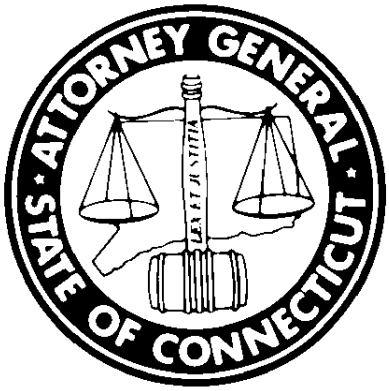

REPORT OF THE ATTORNEY GENERAL AND AUDITORS OF PUBLIC ACCOUNTS

Investigation pursuant to Conn. Gen. Stat. §4-61dd concerning alleged mishandling of taxpayers' Social Security numbers at the Department of Revenue Services

October 13, 2009

RICHARD BLUMENTHAL
ATTORNEY GENERAL

ROBERT G. JAEKLE
AUDITOR OF PUBLIC ACCOUNTS

KEVIN P. JOHNSTON
AUDITOR OF PUBLIC ACCOUNTS

EXECUTIVE SUMMARY

On Friday, August 17, 2007, a laptop computer was stolen from the automobile of Jason Purslow in Islandia, New York. Purslow is an employee of the State of Connecticut Department of Revenue Services (hereinafter "DRS") and the laptop was State property. It was subsequently discovered that the laptop contained the names and Social Security numbers of more than 106,000 Connecticut taxpayers.

DRS has spent more than one million dollars to remediate this data loss and provide identity theft protection to affected taxpayers. To date, no misuse of taxpayer information has been definitively connected to this theft, but the whereabouts of the laptop and its confidential content remains unknown.

Following the laptop theft, the Auditors of Public Accounts and the Attorney General received numerous complaints alleging that DRS was mishandling taxpayer confidential information putting Connecticut taxpayers at risk for identity theft crime and misuse of confidential information. Additional complaints alleged that DRS failed to properly investigate and respond to the theft of the laptop.

The Auditors of Public Accounts and the Attorney General investigated these allegations, including DRS protection of taxpayer information in electronic form as well as its internal inquiry concerning the laptop theft. Seventeen DRS employees testified to investigators on the record and under oath. In addition, investigators examined numerous documents, in excess of 2,000 pages, provided by witnesses and DRS.

The evidence obtained during this investigation supports the following findings:

1. At the time of the laptop theft, DRS policies, procedures and protocols for handling and securing confidential consumer tax information were deficient. These deficiencies exposed taxpayers to identity theft and invasion of privacy and directly contributed to the loss of confidential information for 106,000 state taxpayers. Specific deficiencies included:

- Any DRS employee with computer network access could access from his or her computer many electronic files containing taxpayer information—including a file holding the information of over two million taxpayers. Also lacking were reliable records identifying the DRS employees accessing these data bases. Any DRS employee could see, change or take any information stored on another employee's computer without the knowledge or consent of co-workers. Some of these deficiencies were being addressed at the time of the laptop theft.

- DRS treated improper access to taxpayer information by its employees as a personnel matter, failing to notify taxpayers or criminal authorities.

- DRS failed to monitor or track where all electronic files containing taxpayer information were stored. DRS "strongly recommended" without requiring that employees store taxpayer information on the DRS primary network rather than on individual desktop or laptop computers.

- Although James Norton, Chief of the Internal Audit, Planning and Development Division and others within DRS advised that the agency should require that all information on laptops be encrypted, DRS failed to do so because of technical problems. The information on the stolen laptop was not encrypted.

- Although permitted by State law, DRS's use of real taxpayers as test subjects when developing new electronic systems increased the risk that information would be lost or compromised.

2. DRS's failure to properly manage confidential taxpayer information contributed to the loss of taxpayer information on a laptop.

- Jason Purslow was a DRS Tax Unit Supervisor responsible for the DRS Electronic Commerce Unit, which developed, tested and implemented electronic systems allowing taxpayers to file returns by telephone and through the internet. State law allows employees such as Mr. Purslow to use confidential taxpayer to test DRS tax collection systems, including systems Purslow helped create.

- As part of his duties, Mr. Purslow used a laptop to provide training on electronic tax collection. The laptop also was assigned to enable the agency's tax collection efforts from a remote location in the event of a disaster.

- DRS Information Technology personnel prepared Mr. Purslow's laptop by transferring onto it all information on Mr. Purslow's desktop computer, including the confidential information of 106,000 taxpayers. Neither Mr. Purslow nor the DRS personnel preparing his laptop computer reviewed the content. They were unaware of the unencrypted confidential information of 106,000 taxpayers transferred to the laptop.

- Mr. Purslow took the laptop computer on a weekend family trip to complete critical testing of a new DRS system scheduled to be activated that Monday. The planned testing did not involve or require the taxpayer information unknowingly transferred to Purslow's laptop.

- The laptop was stolen from Mr. Purslow's car outside the hotel where he was staying approximately between 5:00PM and 9:00PM on Friday, August 17, 2007.

3. DRS failed to respond promptly to the theft of the laptop computer.

- During a Saturday, August 18, 2007, conference call, Mr. Purslow informed a number of DRS employees, including several senior managers, that his laptop was stolen. Returning

to work on Monday, August 20, Purslow formally reported the theft to DRS Business Office, Information Services Division, and Internal Audit Division.

- Between August 18 and August 23, no steps were taken to determine whether confidential taxpayer information was stored on the stolen laptop. While the theft of a DRS laptop should have raised alarms that confidential taxpayer information was at risk, DRS personnel aware of the theft assumed that the laptop was Purslow's personal property or that it had no taxpayer information.

- DRS at that time had no established procedures to address information breaches or losses. There was no clear understanding among the various divisions within DRS as to which one should take action when such breaches or losses occurred.

- When James Norton, Chief of the Internal Audit, Planning and Development Division returned from vacation on August 23, he immediately questioned Purslow about the theft of the laptop and quickly determined from a review of Purslow's desktop computer that the stolen laptop contained taxpayer information. Norton informed Commissioner Law and others of his findings that day. After further investigation, Norton informed Commissioner Law on Sunday evening that the laptop contained the tax return information of 106,000 taxpayers. More than a week had passed since the theft.

