Memorandum

U.S. Department of Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: Analysis of Loss of Control Over Sensitive Personally Identifiable Information and Follow-up Actions to Strengthen its Protection

Date: August 28, 2007

From: Theodore P. Alves
Associate Deputy Inspector General

Reply to Attn. of: J-2

To: Inspector General

This memorandum provides the results of an analysis of two incidents involving the loss of control over Sensitive Personally Identifiable Information (SPII):[1] the July 27, 2006, theft of an Office of Inspector General (OIG) laptop from a special agent's vehicle in Doral, Florida, and the April 24, 2006, theft of an OIG laptop from a hotel conference room in Orlando, Florida.

As a result of these two laptop thefts, the OIG lost control over a large amount of SPII. Of particular concern was information on 138,000 individuals that had been collected in connection with Florida-based OIG investigations. Normally, these data would have been encrypted. However, due to a needed system upgrade, the data were not encrypted at the time of these thefts.

While it does not appear that these two incidents resulted in any identity theft or other damage to the persons who had SPII on the laptops, we felt it was critical to understand the factors and circumstances that led to loss of control over SPII, identify what needed to be done to strengthen the protection of SPII, and ensure that these steps were carried out.

This memorandum (1) sets forth the circumstances surrounding the loss of SPII as a consequence of the two laptop thefts in Florida; (2) describes the OIG response,

[1] SPII consists of the combination of names and other personal information (e.g., addresses, dates of birth, and social security numbers) that can be exploited to falsely obtain credit using another person's identity. Personally identifiable information (PII) and SPII are often used interchangeably. Technically, a telephone company's white pages contain PII because the listings identify specific persons and associate their names with a phone number. It is the linking of an individual's name with information that is not readily publicly available (such as a social security number) and that can be exploited to falsely obtain credit that this report refers to as SPII.

including efforts to protect the affected individuals; (3) assesses the risk of identity theft created by our loss of control over the SPII; (4) identifies the factors that contributed to losing control of the SPII; and (5) describes and evaluates OIG efforts to reduce the likelihood of future loss or improper disclosure of SPII.

SUMMARY OF RESULTS

We found that our efforts to protect the SPII entrusted to us were insufficient. We identified three vulnerabilities that contributed to the breaches and took steps to address each of the vulnerabilities to prevent any future loss of SPII. We are also confident that, based on the results of our investigation into the thefts and an independent analysis of credit transactions pertaining to the affected individuals, the SPII contained on the laptops has not been and is not likely to be exploited to perpetrate identity theft.

When the two laptops were stolen, they contained databases with large amounts of SPII. Of particular concern was information on 138,000 individuals that had been collected in connection with Florida-based OIG investigations. This information was collected in connection with investigations related to airman certificates issued in Florida, commercial driver's licenses issued in Miami, and commercial and individual driver's licenses issued in the Tampa area. Because the information on these individuals was stored in Microsoft Access and Microsoft Excel files, which are easily accessible file types, these individuals faced an increased risk of identity theft if the laptop thieves tried to exploit the data contained on these laptops.

Although the laptops were protected by password authentication that met National Institute of Standards and Technology (NIST) requirements, the data files, which had been encrypted, were decrypted[2] at the time of the theft. This decryption took place to allow a needed upgrade of the OIG computer infrastructure. Because the data files were decrypted, the SPII on the laptops was more vulnerable to improper disclosure. Although defeating the password is fairly difficult, there are readily available programs that allow a user to reset a Windows password; if the password were reset, the user would have access to all unencrypted data.[3]

We believe that both laptops were probably stolen for the value of the computers, rather than for the data they contained. As noted in the guidance developed by the

---

[2] There was no encryption requirement at the time of the thefts. Following the May 2006 theft of an external hard drive containing personal information on 26 million veterans from the home of a Veterans Affairs employee, the Office of Management and Budget mandated that all agency data stored on mobile computer/devices be encrypted by August 7, 2006, unless the data were determined, in writing, to be non-sensitive.

[3] Using such a program would not give the user access to *encrypted* data—encrypted data would be rendered unreadable by resetting the password in this manner.

President's Identity Theft Task Force[4] (ITTF guidance): "The risk of identity theft is lower when the control over the data is lost as a result of the theft of a computer that is inadvertently left unprotected in a public location." This is consistent with the results of our investigation into the Doral theft. As part of this investigation we placed a decoy laptop in a vehicle in the same parking lot where the Doral laptop was stolen. We observed an individual[5] break into that vehicle and were able to arrest that individual and break up a computer theft ring. Interviews of the participants revealed that they stole laptop computers, reloaded new operating systems and then sold the computers on the used market without attempting to access the data.

In response to the Doral theft, we took a number of actions to inform the affected individuals. We quickly reviewed backups of the files to identify persons whose SPII was stored on the laptop. We then sent letters to those individuals for whom we could find addresses providing information regarding the theft and steps they could take to protect themselves. We also posted this information on our website and encouraged persons believing that they might be victims of identity theft to contact our hotline, which is staffed 24 hours a day, 7 days a week.

Further, we took steps to protect the individuals from harm in the event that the data were exploited. To do this, we hired ID Analytics, a firm that specializes in helping organizations assess risks and minimize harm following a data breach. ID Analytics is monitoring credit activity for the individuals whose SPII was lost to determine whether identity theft is occurring as a result of the loss of control over these databases.[6] ID Analytics certified that as of August 21, 2007, the date of its most recent analysis,[7] no organized misuse of the databases stored on the stolen computers has occurred.

In analyzing how this loss of control over SPII occurred, we identified three contributing factors: (1) measures taken to protect the physical security of the laptops were insufficient; (2) the data on the laptops were decrypted (to preserve the data) during an upgrade to the OIG's information technology (IT) system; and (3) SPII databases were stored on laptop computers, which are inherently less

---

[4] A September 19, 2006, memorandum setting forth this guidance was circulated by the Office of Management and Budget to the heads of all Federal departments and agencies. This guidance is posted on the internet at: http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

[5] That individual was convicted of theft of Government property and deported.

