000 USDA employees, contractors, and retirees. The USDA reports that it has no conclusive evidence as to whether or not data was compromised so they decided to err on the side of caution and alerted and provided informational notices to all 26,000 employees, contractors, and retirees with identification badge access to facilities within the Washington, D.C. area.

Department of Commerce

The Department of Commerce reported to the Committee on September 22, 2006 that it has confirmed 297 incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[2] According to the Department, 217 laptops containing sensitive personal information have been lost, stolen, or misplaced during this period. The vast majority of these, 214, were Census computers. Another 46 incidents involved the loss of Census thumb-drives containing sensitive personal information. All of the thumb-drives and about half of the laptops were fully encrypted. Other data losses reported by the Department of Commerce include:

- On July 1, 2006, the agency learned that a former employee had copied sensitive letters and a database of employee information. The documents contained medical information on 51 employees, including names, home addresses, description of issues, and employees' medical diagnoses and prognoses. The database included information about 883 cases involving current and former employees. An investigation is ongoing.

- On August 18, 2006, the Census reported that paperwork on 10 new employees – including names, social security numbers, date of birth, and fingerprint cards – was lost. An investigation is ongoing.

In a separate briefing, the Department told members of Congress that, since 2001, a total of 1,137 Department laptops have been stolen, lost, or reported missing. Approximately half of the lost Census Bureau computers simply were not returned by

[2] Letters from Carlos M. Gutierrez, Secretary of Commerce, to Reps. Thomas M. Davis and Henry A. Waxman (Sept. 22, 2006)

departing or terminated employees. The agency did not track computer equipment, nor were employees held accountable for failing to return it.[3]

Department of Defense

The Department of Defense reported to the Committee on September 13, 2006 that it has confirmed 43 incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[4] One component of DoD, the Department of the Army, reported no incidents. The Army did not respond to the Committee's subsequent request for information.[5] The details of four incidents reported by other Departments within DoD are as follows:

- On August 1, 2006, a laptop containing personal information on 30,000 applicants/LEADS, recruiters, and prospects fell off a motorcycle belonging to a Navy recruiter. The recruiter returned to the scene and was told by a road side worker that a car stopped and picked up the bag. The loss/theft is under investigation and a letter of notification is being prepared for those affected.

- On March 17, 2006, a thumb drive containing personal records on approximately 207,570 enlisted Marines who served between the years of 2001 to 2005 was lost. A notification letter was sent to the affected individuals and the Marine Corps.

- On June 17, 2005, a systems administrator discovered potential unauthorized access to the Air Force Personnel Center Assignment Management System containing personal information on 33,000 military members. The system was taken off-line, an investigation was initiated immediately by law enforcement, and notifications were sent out to system users immediately.

- On April 5, 2006, hackers stole data from the Defense Department's Tricare Management Activity system, including personal data on approximately 14,000 active duty and retired service members and dependents. In response to the incident, affected members were notified and new security measures were implemented.

---

[3] Briefing by Carlos M. Gutierrez, Secretary, David Sampson, Deputy Secretary, Nathaniel F. Wienecke, Assistant Secretary, and Barry West, Chief Information Officer, Department of Commerce, for Reps. Thomas M. Davis, Frank Wolf, and Michael R. Turner (September 21, 2006).

[4] Letters from Gordon England, Deputy Secretary, Department of Defense, to Reps. Thomas M. Davis and Henry A. Waxman (September 13, 2006).

[5] E-mail exchange and telephone conversation between Government Reform Committee staff and Department of Defense staff (September 26-27, 2006).

Department of Education

The Department of Education reported to the Committee on July 28, 2006 that it has confirmed 41 incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[6] The details of three of these incidents are provided below:

- On June 19, 2006 a shipping contractor to the Department's National Center for Education Statistics (NCES) lost a package containing a CD-ROM with a password protected zip file containing personally identifiable information for 13,700 study respondents shipped by the contractor to the NCES. In response, NCES issued guidance to cease all mail or courier shipment of personally identifiable information in any and all NCES data collection activities, but did not notify the affected individuals.

.