- By August 31, DRS had notified all 106,000 taxpayers that their confidential information may have been compromised and offered them identity theft protection.

- No instances of identity theft have been identified as related to the stolen laptop. The significant delay notifying taxpayers caused by DRS's five day lapse in detecting the data loss increased the time period during which taxpayers had no knowledge of the loss of their confidential information and, therefore, no opportunity to address potential misappropriation or misuse of their information by identity thieves.

- On October 9, 2007 DRS completed an internal disciplinary investigation of the theft and suspended Purslow for 30 days without pay.

4. DRS appears to have conducted a proper and timely internal disciplinary investigation of the loss of the laptop computer.

- DRS appointed Cheryl Burdick, the DRS Internal Auditor, to investigate the loss of the laptop computer. Although James Norton was her supervisor, and previously held the position of Internal Auditor, and knew the most about this type of security breach, he was not asked to lead the investigation. Instead, he was assigned to assist Burdick.

- It was alleged that James Norton was removed from the internal DRS investigation because he raised concerns about the investigation and wanted to pursue questions that might subject DRS senior management to criticism. This allegation was not substantiated. According to the testimony from DRS employees presented to this office, Mr. Norton was not assigned to lead the investigation because it was to be a disciplinary

investigation and there was concern about the perception that he had already formed opinions as to culpability. Ms. Burdick was therefore directed to lead the investigation with Mr. Norton and others assisting.

- The DRS internal investigation did not pursue the question of whether DRS management properly handled the theft of the laptop computer. DRS's investigation focused only on the loss of the laptop computer. Subsequent actions of DRS management were not directly relevant to that inquiry. DRS management assumed that the Auditors of Public Accounts and the Office of the Attorney General would investigate those issues.

5. Since the laptop theft, DRS has identified and taken corrective actions to provide greater protection to taxpayers' confidential information. The agency has:

- Implemented greater restrictions on taxpayer information access and storage;

- Established more comprehensive procedures to protect taxpayer information;

- Encrypted laptops and electronic mobile storage devices.

CONCLUSIONS

1. The failure of DRS to implement effective security and tracking measures contributed to loss of the confidential information of 106,000 taxpayers.

2. The laptop should not have contained the taxpayer information transferred from Purslow's desktop. If there were a legitimate need to store taxpayer information on the laptop, it should have been encrypted.

3. The failure of DRS to immediately investigate whether the laptop contained confidential taxpayer information exposed taxpayers to an additional five days of possible identity theft and financial harm. After that initial failure, DRS management properly and quickly took steps to protect taxpayers whose information was compromised.

4. DRS conducted a proper disciplinary internal review, assigning its personnel to avoid possible issues in taking future disciplinary action. It was reasonable for DRS to leave the question of management fault to an independent review by the Auditors of Public Accounts and the Attorney General.

5. Since the theft of the laptop computer, DRS has taken significant steps to increase the security of taxpayer information, including establishment of greater restrictions on taxpayer information access, storage and protection, as well as encryption of laptops and other mobile electronic devices.

6. DRS should take additional measures to ensure that all employees understand the seriousness of data breaches and further safeguard confidential taxpayer information.

RECOMMENDATIONS

This investigation identified changes necessary to adequately protect taxpayer information in electronic form at DRS:

1. DRS should train all employees to spot data breaches and teach them what to do if they happen. DRS should hold employees accountable if they fail to follow data breach protocols and procedures.

2. DRS should continue ongoing efforts to update its computer networks so that all confidential taxpayer information is tracked and secured.

3. DRS should study how other states and federal entities such as the Social Security Administration and the Internal Revenue Service test new computer systems, and then reduce as much as possible use of taxpayer "test subjects" in designing and testing new computer systems.

4. DRS should notify affected taxpayers and law enforcement agencies if a DRS employee improperly accesses taxpayers' information so judgments can be made whether a criminal investigation or other action is warranted.

REPORT

This investigation received testimony on the record and under oath from numerous DRS personnel. This included former DRS Commissioner Pamela Law, Deputy Commissioner (now Commissioner) Richard Nicholson, Chief of Staff Christina Lawson, Tax Unit Supervisor Jason Purslow and other personnel involved in responding to the laptop theft. The investigation also involved a review of extensive documentation from DRS concerning the storage and security of taxpayers' information within the agency, the theft of Purslow's laptop in August 2007, and the agency's response to that theft.

1. At the time of the laptop theft, DRS policies, procedures and protocols for handling and securing confidential consumer tax information were deficient. These deficiencies exposed taxpayers to identity theft and invasion of privacy and directly contributed to the loss of confidential information for 106,000 state taxpayers. Specific deficiencies included:

- **Any DRS employee with computer network access could access from his or computer many electronic files containing taxpayer information—including a file holding the information of over two million taxpayers.**

In his work at DRS and his testimony, James Norton, Chief of the Internal Audit, Planning and Development Division, took the position that access to taxpayer information in electronic form should be strictly limited to only those DRS employees that needed access for business purposes. From Norton's point of view, other DRS managers wanted employees to have broader access to taxpayer information.

In February 2007, Norton discovered that many electronic files containing taxpayer information—including a file holding the information of over two million taxpayers—were stored on the DRS network in such a way that any DRS employee with access to network had access to the files. Moreover, there was no measure that recorded access to the files. Eventually, through the intervention of Norton, many of the files were made more secure by limiting access to them.

- **Also lacking were reliable records identifying the DRS employees accessing these data bases.**

Norton testified that, also in February 2007, he and Cheryl Burdick discovered that, instead of disabling the identifications of departing employees and providing new employees with new identifications, identifications had been reassigned from one employee to another. In other words, employees were effectively sharing an identification granting them access to the DRS computer network. This meant that there was no reliable record identifying which employees accessed what information in the event that questions or problems arose with respect to which employees accessed what information.