[6] The ITTF guidance notes that because "approximately 3.6 percent of the adult population reports itself annually as the victim of some form of identity theft . . . for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events other than the data security breach in question." ID Analytics looks for "organized misuse" to distinguish between identity theft related to the breach and identity theft that is the "normal by-product of the routine incidence of identity theft."

[7] Thus far, ID Analytics has provided us with 4 reports. The most recent report was issued on August 21, 2007. ID Analytics will continue to monitor these databases through August 2008.

secure than computers that operate in a centralized environment. Had any one of these factors not existed, the loss of control would not have occurred.

In response to these incidents, we have taken a number of actions to reduce the likelihood of any future loss of control over SPII. For example, we have:

- *Improved laptop physical security* by issuing cable locks to all OIG laptop users, issuing policy for properly securing unattended laptops, and implementing guidance developed by the Department of Transportation (DOT) regarding the security of portable computers.

- *Enhanced the protection of laptop data* by encrypting laptop hard drives and employing a two-factor authentication system, which requires the user to set a password and plug in a small token device to access the laptop.

- *Stored sensitive personal information in a more secure fashion* by removing all such databases from laptops and either moving them to a more secure OIG network server or deleting them if no longer needed. We will also periodically review sensitive data and remove any that is no longer needed.

- *Raised employee sensitivity of the need to protect such information* through security training, management web casts, instructional videos, and other guidance.

CIRCUMSTANCES SURROUNDING THE THEFT OF LAPTOPS CONTAINING SPII

Laptop Stolen in Doral, Florida

On Thursday, July 27, 2006, an OIG laptop computer was stolen from an OIG vehicle near Miami, Florida. The OIG special agent to whom the laptop was assigned was transporting an agent from another Federal law enforcement agency and a Federal prosecutor to see various locations related to an open investigation, and they stopped for lunch at a restaurant in Doral. The special agent left his laptop in an unzipped case, atop a stack of other equipment in the cargo bay of a locked OIG Chevrolet Blazer.[8]

While the agents and prosecutor were in the restaurant, a thief used a tool to punch in the keyhole on the front passenger door of the vehicle to gain entry and stole the OIG laptop, leaving the carrying case behind. No other items were stolen. Upon

[8] Although the vehicle had tinted windows, a re-creation of the scene determined that the laptop could have been seen from outside the vehicle.

returning to the vehicle, the agent did not notice that the passenger side lock had been punched out.

Later that day, the agent notified the Assistant Special Agent in Charge (ASAC) of the Miami office that his laptop was missing from its carrying case. He said that he was concerned because he was certain he had the laptop with him when he left the offices of the Florida Department of Law Enforcement (FDLE) that morning. When the ASAC asked him if the vehicle could have been broken into, he informed her that nothing else was missing and he saw no indication of a break-in, such as broken glass. The ASAC advised that she would notify the Special Agent in Charge (SAC) but suggested that the agent recheck the car and retrace his steps at FDLE. The following day, the agent unsuccessfully searched FDLE; over the weekend, he also searched his residence and found nothing.

Because the laptop was not located on Friday (July 28) or over the weekend, on Monday morning (July 31), the Miami SAC sent an e-mail to various Headquarters personnel, including the OIG System Security Officer (OIG SSO), advising them that a laptop had been stolen. The SAC also instructed the OIG agent to file the required police report with the Miami-Dade Police Department.[9] Because the agent was at a loss to explain how the thief gained entry, the Miami SAC and the agent examined the vehicle on August 1 and discovered the hole in the passenger door lock.

Determination That Sensitive Personally Identifiable Information Was at Risk

Upon receiving the Miami SAC's July 31, 2006, e-mail reporting the theft of the Doral laptop, the OIG SSO, aware of the requirement to promptly report incidents involving loss of control over PII, asked whether the stolen laptop contained PII. Later that morning, the Miami SAC confirmed that the laptop contained some PII, in the form of social security numbers (SSNs) and other personal information obtained from interviewees during criminal investigations.[10] The OIG SSO then immediately notified the Department's Transportation Computer Incident Response Center (TCIRC) that an OIG laptop containing PII had been stolen.

OIG Headquarters was not initially aware, however, that the laptop contained large databases of SPII collected as part of OIG investigations being conducted by the Miami office. In order to precisely determine the type of information contained on the stolen laptop, the SAC began examining a back-up copy of the

---

[9] Although the OIG agent was instructed to file the report on July 31, 2006, the report was not actually filed until noon the next day, August 1, 2006.

[10] Collecting this information from persons who are interviewed in the course of criminal investigations is a standard law enforcement practice.

data stored on the stolen laptop. On August 3, 2006, the SAC advised Investigations Headquarters management that her preliminary review identified two investigative databases that contained SPII, consisting of individuals' names, addresses, and social security numbers. On August 4, 2006, the SAC reported additional databases with similar SPII.

On August 5, 2006, the Acting Inspector General was informed that the stolen laptop contained large databases of SPII. He immediately ordered the Office of Investigations to remove all such databases from laptop computers and directed an investigation into the circumstances surrounding the loss of SPII.

The back-up files were then sent to OIG Headquarters where they were analyzed by computer forensic agents. The initial analysis of the back-up files identified SPII associated with approximately 133,000 persons, including the following: a Microsoft Access database containing names, SSNs, and addresses for 42,792 Florida pilots; 3 Microsoft Excel spreadsheets containing names and SSNs for 80,667 Miami-Dade County area commercial driver's license (CDL) holders; names, SSNs, and addresses for 9,005 individuals who obtained personal driver's licenses from the Largo, Florida, licensing examining facility near Tampa; and names, SSNs, and addresses for 491 individuals who obtained CDLs from the Largo facility.

By letters dated August 9, 2006, the Acting Inspector General notified Members of Congress, the Governor of Florida, and the public that we had lost control over SPII belonging to approximately 133,000 persons as a consequence of the theft of the Doral laptop. On that date, the Acting Inspector General also conducted a telephone briefing with congressional staff and another with news media representatives.