- On November 5, 2005, an unencrypted magnetic tape containing the personal information of 11,329 student borrowers was lost at the Federal Student Aid's Virtual Data Center (VDC). Department of Education staff and the Office of the Inspector General conducted an investigation, determined that no criminal activity had occurred, and closed the case.

- On November 3, 2004, a contractor to Federal Student Aid used a commercial shipping company to send personal information on 8,290 borrowers to a contractor facility. The shipper lost the package in transit. Following an assessment of the incident, the Department decided not to notify the affected individuals. The contractor discontinued use of the shipping company for that facility's shipments.

Department of Energy

The Department of Energy (DOE) reported to the Committee on August 28, 2006 that it has confirmed seven incidents involving the loss or compromise of any sensitive personal information held by the federal government or a contractor since January 1, 2003.[7] The details of four incidents are provided below:

- On June 10, 2003, a component of the National Nuclear Security Administration, the Pantex Plant, reported a compromise of a database. A consultant operating inside Pantex misused system administrator privileges, exposing an unknown amount of personal information to this individual. In response to this incident, the

[6] Letters from William Vajda, Chief Information Officer, Department of Education, to Reps. Thomas M. Davis and Henry A. Waxman (July 28, 2006).

[7] Letters from Thomas N. Pyke, Jr., Chief Information Officer, Department of Energy, to Reps. Thomas M. Davis and Henry A. Waxman (August 28, 2006).

individual's consulting agreement and access to the database was terminated, and the individual was instructed not to disclose any sensitive information.

- In the fall of 2004, a hard drive from the Idaho National Laboratory, which contained DOE information, including some personal information, was sold to the public. The hard drive was returned to DOE in 2006. To date, 34 individuals' personal information has been identified on the hard drive, and all have been notified by the Department.

- In July 2005, NNSA Albuquerque Service Center detected malicious software implanted in one of their systems that caused transfer of files containing personal information of 1,717 NNSA employees and contractors, through the Internet. All individuals affected by the attack have been notified. DOE reports that it has improved its defenses by analyzing the intrusion techniques used in this attack.

- On July 28, 2006, a senior Sandia National Laboratories official left his laptop on a domestic airline while on travel. The laptop contained personal information on 249 individuals. The individuals affected by this loss of information have been notified and the Department in still investigating this issue.

Department of Health and Human Services

The Department of Health and Human Services (HHS) reported to the Committee on September 27, 2006 that it has confirmed 24 incidents involving the loss or compromise of any sensitive personal information since January 1, 2003.[8] Four incidents are highlighted:

- On November 18, 2005, two employees of a Centers for Medicare and Medicaid Services (CMS) contractor stole records for the purpose of identity theft. Approximately 1,574 Medicare beneficiaries may be impacted by this theft. All of the potentially impacted individuals were notified.

- On March 28, 2006, a CMS contractor notified the CMS that eight laptops containing beneficiary and supplier information for CMS has been stolen from the contractor's office. A beneficiary list contained on the laptops had 12,877 Health Insurance Claim Numbers, with the majority of the list (10,855) including names, addresses, and dates of birth. In addition, lists containing 2,932 supplier numbers, 920 physician identification numbers, and 30 law enforcement information requests were also taken.

[8] Letters from Charles E. Johnson, Assistant Secretary for Resources and Technology, Department of Health and Human Services, to Reps. Thomas M. Davis and Henry A. Waxman (September 27, 2006).

- On February 15, 2006, the Centers for Disease Control and Prevention (CDC) reported 22 laptops stolen from a contractor facility. Three of the 22 laptops contained Department of Defense (DoD) service member information, affecting 1,382 DoD service personnel. All of the potentially impacted individuals were notified.

- On June 22, 2006, a CMS contractor reported the theft of a contractor employee laptop containing a variety of personal identifiable information including medical care information. A total of 49,572 Medicare beneficiaries may have been affected. All of the potentially impacted individuals were notified.