Burdick confirmed that she discovered that employees were using identifications that were supposed to be assigned to different employees as well as some missing identifications that

prevented her from determining which employee had accessed return information. Eventually, Burdick was able to ascertain which employees were assigned which identifications and confirmed that reassignment of identifications had stopped.

- **Any DRS employee could see, change or take any information stored on another employee's computer without the knowledge or consent of co-workers.**

These issues came on the heels of a concern Norton raised in November 2006 about the fact that all DRS employees could access files stored on the C: Drive of other employees without the other employee's knowledge. Put another way, any DRS employee could see, change, or take any information stored on another employee's computer without the knowledge or consent of their co-worker. Eventually, this C: Drive access was restricted—approximately one year after Norton alerted others within DRS to the problem.

Norton testified that an electronic file containing return information should be stored on a computer's C: Drive only when the file was needed for immediate use. Commissioner Law also believed that even prior to the laptop theft DRS policy was that taxpayer information in electronic form was to be stored on the agency network, not the individual computers or laptops of employees. However, Law testified that no one within DRS was monitoring or tracking where electronic files containing return information were stored.

- **DRS treated improper access to taxpayer information by its employees as a personnel matter, failing to notify taxpayers or criminal authorities.**

It has been the practice of DRS to treat incidents of employees improperly accessing taxpayers' confidential information, referred to within the agency as "browsing," as a personnel matter. If an internal investigation concluded that an employee had improperly accessed taxpayer information, DRS would discipline the employee, typically by suspending them from work without pay for a period of days. DRS would not notify the taxpayers whose information was improperly accessed. DRS would not alert outside law enforcement agencies to the incident. This report concludes with a recommendation that DRS notify affected taxpayers and outside law enforcement agencies of these incidents because a review of State laws supports the conclusion that such conduct may be criminal and contrary to State law.

James Norton testified that in December 2005 he raised the issue of whether outside law enforcement agencies and taxpayers should be notified when it was determined that a DRS employee had accessed a taxpayer's return information. Norton could not recall what if any response he received when he raised these concerns.

According to Commissioner Pamela Law, when an internal audit uncovers evidence suggesting an employee accessed taxpayer information without a business purpose and an internal investigation confirms that improper access took place, the employee is disciplined. Law testified that DRS does not notify taxpayers when their information has been improperly accessed or inform outside law enforcement agencies of the improper access. Although Law does not recall any formal meetings concerning notification of taxpayers or law enforcement, she

believes that Norton may have raised the issues with her in the past, at which point she asked him to provide more information.

Deputy Commissioner Richard Nicholson testified that he does not have a role in responding to incidents of improper access to taxpayer information. According to Nicholson, taxpayers are not notified when their information has been improperly accessed by DRS employees. Nicholson stated that he was not aware of any discussions at DRS about whether to notify taxpayers. Nicholson was also not aware of whether outside law enforcement agencies were notified when employees had improperly accessed taxpayer information. Nicholson, however, did not remember that specific exchange with Norton. Nicholson generally recalled past discussions in the agency that DRS would notify outside law enforcement if an employee ever improperly accessed *and disseminated return information outside DRS*. Nicholson did not believe that improper access—occurring within DRS, but not resulting in dissemination of taxpayer information outside the agency—violated State law concerning access to taxpayer information.

Chief of Staff Christina Lawson believed that it was DRS's practice to notify taxpayers, but not outside law enforcement agencies when the taxpayers' information was improperly accessed. Lawson served no role in the investigation or disposition of such incidents. She did not remember discussing whether the agency should notify taxpayers of improper access.

Director of Internal Audit Cheryl Burdick described her work investigating complaints of employees improperly accessing return information. Burdick receives such complaints from Calvin Mellor, Chief Enforcement Agent, and James Norton. Upon receipt of an improper access complaint or evidence that creates an improper access concern, Burdick examines records including personnel files and return information access histories in order to attempt to determine whether improper access has occurred. Burdick also interviews the employee and their supervisor as part of her investigative process. Burdick concludes her work on these matters by either finding a proper business purpose for the access or referring the matter to human resources for possible disciplinary action. Burdick does not have a role in the disciplinary process. Burdick was not aware of taxpayers receiving notification when their information has been the subject of improper access or law enforcement outside DRS receiving notification of instances of improper access. Burdick stated that, as of the date of her testimony to this investigation, she had not uncovered actual wrongdoing during her investigations.

Calvin Mellor, Chief Enforcement Agent, testified that on rare occasions he investigates crimes occurring within DRS. Mellor explained that in the past he investigated incidents of employee stealing and cashing checks from DRS. Mellor did not recall investigating the theft of DRS property or employees' property before the theft of Purslow's laptop. Mellor recalled one instance when he investigated a DRS employee for committing a crime within DRS and as part of the investigation Mellor discovered that the employee had improperly accessed return information. In the ordinary course of business, however, Mellor does not investigate complaints alleging improper access of return information as a potential crime and was not aware of any other incidents where DRS treated employees' improper accessing of taxpayer information as a criminal matter.

- **DRS failed to monitor or track where all electronic files containing taxpayer information were stored.**

Commissioner Pamela Law testified that no one within DRS was regularly monitoring or tracking where electronic files containing taxpayer information were stored before the laptop theft in August 2007.

Deputy Commissioner Richard Nicholson testified that before the laptop theft DRS had guidelines advising employees to store taxpayer information on network drives to insure the information was "backed up". Nicholson did not remember whether the guidelines were mandatory before the laptop theft. Nicholson understood that random auditing of taxpayer information occurred and that DRS Information Services Division (ISD) was able to monitor activity within the DRS computer network, but he was not certain whether anyone within DRS was tracking taxpayer information. Nicholson believed that Internal Audit personnel, including James Norton and Cheryl Burdick, would take steps to rectify the improper storage of taxpayer information should such concerns arise.

Christina Lawson testified that DRS ISD and IAPD work together to audit and track movement of electronic files containing taxpayer information. However, Lawson was not aware of anyone within the agency specifically tasked with taking corrective action when electronic files containing taxpayer information where found stored improperly.