Subsequent analysis of the back-up files revealed that 6 more Microsoft Excel spreadsheets were stored on the stolen Doral laptop, amounting to an additional 4,250 individuals with SPII not previously reported. These spreadsheets contained Florida airman certificate information used by the OIG's Miami office in connection with multi-agency task forces focusing on the use of fraudulent information to obtain airman certificates. Our forensic examination also found that the laptop contained databases received from the Department of Justice (DOJ) containing preliminary investigative lead information pertaining to, among other things, possible identity fraud by numerous individuals. We provided DOJ with an accounting of the DOJ-generated databases that were on the stolen laptop.

Re-Examination of the April 2006 Orlando Laptop Theft

After being notified that the Doral laptop contained SPII, the Acting Inspector General directed that an earlier laptop theft be re-examined. That laptop, which

had been assigned to the Miami SAC, was stolen on April 24, 2006, from a hotel conference room in Orlando, Florida. At the time of the theft, which was 4 weeks before the Department of Veterans Affairs (VA) incident was publicly reported, we had treated this matter as a loss of property, rather than a loss of control over sensitive information.

The Orlando laptop was stolen on the first day of a week-long fraud prevention conference, which the OIG co-sponsored at a hotel in Orlando. The conference was organized by the Miami SAC, who had loaded the various PowerPoint presentations for the conference on her laptop. The laptop was attached to printers in a hotel conference room to provide logistical support for the conference.

The Miami SAC stated that she closed the room (she believed the door to be locked but did not recall checking to make sure that it was locked) and left at approximately 8:30 p.m. When she returned 45 minutes later, the conference room was open, the laptop was missing, and a hotel employee was servicing the room. She asked the employee about the laptop, and he stated that it had not been in the room when he entered. Hotel security was then notified, and they in turn notified the local police who responded the following day.

At the time of the theft, the Miami SAC's main concern was that conference speaker presentations were stored on the laptop. Although the laptop theft was reported to OIG senior management, OIG management was not informed that the laptop contained SPII. Consequently, even after the VA incident in May 2006, when OIG Investigations Headquarters became more aware of SPII issues, the Orlando laptop continued to be treated as a property theft, and no attempt was made to determine what information had been stored on the stolen laptop until the Acting Inspector General's decision to expand the inquiry following the theft of the Doral laptop.

Forensic analysis of the Orlando laptop back-up files revealed that it contained some of the SPII that had been found on the Doral laptop; specifically, information for approximately 9,005 individuals who obtained their personal driver's license information from the Largo, Florida, licensing examining facility near Tampa and approximately 491 drivers who obtained CDLs from the same Largo facility. It also contained an additional amount of SPII that was not on the Doral laptop, which consisted of Microsoft Excel spreadsheets containing the information of 713 individuals related to criminal investigations of designated pilot examiners, CDL holders, and airport screeners.

OIG EFFORTS TO PROTECT AFFECTED INDIVIDUALS FROM IDENTITY THEFT AND TO RECOVER THE STOLEN LAPTOPS

We took several steps to protect the affected individuals and recover the stolen laptops. We sent letters to those individuals whose SPII we found in our initial review of the databases contained in the backup of the Doral laptop. Subsequently, we awarded a contract to a firm that specializes in monitoring credit records of groups of individuals affected by a data breach to determine whether the data has been exploited for credit fraud. As of August 21, 2007**,** that firm has reported that no organized misuse of the databases had occurred.

Shortly following the Doral laptop theft, we announced a $10,000 reward offer for information leading to its recovery, placing a notice in local newspapers and distributing reward posters throughout the area. We also conducted a joint investigation with the Miami-Dade Police Department and the Federal Bureau of Investigation (FBI) in an effort to recover the Doral laptop. Although we were not successful in recovering the laptops, our investigation identified a small ring of computer thieves who stole laptop computers, reloaded new operating systems and sold the computers on the used market. One individual was arrested, convicted, and deported for theft of Government property.

Notification to Persons Who Had SPII on Stolen Laptops

Shortly after we identified 133,000 individuals who had SPII in the databases stored on the Doral laptop[11], we began sending letters to those individuals for whom we could obtain valid addresses. A fact sheet and the letters sent to affected citizens, available in both English and Spanish versions, were also placed on our website.

The letters described the incident and recommended actions that affected individuals could take to protect themselves. Specifically, we suggested that they contact one of the three major credit reporting bureaus to request that an initial fraud alert be placed on their credit record and to obtain a free credit report. We also suggested that they monitor bank and credit card statements and contact financial institutions to check for any suspicious activity on their accounts.

[11] As previously noted, the Office of Management and Budget circulated a September 19, 2006, memorandum from the Identity Task Force that provided guidance for agencies to follow in responding to breaches that could lead to identity theft, and we have followed those guidelines since their issuance. The guidelines ask agencies to evaluate whether any of the information presents a risk of identity theft. Because the Microsoft Access and Excel databases contained names linked to other identifying information and were in readily accessible form, we concluded that they presented a risk of identity theft. This was not true for all personal information on the laptop. For example, we believe that it is unlikely that anyone would search through the investigative reports on the laptop in order to collect a small number of SSNs that special agents collected from interviews.

We advised these individuals to be careful about phone calls, e-mails, and other communications from individuals purporting to be Government officials and "phishing" for or asking to verify personal information. We encouraged those suspecting that they might be a victim of identity theft as a result of the laptop thefts to contact our hotline. We also placed this information on our website and provided it to trade publications aimed at pilots and commercial truck drivers as most of the affected individuals were in these two groups.