Department of Homeland Security

The United States Department of Homeland Security (DHS) reported to the Committee on September 15, 2006 that it has confirmed six incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[9] The details of three incidents are provided below:

- On July 31, 2006, a Citizenship and Immigration Services (CIS) employer left several boxes of documents that contained sensitive information by a dumpster. The documents included a user password for the USCIS Basic Pilot program, copies of completed I-9 forms, social security numbers, and other personal information.

- On July 21, 2006, a CIS document containing personally identifiable information on DHS employees and contractors was placed on an internal website. This document was accessible to anyone within DHS. In response to this event, a department wide effort focused on finding all postings of this document.

- On June 14, 2005, payroll information was provided to a soon to be ex-wife of an Immigration and Customs Enforcement (ICE) employee. A Citizenship and Immigration Services user obtained the payroll information through her everyday access to the system without prior or proper authorization. This incident is under further investigation.

Department of Housing and Urban Development

The Department of Housing and Urban Development reported to the Committee on July 24, 2006 that it has confirmed one incident involving the loss or compromise of sensitive

[9] Letters from Scott Charbo, Acting Under Secretary for Management, Department of Homeland Security, to Reps. Thomas M. Davis and Henry A. Waxman (Sept. 14, 2006).

personal information held by the federal government or a contractor since January 1, 2003.[10] The details of the incident are as follows:

- On June 26, 2006, a HUD employee discovered that a backup disk containing sensitive and confidential personal information on 757 current and former HUD employees was missing from HUD headquarters. In response to the incident, a variety of notices were provided to the potentially affected individuals.

Department of the Interior

The Department of the Interior reported to the Committee on July 25, 2006 that it has confirmed eight incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[11] The details of three of these incidents are as follows:

- On January 13, 2005 a computer server containing the personal information on an unknown number of field office staff was stolen during an office break in. In response to the incident, a report was filed with all appropriate officials, and the stolen server was located at a pawn shop.

- On December 13, 2004, National Capital Regional Office mistakenly accessed a fraudulent website which may have exposed that individual's personal information. Upon notification, a police report was filed, the user changed their employee password, and the desktop was scanned.

- In December 2005, the Department's charge card issuer under GSA's SmartPay program lost data tapes containing information on 61,000 cardholders. In response to the incident, appropriate security officials were contacted and a variety of notices were provided to the potentially affected cardholders.

Department of Justice

The Department of Justice reported to the Committee that it has confirmed two incidents involving the loss or compromise of sensitive personal information held by the federal

[10] Letters from L. Carter Cornick III, General Deputy Assistant Secretary for Congressional and Intergovernmental Relations, Department of Housing and Urban Development, to Reps. Thomas M. Davis and Henry A. Waxman (July 24, 2006).

[11] Letters from W. Hord Tipton, Chief Information Officer, Department of the Interior, to Reps. Thomas M. Davis and Henry A. Waxman (July 25, 2006).

government or a contractor since January 1, 2003.[12] The details of the incidents are as follows:

- On July 7, 2006, an envelope containing personal information on one FBI employee was lost by a contract employee and was turned in by a tourist. In response to the incident, the employee was contacted and the contractor was terminated. To date, there is no indication of compromise of this information.

- On July 26, 2006, a time-and-attendance program containing reports exposing social security numbers, were submitted by six employees, downloaded 220 times, and viewed 7,772 times. Although the social security numbers were supposed to be blacked out, they were visible. In response to the incident, the reports were removed from the computer system and the affected employees were notified. The investigation of this incident is ongoing.

Department of Labor

The Department of Labor (DOL) reported to the Committee on July 24, 2006 that it has confirmed three incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[13] A follow-up letter from the Department on August 18, 2006 provided additional information about one of these incidents.[14] The details of the incidents are as follows:

- On March 3, 2005, a DOL password protected laptop containing personal information on 91 members of the public was stolen. In response to the incident, a police report was filed, the computer was removed from the Active Directory environment, and a notification letter is being prepared for those affected.

- On November 23, 2005, a DOL password protected laptop was stolen, containing encrypted personal information on 203 members of the public. In response to the incident, the laptop was removed from the Active Directory and a notification letter is being prepared for those affected.