Cheryl Burdick, Director of Internal Audit, testified that she performs both regular and *ad hoc* audits to determine whether employees have a proper business purpose for accessing taxpayer information, including taxpayer information in electronic form. However, Burdick further testified that she was not aware of anyone within DRS that was tasked before August 2007 with tracking where taxpayer information in electronic form was kept or acting to rectify the improper storage of taxpayer information in electronic form. When discussing her internal investigation of the laptop theft, Burdick commented that the question of whether there was adequate management and supervision of Purslow could not be reviewed during the investigation because DRS had no procedure for documenting or tracking the content of laptops and, therefore, there was nothing for Purslow's managers to supervise in that respect.

Jason Purslow recalled a series of documents about protecting taxpayer information being circulated to DRS employees, but did not remember attending any meetings about safeguarding taxpayer information in electronic form before his laptop was stolen. Purslow recalled that agency policy required that taxpayer information be kept secure, which he understood to consist of password protection and keeping the taxpayer information in the building. Purslow remembered receiving guidance to the effect that information *should* be stored on DRS network drives instead of individual computer hard drives because information on hard drives was not "backed up." In other words, the information would not be protected from loss should the individual computer suffer damage or a system failure of some sort. This suggestion was never communicated to Purslow as a security concern. Aside from the instruction to lock the laptop in a file cabinet when not in use, Purslow did not remember any other instructions on laptop safekeeping. Purslow did not recall receiving any notice of restrictions on information storage on laptops.

Calvin Mellor testified that his main duties were the investigation of tax crimes and enforcement action where such crimes had occurred. Accordingly, Mellor does access taxpayer information when performing his duties and he recalled receiving some instructions on securing taxpayer information. Mellor did not remember instructions specific to taxpayer information *in electronic form* or directions regarding where within the DRS computer system taxpayer information should be stored. Mellor understood the instructions to essentially require that taxpayer information be kept secure and confidential, and such information should be shared or disclosed only when required. Mellor did not know whether anyone within DRS was tracking taxpayer information in electronic form or taking action when taxpayer information in electronic form was discovered stored improperly.

- **DRS "strongly recommended" without requiring that employees store taxpayer information on the DRS primary network rather than on individual desktop or laptop computers.**

Before the laptop theft, DRS "strongly recommended" that employees store information in electronic form on the agency computer network instead of individual computer hard drives. This recommendation alerted employees to the risk that information stored on individual hard drives could be lost because hard drives did not preserve information with the same "back up" process used to preserve information on the network. Since the laptop theft, storage of information on individual hard drives has been restricted by a mandatory agency directive.

- **Although James Norton, Chief of the Internal Audit, Planning and Development Division and others within DRS advised that the agency should require that all information on laptops should be encrypted. DRS failed to do so because of technical problems. The information on the stolen laptop was not encrypted.**

James Norton testified that before the laptop computer theft in August 2007 DRS policy required employees to treat their laptops as they would any other valuable property. Furthermore, employees should keep only necessary information on laptops.

According to Norton, encryption, a process whereby information is transformed so that it is unusable to anyone except those who should be allowed access, had been proposed and discussed within DRS as a means of protecting electronic files on agency laptops. However, it had not been installed to protect laptops deployed to DRS employees. Efforts to encrypt laptop computer were underway before the theft of the laptop computer in August 2007. Norton and others within DRS had proposed that all laptops be encrypted. These efforts were stymied, however, by aspects of the DRS computer network that caused encrypted laptops to become inaccessible when regularly scheduled password changes occurred.

As a result, at the time of the laptop theft in August 2007, Purslow's laptop was not encrypted.

- **Although permitted by State law, DRS's use of real taxpayers as test subjects when developing new electronic systems increased the risk that the information may be lost or compromised.**

DRS uses real taxpayers as test subjects when developing new electronic systems. Although permitted by State law, this is a problematic practice because any use, transfer or manipulation of a taxpayer's information increases the risk that the information might be lost or misused.

James Norton testified that he raised the issue of whether real taxpayers' return information should be used to test DRS systems. Norton believes that fictitious taxpayer information could be generated, but currently DRS is not seeking to make that change.

Commissioner Pamela Law testified that she has some knowledge of DRS using real taxpayers' information to test agency systems, but there had been discussions in passing about ending that practice. Law believed it was the responsibility of James Norton and the Information Services Division to look into means of eliminating the use of real taxpayer information. Law understood that James Norton was looking into the matter, but she had not yet received any recommendation from him.

Jason Purslow is involved in most if not all testing of new electronic systems at DRS. Purslow explained that DRS tries to use fictitious taxpayer information to test its systems, but in some cases the agency still uses real information for testing purposes. Testing with real taxpayer information allows for a greater number of problems to arise and be corrected during testing. Purslow stated that DRS is always looking for ways of improving the security of return information.

2. DRS failure to properly manage confidential taxpayer information contributed to the loss of taxpayer information on a laptop.

Through interviews of DRS employees and examination of pertinent documentary evidence, the series of events that led to the loss of the laptop holding more than 106,000 taxpayers' confidential information were investigated.

- **Jason Purslow was a DRS Tax Unit Supervisor responsible for the DRS Electronic Commerce Unit, which developed, tested and implemented electronic systems allowing taxpayers to file returns by telephone and through the internet.**

In 2007, Jason Purslow was a DRS Tax Unit Supervisor responsible for the DRS Electronic Commerce Unit. In recent years, Purslow's unit has developed and implemented electronic systems to allow taxpayers to file returns by telephone and through the Internet.

- **State law allows employees such as Mr. Purslow to use confidential taxpayer information to test DRS tax collection systems, including systems Purslow helped create.**

Purslow knew taxpayer information was stored on his desktop in his office. Purslow used the information to help develop and test electronic and computer systems for DRS. It was not until after the theft, however, that Purslow stated he learned that taxpayer information was copied from his desktop onto his laptop.

DRS uses taxpayers' confidential return information to test systems at the agency. State law, Conn. Gen. Stat. § 12-15, permits DRS to use return information for this purpose. The practice of using taxpayers as test subjects will be addressed in the recommendation section of this report.