Our hotline received 1,769 telephone calls, 47 e-mails, and 11 letters.[12] We responded with information and instructions on how to request that the major credit reporting bureaus place a fraud alert on their accounts. In instances where individuals believed that they were the potential victim of identity theft, our agents investigated the particular facts and circumstances. Every individual who contacted the OIG and requested a telephone or e-mail response received a reply. We have found no evidence of any suspected identity theft attributable to the databases stored on the stolen laptops. While some of these individuals had, in fact, been victims of identity theft, we determined that those incidents were unrelated to the stolen laptops.[13]

Efforts To Protect Affected Individuals From Identity Theft

We engaged ID Analytics, a San Diego, California, firm that the VA employed following two incidents in which it lost control of SPII.[14] ID Analytics will monitor the databases stored on the stolen Doral and Orlando laptops for 2 years for signs that these data are being misused. ID Analytics detects suspicious patterns in bank and credit account activity to manage identity risk and prevent all types of credit fraud, from the opening of new bank and credit card accounts to transaction and collection activity on existing accounts. The firm has developed a network that gathers information from applications for credit, changes of address, and other identity risk information from companies; this network includes 5 of the top 10 banks in the United States, almost all major wireless carriers, and a leading retail credit card issuer. The firm's technology is designed to flag misuse of credit data, identify individuals whose credit has been misused, and determine the location of the misuse.

According to ID Analytics, the advantages of its method of fraud detection are that it identifies organized misuse of data, quickly identifies the intended victims, actively and constantly monitors a file of PII data, and identifies the location of the

[12] As of August 23, 2007.

[13] As of August 23, 2007, we have finished investigating 38 of 39 complaints and thus far have not found any evidence of identity theft stemming from the stolen laptops.

[14] The first incident involved the theft of an external hard drive and personal laptop from the home of a VA employee. The second incident involved the theft of a computer from a VA contractor.

suspects so law enforcement officers can apprehend them. It can also help determine whether the data are being used by more than one criminal suspect and provides a deterrent effect when it is publicly announced. As stated previously, no organized misuse of the databases that were stored on the stolen OIG laptops has been detected as of August 21, 2007 (the date of the firm's most recent analysis).

Efforts To Recover the Doral Laptop

Shortly following the theft of the Doral laptop, our Office of Investigations began coordinating with the Miami-Dade Police Department and the FBI to investigate the theft and recover the laptop.[15] As part of this investigation, we examined the circumstances of laptop thefts in the area.[16] This resulted in identifying several vehicle burglaries around the restaurant where the OIG laptop had been stolen, which bore similarities to that theft. Based on that information, our agents established surveillance in the vicinity. On September 11, 2006, our agents observed two men attempting to break into a "bait" vehicle containing a decoy laptop computer, which we parked near the restaurant. They appeared to use a tool to punch in the lock keyhole on the front passenger door—the same technique used to break into the OIG vehicle on July 27. Although this theft attempt was unsuccessful, our agents were able to identify the two men based on follow-up investigative work.

On September 19, 2006, our agents observed one of these men breaking into two vehicles near the restaurant and removing laptop computers. One of the vehicles was a "bait" vehicle containing a decoy laptop provided by the FBI. The other was a private vehicle that contained a Hewlett-Packard laptop belonging to a Miami resident. Investigative activity determined that the decoy laptop thief passed the laptops to a middleman who took the laptops to the owner of a computer business in the Miami area. After coordinating with the U.S. Attorney's Office in Miami, our agents obtained a Federal search warrant for the computer business. During the search of this business, agents recovered both the decoy and Hewlett-Packard laptops.

On September 21, 2006, Miami-Dade Police arrested the individual who stole the decoy laptop ("decoy thief"). That same day, our agents and police received consent to search the decoy thief's apartment and found 10 additional laptop computers—the Doral laptop was not found in any of the searches. Police checked the laptop serial numbers against information maintained by the National Crime Information Center (NCIC) and determined some of them were stolen.

---

[15] We took the same preliminary investigative steps with respect to the Orlando laptop, but no useful leads were developed. This is not surprising given that the investigation did not start until 3 and a half months after the theft.

[16] We also posted a $10,000 reward and distributed numerous posters announcing that fact. Although we received numerous tips, none of them led to recovery of the Doral laptop or payment of the reward.

Subsequent to the arrest, police found a punch tool in the decoy thief's vehicle. When interviewed, the decoy thief admitted to using the punch tool to break into vehicles and to stealing laptops from vehicles near the restaurant. He did not specifically recall, however, stealing the OIG laptop on July 27.

On October 5, 2006, the decoy thief was indicted by a Federal grand jury. He pleaded guilty in U.S. District Court on December 4, 2006, to a single felony charge of theft of Government property (the decoy laptop). He was sentenced to time served and 3 years of supervised probation. However, because he was a Colombian national in the United States illegally, he was transferred to the custody of U.S. Immigration and Customs Enforcement and deported to Colombia.

Also on September 21, 2006, Miami-Dade police interviewed the computer business owner. He told the investigators he did not know the laptop computers were stolen, but later admitted that he suspected they were stolen. He said he received $25 per laptop to load new operating systems (i.e., Microsoft Windows) onto the laptops. He specifically admitted to having loaded new operating systems on the stolen decoy and Hewlett-Packard laptops. He asserted that he did not attempt to access data on any laptops prior to loading new operating systems. Reloading a new operating system would dramatically decrease the likelihood that a subsequent user of the laptop would be aware of or be able to access the SPII that was stored on it at the time of its theft.

OIG agents interviewed the suspected middleman involved in the theft ring. He admitted to receiving $75 per laptop from the thief and delivering the laptops to the computer business owner who loaded new operating systems for $25 per laptop. He further admitted to having loaded some new operating systems himself. He maintained that he never tried to access data on any laptops prior to loading new operating systems. OIG agents and Miami-Dade police detectives located and interviewed the individual who had been observed breaking into vehicles with the decoy thief on September 11, 2006. He admitted to stealing laptop computers from vehicles with the decoy thief.