- On February 28, 2006, a DOL laptop containing personal information on 1,137 individuals was lost by an employee conducting an investigation of potential civil and criminal violations. The laptop contained the social security numbers of

[12] Letters from William E. Moschella, Assistant Attorney General to Reps. Thomas M. Davis and Henry A. Waxman (Aug. 22, 2006).
[13] Letters from Patrick Pizzella, Assistant Secretary for Administration and Management and Chief Information Officer, Department of Labor, to Reps. Thomas M. Davis and Henry A. Waxman (July 24, 2006).
[14] Letters from Patrick Pizzella, Assistant Secretary for Administration and Management, Department of Labor, Chief Information Officer, to Reps. Thomas M. Davis and Henry A. Waxman (August 18, 2006).

about half (570) of these individuals. In response to the incident, a notification letter is being prepared for those affected.

Department of State

The Department of State reported to the Committee on July 31, 2006 that it has confirmed one incident involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[15] The details of the incident are as follows:

- On May 11, 2005, an analysis of network traffic revealed that one employee's banking password had been compromised. In response to the incident, the user was informed and later reported there has been no unauthorized access to the account.

Department of Transportation

The Department of Transportation reported to the Committee on July 31, 2006 that it has confirmed one incident involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[16] The details of the incident are as follows:

- On July 11, 2006 a Federal Aviation Administrative (FAA) employee reported that he had inadvertently acquired access to five other Federal employees' personal information located on the travel vouchers in the FAA's Travel Management System. The FAA immediately resolved the issue by increasing security measures on the Travel Management System.

Following the Committee's receipt of this report from the Department of Transportation, a public Freedom of Information Act request revealed a series of data breaches at the Department that compromised the personal information of at least 133,000 people.[17] According to this report, in August 2006, the Office of Inspector General at the DOT lost two laptops containing the information of more than 133,000 people. In addition, DOT has lost nearly 400 laptop computers and had nine instances when Personal Identification Information was lost or stolen, and a theft of electronic media and hard copy paper

[15] Letters from Jeffrey T. Bergner, Assistant Secretary Legislative Affairs, Department of State, to Reps. Thomas M. Davis and Henry A. Waxman (July 31, 2006).
[16] Letters from Maria Cino, Acting Secretary of Transportation, to Reps. Thomas M. Davis and Henry A. Waxman (July 31, 2006)
[17] *Lost DOT Laptops: Compromised Personal Data?* WTOP News (October 6, 2006).

information at the National Highway Traffic Safety Administration has jeopardized the information of almost 100 people.[18]

In an email to Committee staff, DOT stated: "The letter regarding PII was accurate at the time of the request," and that the Department has been "focused on putting a PII protection and incident response program in place."[19]

Department of the Treasury

The Department of the Treasury reported to the Committee on September 27, 2006 that it has confirmed 340 incidents involving the loss or compromise of sensitive personal information since January 1, 2003.[20] In all but four of those instances, the Department could not report the number of individuals impacted, whether notification of individuals had occurred, or whether incident-specific remedial efforts were undertaken. These instances include:

- On February 27, 2006 a Revenue Officer reported that his IRS computer and 14 taxpayer cases were stolen from his vehicle.

- On April 28, 2006, the Computer Security Incident Response Center was informed that an IRS employee laptop containing 48 corporate taxpayer records and four individual taxpayer records had been stolen.

- On June 13, 2005, an IRS employee reported that his external computer disk drive was missing, and that he had last seen it on June 3.

Department of Veterans Affairs

On September 5, 2006, the Department of Veterans Affairs provided the Committee with two large spreadsheets with information about hundreds of security and privacy incidents that have occurred at the Department since January 2003.[21] The well-publicized case involved the theft of a laptop and hard drive in May 2006 that resulted in the compromise of personal information for 26.5 million individuals. Some of the other cases appear to have involved the compromise of a single individual's personal information. The details of four incidents are as follows:

---

[18] *Id.*

[19] Email from Joe Guzzo, Department of Transportation, to Government Reform Committee Staff (Oct. 6, 2006).