- **As part of his duties, Mr. Purslow used a laptop to provide training on electronic tax collection. The laptop also was assigned to enable the agency's tax collection efforts from a remote location in the event of a disaster.**

Purslow's duties included travel and training outside his office. DRS provided Purslow with a laptop to enable him to perform these duties. Purslow was also tasked to use a laptop to continue DRS's tax collection operations from a remote location as part of the agency's contingency plan for a disaster.

In April 2007, Jason Purslow received a new laptop to enable him to continue to perform his duties as described above.

- **DRS Information Technology personnel prepared Mr. Purslow's laptop by transferring onto it all the information on Mr. Purslow's desktop computer, including the confidential information of 106,000 taxpayers. Neither Mr. Purslow nor the DRS personnel preparing his laptop computer reviewed the content. They were unaware of the unencrypted confidential information of 106,000 taxpayers had been transferred to the laptop.**

After the laptop theft, an investigation uncovered that the laptop Purslow received in April 2007 in all likelihood contained more than 106,000 taxpayers' confidential information. This information arrived on Purslow's laptop through the process used to prepare the laptop for Purslow's use. Instead of manually adding the necessary applications and data to Purslow's laptop, the DRS Information Services Division (hereinafter "DRS ISD") used a program known as "PC Mover" to copy all of the content, including all applications and data, from Purslow's desktop onto his laptop.

The DRS internal investigation determined that Purslow was told PC Mover would copy the data from his desktop onto his laptop and that Purslow was instructed to "clean up" the content of his desktop before PC Mover was used to make the copy.

Purslow, however, does not recall any communications advising him that ***all data*** would be moved from his desktop to his laptop. Purslow did not remember any discussions about *how* the laptop would be prepared and applications moved from his desktop. Purslow does not recall receiving instructions to clean unnecessary files off his desktop or any mention of the PC Mover

application at the time his new laptop was prepared for him. Purslow testified that upon receipt of the laptop in 2007 he understood the laptop would contain all the applications on his desktop. Purslow stated that the confidential taxpayer information on his desktop did not need to be moved.

- **Mr. Purslow took the laptop computer on a weekend family trip to complete critical testing of a new DRS system scheduled to be activated that Monday. The planned testing did not involve or require the taxpayer information unknowingly transferred to Purslow's laptop.**

During the afternoon of Friday, August 17, 2007, Purslow and his son traveled to Islandia, New York for his son's youth hockey tournament.

Purslow brought his laptop with him because the DRS Taxpayer Service Center (hereinafter "TSC") was scheduled to "go live," that is, be available for public use that Monday. The final decision about whether to "go live" depended upon testing by Purslow producing positive results. The testing concerned final corrections to the TSC that would be made on Friday afternoon and needed to be checked Friday night before a conference call scheduled to occur on Saturday morning, at which time the "go live" decision would be confirmed. Purslow believed that unless he performed the testing Friday night the activation of the TSC would have to be delayed. Purslow recalls discussing with others at DRS that he had committed to take his son on this trip, but would perform the testing Friday night while on the trip. Purslow does not believe he mentioned his intended means of testing—the laptop—to anyone. Purslow brought the laptop so that he could access the Internet from his hotel room, thereby completing the testing while also meeting his obligation to supervise and care for his son.

The confidential taxpayer information that had been transferred onto Purslow's laptop was not needed for the testing Purslow intended to perform that weekend. Purslow repeatedly indicated during his testimony that he did not know that taxpayer information was on his laptop that weekend.

- **The laptop computer was stolen from Mr. Purslow's car outside the hotel where he was staying approximately between 5:00PM and 9:00PM on Friday, August 17, 2007.**

Purslow and his son drove in Purslow's personal automobile, taking a ferry from Bridgeport, Connecticut to Port Jefferson, New York and arriving at the Marriott Hotel in Islandia, New York at approximately 5:00PM. Upon arrival at the hotel, Purslow carried some items inside, but left the laptop and some of his personal valuables in his automobile. Purslow believed that the laptop and other valuables were secure because his automobile had tinted windows and he remembered locking its doors.

Purslow returned to his automobile at approximately 9:00PM and noticed that the laptop was not there. Purslow recalled that he "freaked out a little" at that moment. However, Purslow did not believe the laptop was stolen because he observed no sign of forced entry and, moreover, saw that several personal valuables remained in the vehicle where he left them. Purslow thought

he left the laptop at home and tried to call his wife to ask about it, but could not reach her. Purslow proceeded to use internet access at the hotel's "Business Center" to perform the testing.

Purslow testified that he used fictitious taxpayer information to perform the testing that night. The DRS internal investigation, however, determined that Purslow used real, not fictitious, taxpayers' information that evening. The agency investigation accordingly faulted Purslow for carrying and storing what was revealed to be real taxpayers' information in his automobile, in addition to the laptop. In any event, it is not disputed that the taxpayer information on the laptop was not needed for the testing Purslow performed that night.

Early the next morning Purslow called his wife and learned the laptop was not at his house. At that time Purslow was driving his vehicle and observed that certain other items were also missing from the vehicle. Purslow realized that a theft had occurred. When Purslow returned to the hotel later that morning he notified the front desk and reported the theft to the local police department.

That same morning Purslow took part in the conference call with several other DRS employees about the TSC. During the conference call, Purslow remembers some idle chatter during which he was asked something to the effect, "How was he doing?" At that point, Purslow recalled that he said something to the effect, "his laptop had been stolen, but he was still able to get the testing done." Purslow did not remember anyone raising concerns about the loss of DRS property or potential loss of taxpayer information on the laptop.

Witness testimony and evidence examined indicate that Purslow first discovered the laptop missing during the evening of Friday, August 17, 2007. Early in the morning on Saturday, August 18th, Purslow confirmed with his wife that he had not left the laptop at home. Purslow reported the theft to police in Islandia, NY at approximately 12:00PM Saturday. When he returned to work on Monday, August 20, 2007, Purslow first attended a 7:00 AM meeting. After the meeting, Purslow reported the theft to the DRS Information Services Division (hereinafter "ISD") by email at 10:45AM. ISD in turn notified the DRS Business Office and instructed Purslow to notify the DRS Internal Audit Division (hereinafter "DRS IAD"). Purslow sent an email to James Norton and Cheryl Burdick notifying them of the theft that afternoon. Both Norton and Burdick were out of the office on vacation that week.