None of these four individuals recalled stealing or receiving the Doral laptop. However, one of them commented that, after seeing the OIG reward posters, he and the other suspects joked that they probably had stolen the OIG laptop and missed out on the $10,000 reward. During their interviews, two of the suspects provided additional insight regarding disposal of the stolen laptops. They stated that older laptops were sold locally, often to high school students, while newer, high-end laptops were shipped to Columbia. One suspect identified a shipping company he used. They opined that because the OIG laptop stolen on July 27 was relatively old, it was likely sold to a local student.

ASSESSMENT OF RISK THAT SPII WILL RESULT IN IDENTITY THEFT

In a September 19, 2006, memorandum, the President's Identity Theft Task Force provided guidance for agencies to use in assessing how likely it is that a data security breach will result in identity theft and determining whether affected individuals should be notified of the risk.[17] Specifically, the Task Force suggested that agencies consider the following four factors:

- How easy or difficult it would be for an unauthorized person to access the [SPII] in light of the manner in which the [SPII] was protected;
- The means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;
- The ability of the agency to mitigate the identity theft; and
- Evidence that the compromised information is actually being used to commit identity theft.

As set forth below, the application of these factors suggests that, although there was information on the laptops that could be used to commit identity theft, it is unlikely that such theft will occur. Based on our application of this guidance, we also concluded that it was not necessary to notify the additional individuals who were listed in databases that were identified during the subsequent, more detailed forensic analysis. The significant factors that led us to this conclusion were (1) the likelihood that the thieves reloaded the laptop's operating system and sold the computer on the used market, and (2) the periodic analysis of credit risks being performed under the ID Analytics contract, which will help us to determine if there was an attempt to exploit this data and would allow us to target the perpetrators if that took place.

Task Force Factor 1: Accessibility of the Data

Both of the stolen laptops were password-protected with passwords that were consistent with the standards set by the NIST for systems that store personal

[17] The President's memorandum did not use the term "SPII" and instead referred to it as "personal information of the type that can result in identity theft." The guidelines can be found on the FTC's website, www.FTC.gov, by clicking on "Fighting Back Against Identity Theft," clicking on "President's Identity Theft Task Force," and clicking on "President's Identity Theft Task Force Summary of Interim Recommendations." Currently, it can be directly accessed at: http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf. As these guidelines were not issued until September 19, 2006, we were unable to use them to formulate our initial response. We have, however, followed them with respect to decisions made after September 19, 2006. On May 22, 2007, the Office of Management and Budget issued a memorandum that required agencies to implement the recommendations of the Task Force with respect to "safeguarding and responding to the breach of personally identifiable information" within 120 days. This memorandum is available at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

information. To illustrate, we required that the passwords be at least 8 characters in length and contain at least one letter, one number, and one special character.[18] The laptops were configured so that the user could not select a password that did not meet these standards. The laptops were also configured to "time-out" after 30 minutes (i.e., if the computer was not being used for 30 minutes, the user's password would have to be re-entered to operate the system). This affords some protection, in that a password meeting this standard is relatively difficult to defeat.

It is possible, however, to gain access to the computer without defeating the password. There are easily obtainable programs that allow a Windows password to be reset. Had the data been encrypted, this would not have posed a serious risk since use of these programs renders encrypted data unreadable. Unfortunately, as previously discussed, before the theft, both laptops had been decrypted to allow a needed upgrade to the OIG's operating system. Consequently, the SPII stored on these laptops was more vulnerable to disclosure if the person stealing the laptops was technically proficient and interested in accessing the data.

Task Force Factor 2: How the Loss Occurred

The circumstances of the thefts suggest that the laptops were stolen for the value of the computers and not for the value of the data. Regarding this issue, the President's Task Force on Identity Theft notes:

> For example, as a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if the information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby. Similarly, in some cases of theft, the circumstances might indicate that the data storage device, such as a computer left in a car, rather than the information itself, was the target of the theft.

The results of our investigation into the Doral, Florida, theft ring confirm that the laptop was stolen for the value of the computer, rather than for the information itself. As discussed above, the thieves stated that they would load a new operating system on the computers and then resell them. This was corroborated by our subsequent forensic analysis of the Government decoy computer. When that computer was recovered, we determined that a new operating system had been installed and that the data had not been accessed.

While loading a new operating system is unlikely to destroy all existing data, it does make it invisible to someone who is not actively looking for it. A Windows operating system maintains a list of all files stored on the computer's hard drive.

---

[18] Federal Information Processing Standard (FIPS) 112.

Running a program such as Windows Explorer will generate a list of the files on the hard drive. However, when a new operating system is loaded onto the computer, the existing file list is erased. This essentially hides the existence of old information from the new user. As new information is stored on the computer's hard drive, the old data is eventually overwritten.

Task Force Factor 3: Ability To Mitigate Possible Identity Theft

As noted above, we have contracted with ID Analytics to monitor the SPII databases on the stolen laptops. ID Analytics analyzes a wide variety of credit data to determine if there is any organized misuse of the SPII data. If such misuse occurred, it would provide us with pertinent information regarding the identity of both the victims and the perpetrators. We would then be in a position to notify the affected individuals and pursue the perpetrators. Early awareness of identity theft can significantly reduce the harm suffered by the victims. Further, as an agency with law enforcement authority and investigative capabilities, we would immediately coordinate with other law enforcement agencies to apprehend the persons seeking to misuse the data.

Task Force Factor 4: No Evidence That the Compromised Information Is Actually Being Used To Commit Identity Theft

While it is possible that persons planning identity theft could intentionally delay their attempt to exploit the data, it is significant that it has been 1 year since the Doral laptop was stolen, and there has been no evidence of identify theft based on these databases. As of August 21, 2007, ID Analytics has concluded, based on comprehensive expert analysis of credit information relating to the affected individuals, that there has been no organized misuse of these data.

The reports from ID Analytics are consistent with the information we have developed in our own investigation. As noted above, the information concerning the Doral theft was widely distributed through individual letters to most of the people whose SPII was contained in the laptop's databases and through a posting on our website. In these notifications, we advised people to contact us if they believed they were victims of identity theft. As of August 23, 2007, we have finished investigating 38 of 39 complaints and thus far have not found any evidence of identity theft stemming from the stolen laptops.