[20] Letters from Sandra L. Pack, Assistant Secretary for Management and Chief Financial Officer, Department of Treasury, to Reps. Thomas M. Davis and Henry A. Waxman (Sept. 27, 2006).

[21] Letters from R. James Nicholson, Secretary, Department of Veterans Affairs, to Reps. Thomas M. Davis and Henry A. Waxman (Sept. 5, 2006)

- On June 13, 2004, a personal computer containing health summary extracts was stolen from an outpatient clinic area. Approximately 600 individuals were impacted. The individuals were notified, the Department held a question and answer session, and installed an automated computer program to limit the download of health summary extracts.

- On October 14, 2005, a computer containing 421 patient health summaries and other personal information was stolen. Agency privacy and security officials were notified but since full social security numbers were not lost, no further action was taken.

- On May 8, 2006, a data backup tape containing veteran and VA employee sensitive case tracking information on 7,579 individuals was reported missing. The OIG is investigating and the affected individuals have been notified.

- On June 25, 2006, a CD containing 30,000 veterans' names and addresses was lost by a Government Printing Office subcontractor.

Office of Personnel Management

The Office of Personnel Management reported to the Committee on August 3, 2006 that it has confirmed three incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[22] The details of the incidents are as follows:

- On June 13, 2006, personal information was mistakenly faxed to another government agency containing personal information affecting an unknown number of individuals. However, OPM does not believe the information was compromised because the recipient promptly destroyed the information upon receipt. In response to the incident, the department responsible for the incident reminded the staff to be more cautious when sending faxes.

- On November 16, 2004, an unknown number of people were affected due to a glitch on the OPM website that allowed the use of any password or PIN to access personal information on the site. Compromised claims were restored to prior status before any changes were actually processed to affect benefits. In response to the incident, access controls were strengthened.

[22] Letters from Linda M. Springer, Director, Office of Personnel Management, to Reps. Thomas M. Davis and Henry A. Waxman (August 3, 2006)

- On October 30, 2004, a van was stolen from a courier containing personal information on 300 retirees in 13 boxes and six locked cases of tapes that were allegedly dumped in a field. In response to the incident, an investigation was performed, recovering 10 of the 13 boxes, firing the courier driver, and implementing stricter guidelines for handling sensitive personal information.

Social Security Administration

The Social Security Administration (SSA) reported to the Committee on August 3, 2006 that it has confirmed three incidents involving the loss or compromise of sensitive personal information held by the federal government or a contractor since January 1, 2003.[23] The three incidents are as follows:

- In August of 2003, an SSA employee accessed records of members of the public and disclosed the information to a third party, affecting one person. In response to the incident, the employee retired in face of being suspended under SSA's sanctions provisions.

- On April 15, 2006, an employee lost a flash drive containing as many as six files with hearing related information impacting six people. In response to the incident, the case was referred to OIG for an investigation, which is currently in process.

- An SSA employee used an SSA computer multiple times between the years of 2003 and 2004 to obtain earnings records on three members of a family to assist his cousin's husband in a child support case impacting three people. In response to the incident, all individuals impacted were notified and a criminal case is pending on the arrest of the employee.

CONCLUSION

Taken as a whole, the agency reports outline hundreds of instances of data breaches involving sensitive personal information since January 1, 2003. The reports show a wide range of incidents, involving employee carelessness, contractor misconduct, and third-party thefts. The number of individuals affected in each incident ranges from one to millions. However, in many cases, the agency does not know what information was lost or how many individuals potentially could be affected. Few of these incidents have been reported publicly, and it is unclear in many cases whether affected individuals have been notified or whether remedial action has been taken.

[23] Letters from Jo Anne B. Barnhart, Commissioner, Social Security Administration, to Reps. Thomas M. Davis and Henry A. Waxman (August 3, 2006)

Data held by Federal agencies remains at risk. In many cases, agencies do not know what information they have, who has access to the information, and what devices containing information have been lost, stolen, or misplaced. In addition, in almost all of the reported cases, Congress and the public would not have learned of each event unless the Committee had requested this information.

Finally, each year, the Committee releases information security scorecards. This year the scores for many departments remained low or dropped precipitously. The federal government overall received a D+.