In sum, the evidence obtained through this review supports the internal conclusion of DRS that Purslow did not immediately notify law enforcement upon discovering the theft, but did provide timely notification to DRS.

3. DRS failed to respond promptly to the theft of the laptop computer.

- **During a Saturday, August 18, 2007 conference call, Mr. Purslow informed a number of DRS employees, including several senior managers, that his laptop was stolen. Returning to work on Monday, August 20, Purslow formally reported the theft to DRS Business Office, Information Services Division, and Internal Audit Division.**

On Saturday, August 18, 2007, Purslow took part in a conference call with a number of DRS employees and senior managers—including the Chief of Staff, the ISD Director, and Tax Chiefs—after his laptop had been stolen the night before. During the call, Purslow made some statement communicating that his laptop was stolen. However, according to the testimony of the call participants, at the time of the call the circumstances did not lead those participating to conclude that Purslow was referring to a State owned laptop that contained confidential taxpayer information.

In her testimony, Christina Lawson confirmed that she first learned about the laptop theft during the Saturday conference call. The purpose of the call was to discuss testing of the new TSC. Lawson recalled that Purslow had left work early Friday to attend a family event, but had assured her that he would complete the necessary testing. Lawson does not remember exactly what Purslow said during the call, but remembers that this is how she heard of the theft.

Division Chief Gary Dowling and Bureau Chief Edward Mehmel both had different recollections that there was some additional discussion between Dowling, Mehmel and Purslow about the laptop that, in any event, did not cause them to worry that taxpayers' information had been lost when the laptop was stolen.

Although a summary of the conference call discussion relevant to TSC project was prepared, it does not document what was said concerning the laptop. There is no recording or verbatim record of what Purslow and others said during the call and, accordingly, what the conference callers should have understood about the consequences of the laptop theft cannot be determined with certainty.

The Commissioner's Executive Assistant, Donna Pomeroy, testified that she took part in the conference call and subsequently notified Commissioner Law of the positive results of testing and decision to activate the TSC. Pomeroy also recalled telling the Commissioner that Purslow's laptop was stolen, essentially as a piece of incidental news Pomeroy heard during the call. Pomeroy did not believe she had any discussion with the Commissioner about the laptop being State property or that taxpayer information was stored on the laptop because that was not her understanding of the situation or a concern she had at the time she called the Commissioner.

Commissioner Law confirmed that she first learned of the laptop theft when Donna Pomeroy called Law at home on Sunday to report on the testing of the TSC. During the call Pomeroy mentioned the laptop theft. At the time of the call Commissioner Law did not know that Purslow had a DRS laptop or, for that matter, which employees at DRS possessed laptops. Law thought that because Purslow had left work early on Friday he would not be using a DRS laptop to perform his testing.

- **Between August 18 and August 23, no steps were taken to determine whether confidential taxpayer information was stored on the stolen laptop. While the theft of a DRS laptop should have raised alarms that confidential taxpayer information was at risk, DRS personnel aware of the theft assumed that the laptop was Purslow's personal property or assumed that it had no taxpayer information.**

Cheryl Burdick, Director of Internal Audit, first learned about the loss of Purslow's laptop when she returned from vacation on Wednesday, August 22, 2007 and received the email from Purslow notifying her of the theft. At that time, Burdick did not believe that she had a responsibility to act upon notice of theft. Burdick did not know whether or why the DRS ISD told Purslow to notify her of the theft. After receiving the email, Burdick saw Gary Dowling, Purslow's supervisor and a DRS Tax Division Chief, in the hallway and asked what was on the laptop. Dowling responded that he did not think anything was on the laptop. Burdick decided to wait for James Norton to return from vacation because at the time it appeared there was nothing on the laptop and she had never previously received this type of notification about the loss of DRS property. Accordingly, Burdick scheduled a meeting with Purslow to occur after Norton returned from his vacation. Burdick took no other action before Norton returned to work because she knew Purslow had notified others within the agency on Monday prior to her return, Gary Dowling told her there was nothing on the laptop, and Burdick did not see any urgency to act. Burdick also pointed out that an email she received from Purslow forwarded an email to her from DRS ISD that suggested ISD was investigating a possible security breach and, therefore, Burdick did not believe that she needed to take immediate action.

Burdick decided to wait for James Norton's return to meet with Purslow because she knew Norton would want to speak with Purslow. Also, Burdick stated that Norton always thought of questions that did not occur to Burdick. Burdick had not previously dealt with this type of incident and decided that Norton, due to his expertise and experience as well as his position as her mentor and supervisor, should attend the meeting.

At the time of the conference call, Chief of Staff Christina Lawson did not know whether Purslow was referring to a DRS laptop. As far as Lawson recalled, none of the conference call participants raised concerns about return information on the laptop during the call. Upon learning of the laptop theft, Lawson did not worry that return information was jeopardized because she believed no return information was needed for the testing that weekend and, therefore, Purslow would not have any return information on the laptop, if it indeed was a DRS laptop.

Commissioner Pamela Law remembers that James Norton was the first to bring concerns to her about taxpayer information on the laptop on Thursday, August 23, 2007, following the laptop theft. Law called a meeting to discuss the responsibilities of the agency. Law testified that she heard nothing and nothing was brought to her attention about the laptop theft before Thursday when Norton spoke to her, other than her conversation on Sunday with Donna Pomeroy. At the time of the call Commissioner Law did not know that Purslow had a DRS laptop or, for that matter, which employees at DRS possessed laptops. Law thought that because Purslow had left work early on Friday he would not be using a DRS laptop to perform his testing.

Deputy Commissioner Richard Nicholson also testified that he first learned of the laptop theft on Thursday, August 23, 2007, when he was pulled into a meeting with Commissioner Law and James Norton. Nicholson said that James Norton was the first person to raise the concern about taxpayers' information being lost with the laptop.