FACTORS CONTRIBUTING TO THE LOSS OF SPII

Our review of the facts and circumstances surrounding the laptop thefts, indicates that the loss of SPII was a combination of three factors: (1) the laptops were not

protected from loss as well as they should have been; (2) the data on the two laptops had been decrypted to allow needed IT upgrades; and (3) SPII was being maintained on laptops, which are inherently more vulnerable than computer servers that operate in a secured environment.

Physical Security of the Laptops

Our examination of the two thefts found that although the OIG agents took some precautions, they could have done more to safeguard the laptops.

Prior to the two laptop thefts, neither DOT nor the OIG had specific policies for physically safeguarding laptop computers removed from an employee's regularly assigned workplace. As a result, it was left to the judgment of the individual special agents and their supervisors to determine how best to protect the equipment and information entrusted to their care. OIG policy required Office of Investigations employees to safeguard any information in their possession and to safeguard files from loss, theft, mutilation, and unauthorized disclosure.[19] OIG policy also directed that laptops should remain "in the possession of the OIG employee as much as possible."[20]

In the Doral incident, the laptop was stolen from an unoccupied Government vehicle while the agent was at lunch. While the vehicle was locked, this level of physical protection was not adequate for several reasons. First, the agent had been informed that his laptop had been decrypted and warned to protect the computer while the data was unencrypted. Second, the agent knew that the vehicle did not have a trunk and was parked in an area of South Florida with a high incidence of vehicle break-ins and thefts. Although the vehicle windows were tinted, the laptop was still visible through the back and rear windows. Lastly, the agent was aware of the widely publicized theft of the VA data and its consequences.

These considerations could have led the agent to properly conclude that his laptop, which contained SPII databases, should not be left unattended in his vehicle. Even if the laptop had to be left in the vehicle (i.e., in the event the agent had to quickly exit and leave the vicinity of the vehicle), it should have been covered to conceal it from view.

In the case of the stolen Orlando laptop, similar considerations apply. While the Miami SAC believed that she locked the conference room (she acknowledged that she did not recall specifically checking to ensure that it was locked), the laptop

---

[19] Operating Procedures Manual (OPM), Part 4 (JI) Chapter 1, Section 2. Similar guidance exists for Office of Audit staff at OPM, Part 2 (JA) Chapter 6: staff is directed to "safeguard working papers developed during an audit to ensure that they are not lost stolen or altered."

[20] OPM Part 1 (General and Administrative), Chapter 19, Paragraph 3(a)(2).

was unattended for approximately 45 minutes, and the Miami SAC should have anticipated that hotel staff might access the room and fail to re-secure it.

It also appears that the Miami SAC believed, at the time that her laptop was stolen, that the laptop contained cases files and that the laptop had been decrypted.[21] According to a copy of the police report, which we obtained after the Doral theft, she told the police officer that her laptop "contained several case files which are not encrypted due to computer conversions at work." Believing that the laptop contained sensitive information and that the information was not encrypted should have led the SAC not to leave the laptop unattended.

Encryption Capability Disabled at the Time of the Laptop Thefts

Although there was no Office of Management and Budget or DOT requirement to encrypt laptop data until August 7, 2006, it had been OIG policy since the OIG began issuing laptops, that users should store all data in a special folder that was pre-configured to be encrypted. All documents placed in this folder were automatically encrypted.

If the databases on the laptops had been encrypted at the time of the thefts, there would have been almost no risk of the data being misused. Unfortunately, we believe that neither stolen laptop was encrypted at the time of the thefts because of an IT upgrade that involved creating an active directory, installing new servers, and upgrading server software. This upgrade was needed because the existing network was approximately 10 years old and had become obsolete, inefficient, and more vulnerable to security threats.

Had the files been transferred in an encrypted form from the old operating system to the new system, the laptop users would have been unable to access these files after the transfer. Consequently, it was necessary to decrypt all files before their transfer. The upgrade plan was to decrypt all the computers, upgrade the various OIG offices in Headquarters and field locations in stages, and then simultaneously re-encrypt all the computers once all locations had been upgraded.[22] This was viewed by the OIG CIO staff as the most efficient method to minimize resource demands and the disruption of day-to-day OIG operations.

Decryption of OIG computers began on March 9, 2006, by running an automated program on the DOT network. This program automatically decrypted computers attached to the network unless the user stopped the process before it was

[21] Because we were unable to examine the actual laptop, we were unable to determine conclusively whether the laptop had been decrypted.

[22] Had some of the files been encrypted and some unencrypted, it would not have been possible for employees whose computer had been upgraded to exchange files with employees whose computer had not been upgraded. The last OIG computers, assigned to our Lakewood, Colorado, office, were upgraded on July 27, 2006.

completed. Thus, most of the OIG's computers were decrypted in March 2006. However, computers assigned to the Miami office were not decrypted at that time because Miami users accessed the OIG computer system through a Virtual Private Network (VPN). The nature of the VPN connection prevented those laptops from being decrypted by the automated program, so significantly more effort and end-user interaction was required to decrypt those laptops. The majority of the Miami laptops, including the Doral laptop, were decrypted on June 23, 2006, with assistance from a computer forensic agent who worked in that office.[23]

Although the OIG CIO office worked diligently to complete the process as quickly as possible, given the length of time required to complete the upgrade, we believe that the OIG's security certification required a more formal risk assessment with respect to the decryption of the laptops for such an extended period. At the time the decryption took place, the OIG Infrastructure Risk Assessment Report recognized that information stored on laptops is less secure and identified encryption as the method to address the increased risk. Specifically, the Report noted that, "access to encrypted files is controlled by user logon and provides extra protection to ensure the confidentiality and integrity of the data, which may not be physically secured due to the portability of the systems."

Under the Federal Information Security Management Act of 2002 (FISMA), agencies are required to continuously monitor their systems and assess whether changes to the system or the environment create any new vulnerabilities.[24] Because our Certification and Accreditation specifically identified encryption as a security measure employed to reduce the risk of storing sensitive information on laptop computers, the planned decryption of the laptops should have been identified as creating a security risk, especially given that the information would remain decrypted for at least several weeks.

The OIG CIO office advised us that it had assessed the risks associated with decryption. However, that assessment was not recorded in writing or shared with OIG senior management or investigations management in the field offices. The OIG CIO office did send an e-mail to the Miami investigations staff and other Virtual Private Network users in which it described the decryption process and advised them to "protect your PCs as files will no longer be encrypted." It did not, however, offer any specific guidance as to how the laptops should be protected,

---

[23] Had the Miami SAC's computer been decrypted at the same time as the rest of her office's computers, the data stored on it would have been encrypted at the time that laptop was stolen. Unfortunately, we have concluded that it probably was decrypted when the Miami SAC came to Headquarters on March 22 through 24 to prepare for the fraud prevention conference. Because the automated program was running on the OIG computer network, it would have decrypted her computer when she physically connected her laptop to the network unless she stopped the process. Since we have not recovered the laptop, there is no way to determine whether the program successfully decrypted the laptop.

[24] NIST Special Publication 800-53A "Guide for Assessing the Security Controls in Federal Information Systems." Chapter 3.4.

and those OIG employees who did not have to use a Virtual Private Network (VPN) to connect to the network did not receive this warning.

A more formal OIG-wide assessment of potential security risks associated with removing encryption and a discussion of whether compensating security measures should be employed would have been more consistent with OIG's information security certification. Our favorable history with regard to maintaining control over laptops may have caused the CIO office to underestimate the risk of laptop theft. Prior to the Orlando theft, we had only lost one laptop. That laptop, which was lost in 2001, had been assigned to an auditor and was determined not to contain any sensitive information. Until the Orlando theft, the Office of Investigations had never lost a laptop. Nevertheless, a formal risk assessment would have given OIG decision makers the opportunity to decide whether these risks were acceptable and whether additional steps were needed to mitigate the risks.

It should also be noted that the OIG CIO has significant responsibilities in addition to Information Resources Management. The OIG CIO also serves as the Chief Financial Officer and as the head of Administration, positions that have their own time-consuming and mission-critical responsibilities.[25] Although we do not believe that the additional responsibilities contributed to the loss of control over SPII, given the increasingly complex and fast-paced demands the OIG faces with respect to effective management of information technology and computer security, as well as financial management and general administration, consideration should be given to establishing a separate CIO within OIG whose only responsibilities are to manage our information technology program, including information resources and computer security. This would be more consistent with best practices, which generally call for Information Resources Management to be the primary duty of a CIO.[26]

It is also true that anyone in OIG management who was familiar with the sensitivity of the type of information stored on special agents' laptops could have recognized the increased vulnerabilities presented by decrypting the information on the laptops and taken steps to mitigate those risks. Persons in the Office of Investigations who were familiar with the sensitivity of the information stored on Special Agents' laptops include the Special Agent in Charge, the Deputy Assistant Inspector General for Investigations,[27] the Assistant Inspector General for Investigations, and the Acting Inspector General. Had these individuals been

[25] In 2001, the Deputy Inspector General designated the Chief Financial Officer/Director of Administration, who had qualifications and prior experience as an IT professional, as OIG's CIO.

[26] The Clinger-Cohen Act, 40 U.S.C. 1401(3) requires that larger Federal agencies appoint a CIO with information resources management duties as that official's primary duty. Although not required, it is also considered a best practice for smaller agencies and agency components.

[27] Because OIG's Office of Investigations was subsequently reorganized, this position no longer exists.

more sensitive to the risks associated with decrypting the laptops used by OIG special agents, they might have recognized the increased vulnerabilities presented by the decryption and taken steps to mitigate those risks.[28]

SPII Databases Stored on Laptops

At the time of the laptop thefts, the OIG, like most Government agencies, did not have specific procedures for handling SPII. It fell within the general category of sensitive information to which OIG employees were expected to apply appropriate judgment to protect. In the case of special agents, the OIG Operating Procedures Manual stated, "All JI employees must safeguard files from loss, theft, mutilation, or unauthorized disclosure."[29] OIG procedures also called on special agents to "prevent the accumulation of unnecessary documentation and files."

Because laptops are inherently more vulnerable to theft than computers that operate in a secure environment, properly safeguarding files from disclosure requires making judgments about what kind of information can prudently be stored on a laptop. Because of the significant damage that can occur from disclosure of SPII, storing SPII databases on laptops is unwise. Unfortunately, our special agents and their supervisors did not sufficiently recognize the sensitivity of the data or the risk associated with keeping this data on laptop computers.

OIG ACTIONS TAKEN TO PREVENT LOSS OF CONTROL OVER SPII IN THE FUTURE

We determined the factors involved in the loss of control over SPII so that we could focus our efforts to prevent any future occurrences. Our efforts to accomplish this have been in four areas: (1) improving physical security of the laptops, (2) encrypting all data and deploying two-factor authentication, (3) storing SPII in a more secure fashion, and (4) improving employee awareness to protect SPII.[30]

We Have Improved Laptop Physical Security

Both DOT and the OIG are taking actions to strengthen guidance provided to employees related to the safeguarding of computers and the information contained

---

[28] For example, SACs and special agents could have been advised to take additional precautions, such as removing SPII from the laptops.

[29] "JI" is the designation used for investigations personnel.

[30] By re-encrypting the data and enacting policies regarding the inventory and oversight of sensitive information, we complied with Office of Management and Budget requirements for the protection of sensitive information that took effect on August 7, 2006. The May 22, 2006, memorandum from Office of Management and Budget (M-06-15) is posted on the Internet at www.whitehouse.gov/omb /memoranda/fy2006/m-06-15.pdf.

on them. We have issued new policies regarding properly securing unattended laptops[31] and have issued cable locks to all laptop users. These locks prevent the laptop from being undocked while in the user's office and provide an effective way to secure the laptop while on travel.