During the course of those interviews, most conference call participants recalled Purslow giving some indication that his laptop had been stolen although they could not recall the exact words he used. Some employees testified that at the time they believed Purslow was referring to a laptop that was his personal property and, therefore, they did not develop a concern that confidential taxpayer information could have been lost when the laptop was taken. Other employees testified that at the time they believed Purslow was referring to his State owned laptop, but their understanding of the type of testing Purslow did that Friday—that is, testing using fictitious taxpayer information—led them to believe no confidential taxpayer information would be jeopardized by the theft.

As the evidence described indicates, the delay in inquiring into the content of the laptop was also the result of many at DRS summarily concluding that the laptop theft should not prompt a concern about potential information loss. Although the primary purpose of a computer is the storage and retrieval of information, several witnesses interviewed for this investigation concluded that the laptop did not contain taxpayer information without actually investigating its content. The loss or theft of a computer should always and immediately trigger a concern and query about what information the computer contained. If a file cabinet or file folder was stolen or missing, no doubt one of the first questions would be "What was in it?" followed by an effort to determine its contents. The same question should be asked whenever a computer is lost, stolen or otherwise compromised.

- **DRS at that time had no established procedures to address information breaches or losses. There was no clear understanding among the various divisions within DRS as to which one should take action when such breaches or losses occurred.**

DRS did not begin to investigate whether taxpayer information was jeopardized by the laptop theft until several days after being notified of the theft. It is clear from our interviews of various DRS personnel that prior to the theft of the laptop DRS had no set procedure in place to address instances of information breaches or information loss. In fact, DRS personnel at various levels had different understandings as to what should have taken place. The delayed response can be attributed in part to this lack of procedure and consensus.

According to James Norton, Chief of the DRS Internal Audit, Planning and Development Division (hereinafter "DRS IAPD"), in the event that a DRS laptop is lost or stolen the employee responsible for the laptop should notify his manager, the Information Services Division, and the Internal Audit group.

In August 2007 Cheryl Burdick, Director of Internal Audit, however, believed the Business Office and Information Services Division were responsible for responding to the theft of a laptop. Burdick testified that there was no process in place in August 2007 for identifying whether taxpayer information was on laptops in the event the laptops were stolen.

Commissioner Law testified that Chief Enforcement Agent Calvin Mellor and his Special Investigations Section would be responsible for responding to the theft of DRS property in addition to ISD and Internal Audit. Law stated that Internal Audit would be responsible for determining whether taxpayer information was lost.

Chief of Staff Christina Lawson testified that the Business Office, Information Services Division, and Internal Audit should be notified of the theft of DRS computer property in order to take appropriate steps in response. Lawson understood that the Business Office would address the loss of any item of DRS property, while Information Services Division and Internal Audit would be responsible for assessing whether taxpayer information was lost.

- **When James Norton, Chief of the Internal Audit, Planning and Development Division returned from vacation on August 23, he immediately questioned Purslow about the theft of the laptop and quickly determined from a review of Purslow's desktop computer that the stolen laptop contained taxpayer information. Norton informed Commissioner Law and others of his findings that day. After further investigation, Norton informed Commissioner Law on Sunday evening that the laptop contained the tax return information of 106,000 taxpayers. More than a week had passed since the theft.**

On Thursday, August 23, 2007, Norton returned from vacation one day early and received word that Jason Purslow's laptop had been stolen. Norton determined that no one from the Internal Audit Division had interviewed Purslow and so Norton scheduled a meeting with Purslow and Burdick for 11:00AM that same day.

During that meeting Purslow initially stated that his laptop contained no taxpayer information. Through further questioning of Purslow and queries to DRS ISD, however, Norton and Burdick learned that several months prior every file on Purslow's desktop computer was copied onto his laptop and, therefore, the laptop might have contained taxpayer information at the time it was stolen.

Norton undertook a quick review of the contents of Purslow's desktop, which revealed files containing taxpayer information. By approximately 1:30PM, Norton notified Commissioner Law that taxpayer information had been stolen along with the laptop.

Later that day at Norton's request DRS ISD created a copy of the content of Purslow's desktop C: drive that Norton and Burdick used to perform a more thorough search in order to produce a database identifying each taxpayer whose return information was on the stolen laptop. Burdick assisted Norton with the creation of a check list that allowed them to proceed to further review the contents of Purslow's desktop so as to determine what the stolen laptop held. From Friday through Sunday, Burdick and Norton worked on this search of Purslow's C: drive. By Sunday evening Norton advised Commissioner Law that the laptop contained the confidential information of over 106,000 taxpayers.

DRS's Chief Enforcement Agent, Calvin Mellor, first learned of the laptop theft from James Norton, who asked Mellor to work with law enforcement to attempt to recover the laptop. As an Enforcement Agent, Mellor investigates criminal violations of State tax laws. Mellor stated that he was not involved in the internal investigation because he needed to focus on efforts to recover the laptop. Mellor worked with law enforcement, including the Suffolk County Police Department, the Connecticut State Police and the Treasury Inspector General for Tax

Administration ("TIGTA"), to assist with recovery efforts. In furtherance of that effort, Mellor conducted an interview with Jason Purslow.

Mellor saw no reason to doubt Purslow's account of the theft and no one disputed his account to Mellor. Mellor had no concern about Purslow being truthful and took no additional steps to determine whether Purslow gave him a true account. Mellor testified that he had known Purslow for many years, had a good professional working relationship with him, and Purslow seemed truthful when speaking with Mellor. Nothing suggested to Mellor that Purslow should be considered a suspect. From Mellor's point of view, Purslow stood to lose so much by taking part in this theft it was inconceivable that Purslow would be involved. Put another way, Mellor did not believe that Purslow would jeopardize his career prospects at DRS by risking arrest for the theft of the laptop or the information it held. However, Mellor testified that he had not determined the value of the information the laptop contained and was not aware of any valuation of the information. Mellor did research whether Purslow's admitted conduct—taking the laptop and leaving it in his vehicle—constituted a crime. Mellor concluded that the known facts did not establish that Purslow committed a crime. There was no indication that other prosecutorial or law enforcement agencies reviewed Mellor's conclusion.