In addition, we have provided all employees with guidance developed by DOT regarding the security of portable computers. That guidance includes the following:

> When carrying portable computers or portable storage devices while on travel or when working outside of their normal DOT workspace (e.g., teleworking), employees shall take all reasonable precautions to protect these items against loss or theft. Employees shall not leave computer or portable storage devices unattended and in the open in their homes, hotel rooms, vehicles, places of public transportation, or offices they are visiting. If cable locks are available, they should take them while traveling and use them as necessary to secure portable computers.[32]

We Have Encrypted all Data on the Laptops and Implemented Two-Factor Authentication on all Laptops

We have significantly strengthened the data security on our laptops. All OIG laptops now have their entire hard drive encrypted using a system called "SafeBoot." This system uses strong pre-boot user authentication and powerful encryption to prevent unauthorized access.

In addition, all OIG laptops now employ two-factor authentication. In addition to typing in a password, the user has to insert a small token into the laptop's USB port to access data on the laptop. Two-factor authentication significantly reduces the chances that unauthorized persons could access data on the laptop. Even if unauthorized persons gained control of the laptop, they would need to both defeat the password and obtain the token before they could access any of the data on the laptop.

To further ensure that sensitive information is encrypted, OIG users' computer is automatically checked to determine if the encryption process is functioning as intended whenever they log onto the OIG network. If it is not functioning

---

[31] As an interim measure, while a new policy was being developed, OIG employees were instructed not to leave Government laptops or electronic storage media unattended in vehicles under any circumstances.

[32] This guidance was originally developed by DOT in 2000 but was not widely distributed, and copies were not easily obtainable. Following the loss of the Doral laptop, this policy was posted on the DOT Intranet and is referenced in the Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII), which was issued on October 11, 2006.

properly, the OIG CIO office is notified so that corrective action can be taken immediately.

We Have Begun Storing SPII in a More Secure Fashion

On August 7, 2006, the Acting Inspector General directed that all OIG employees remove any databases containing SPII from laptops and ensure that all other sensitive information is stored in encrypted folders. Each OIG employee was required to certify compliance with this requirement, and OIG managers were instructed to verify employees' compliance.

All databases containing SPII were removed from OIG laptops and either deleted if no longer needed or moved to a secure OIG network server. In addition, all remaining databases containing SPII were inventoried to enable supervisors to monitor and keep track of this sensitive information. Sensitive information will be periodically reviewed and removed when no longer needed.

Because the only computers assigned to most special agents and most other OIG employees are laptops, each user has been assigned a "home drive" on a network server that can be used to store sensitive information. This drive is physically located on a non-portable server that operates in a secure environment but allows access only to the specific user.

We Have Increased Employee Awareness of the Need To Protect SPII

On August 2, 2006, the OIG CIO circulated to all OIG employees a message from the DOT CIO reminding all DOT employees and contractors about the importance of safeguarding SPII. The Acting Inspector General held an all-OIG employee web cast on August 14, 2006, to reinforce requirements for safeguarding information on computer hardware and storage media.

In addition, to reinforce awareness of departmental security polices, during August 2006, all OIG employees were directed to re-certify that they had read and understood departmental guidance on safeguarding information and computer security. Employees were also required to complete DOT's on-line Privacy Act Awareness Training course emphasizing the importance of protecting information and the proper techniques for handling personal information. OIG employees completed these actions by August 30, 2006.

In connection with the implementation of the SafeBoot system, all laptop users were required to review a guide that outlines the use of the locks and stresses the importance of protecting laptop data. In addition, all laptop users were required to watch a training video that illustrates the various ways in which laptops can be

stolen and highlights the significant damage that an organization can suffer when it loses control of a laptop computer.

CONCLUSIONS AND RECOMMENDATIONS

The loss of control over the SPII databases had three primary causes:

- Inadequate protection of laptops by OIG employees;
- Our removal of encryption from sensitive data during a system upgrade; and
- Our storage of SPII on laptops, which are inherently less secure than desktops or servers that remain in a secure operating environment.

While these causes involved various individuals and circumstances, they were all a consequence of an insufficient emphasis on protecting sensitive information from loss. Like many other agencies, our security focused more on safeguarding physical property rather than information. Given the rise in identity theft and other misuse of personal information, the variety of information that is collected by the Government and private parties, and the amount of information that can now be stored on easily portable devices, this mindset cannot continue.

While it is unlikely that any of the lost SPII will be misused, approximately 138,000 people were exposed to an unacceptably high risk that their personal information would be improperly disclosed and possibly misused. Given the severity of the personal and financial disruption that victims of identity theft suffer, creating this level of risk is unacceptable.

This failure to adapt to the new demands created by changes in information technology is not limited to our office. Very few Government agencies had policies relating to the treatment of SPII at the time of the VA theft, and very few required encryption of sensitive data stored on laptops. Current Office of Management and Budget policies on this subject were drafted in the wake of the VA theft, and the requirement that agencies encrypt all sensitive data stored on mobile computers and other mobile devices did not take effect until August 7, 2006.

It is impossible to completely eliminate the risk that an agency will lose control of sensitive data. There is, for example, no way to eliminate the possibility that a trusted employee with access to sensitive data will disregard agency policy and recklessly or intentionally expose sensitive information to improper disclosure. Ensuring that these changes do in fact result in increased protection of SPII will require the continued involvement of OIG senior management. Specifically, OIG senior management must:

1.) Evaluate the effectiveness of recent OIG improvements, such as installing the SafeBoot encryption software, using two-factor authentication, deploying cable locks, and providing each OIG employee with a home drive on the network;

2.) Ensure that both new employees and existing employees receive adequate privacy awareness training.

3.) Perform periodic reviews of data stored on OIG laptops and document compliance with policies regarding the storage of SPII and other sensitive data; and

4.) Consider separating the CIO and CFO/Administrative functions, so that one senior OIG management official will have information resources management as their primary responsibility.

#