However, the local Suffolk County Police Department in Islandia, NY, the Connecticut State Police, and TIGTA also investigated the laptop theft and surrounding circumstances. Purslow was interviewed during each of their investigations. The conclusion of this report includes the recommendation that in the event DRS learns of unauthorized access or disclosure of taxpayers' information, DRS should notify outside law enforcement authorities and allow those outside authorities to determine whether the conduct is a criminal offense or otherwise warrants further action.

On Monday, August 27, 2007, meetings were held within DRS to address the situation. James Norton was tasked with completing the process of identifying all affected taxpayers, notifying DRS affiliates such as the Internal Revenue Service of the theft, and investigating how DRS might provide identity theft protection to affected taxpayers. Having worked over the weekend to identify the taxpayer information lost with the laptop, Burdick now began assisting with an effort to create an Internet database to allow taxpayers to check whether their information was on the laptop.

- **By August 31, DRS had notified all 106,000 taxpayers that their confidential information may have been compromised and offered them identity theft protection.**

Having been apprised Monday that 106,000 taxpayers' confidential information was taken and possibly jeopardized by the theft, Commissioner Law directed that the Internal Audit Division make identification of affected individuals a priority. The agency also prepared to notify the public and provide identity theft protection to affected taxpayers. The theft of the laptop was disclosed to the public the next day, Tuesday August 28th, and by Friday August 31st affected taxpayers were notified and offered identity theft protection by press release, Internet, and regular mail.

The evidence, including witness testimony and documentary records, supports the conclusion that DRS management and employees did not begin a timely inquiry to determine whether the content of the laptop included taxpayer's confidential information when notified of the theft between Saturday, August 18th and Wednesday, August 22nd. Based upon the testimony and evidence, however, the managers and employees with knowledge of the theft did not believe at that time that the theft would put taxpayer information in jeopardy. The evidence also supports the conclusion that once employees and managers were told that the laptop theft had resulted in the loss and possible compromise of taxpayers' confidential information, the agency responded in a timely and appropriate manner by identifying and notifying affected taxpayers and offering them identity theft protection.

- **No instances of identity theft have been identified as related to the stolen laptop. The significant delay notifying taxpayers caused by DRS's five day lapse in detecting the data loss increased the time period during which taxpayers had no knowledge of the loss of their confidential information and, therefore, no opportunity to respond to or address potential misappropriation or misuse of their information by identity thieves.**

Calvin Mellor testified that on behalf of DRS he received identity theft complaints from approximately 60 taxpayers' whose return information was on the stolen laptop. So far none of the complaints can be connected to the laptop theft. Mellor determined that in some cases no identity theft occurred, but something, such as a suspicious email, caused the taxpayer to believe identity theft occurred. In other cases some type of identity theft occurred, but Mellor was able to determine the theft occurred before the laptop theft or was attributable to an unrelated data breach somewhere outside DRS.

- **On October 9, 2007 DRS completed an internal disciplinary investigation of the theft and suspended Purslow for 30 days without pay.**

In addition to identifying the affected taxpayers and taking steps to provide them with notice and identity theft protection, DRS proceeded with an internal investigation of the laptop theft to determine the facts and circumstances of the theft and whether agency policies had been violated.

Cheryl Burdick, the DRS Internal Auditor, completed the internal agency investigation, which is reviewed in more detail in Part III, *infra*, on October 9, 2007. The report of the investigation concluded that Purslow used poor judgment and disregarded agency policy and guidelines. Burdick concluded that Purslow had authorization to *access* the taxpayer information on his laptop, but he did not receive approval to retain the information on his laptop hard-drive. Evidence gathered at DRS and reviewed during this investigation confirms that PC Mover was used to configure Purslow's laptop. As a result, Burdick knew of no reason to doubt that all the taxpayer information on Purslow's desktop computer at the time his laptop was configured remained on his laptop when it was stolen. The DRS ISD employee who prepared Purslow's laptop in April 2007 was emphatic that she explained to Purslow that PC Mover would make a copy of his computer's hard-drive, including all data, and place that on his new laptop computer. As described above, Purslow denied knowing that PC Mover had added taxpayer information to

his laptop. In an effort to determine what Purslow knew or should have known, Burdick interviewed other DRS employees that received new computers configured using PC Mover. The evidence reviewed concerning the extent of knowledge of employees receiving computers prepared with PC Mover did not support a clear conclusion of what Purslow knew or should have known about PC Mover and the content of his laptop. Burdick's report concluded that this conduct did not rise to the level of "willful neglect."

Purslow testified that although he never performed a reconciliation of the data on his laptop he had no reason to disagree with or doubt the conclusion that more than 106,000 taxpayers' information was on the laptop. Purslow explained that he used the taxpayers' information on his desktop for testing, but never used the information copied onto his laptop for any purpose. Purslow acknowledged that he essentially was storing the return information on his desktop, but explained that this enabled him to perform his work more efficiently.

Purslow disagreed with the claim that he knew taxpayer information was on the laptop at the time of the theft. Purslow stated that he did not know, need or want the return information on the laptop and acknowledged he had no business need to have it on the laptop.

Purslow also disagreed with the assertions that he disregarded agency policy or acted improperly by storing return information on his desktop. Purslow explained his belief that it was appropriate to store on a desktop that was password protected within a secure building. Purslow said the only advice he received against storing information on his desktop was stated as a concern about losing information that was not "backed up." Purslow states this advice was never communicated to him as a security concern. Purslow states that, although others may have a different recollection, no one at DRS told him that storing information on a desktop caused a security risk before August 2007.

As a result of the findings of the internal investigation, DRS disciplined Purslow by suspending him for 30 days. Commissioner Law approved the length of the suspension. Law further agreed to allow Purslow to serve his suspension every other week primarily so that Purslow retained insurance benefits, but also because the agency needed him for certain critical work.

Chief of Staff Christina Lawson testified that the outcome of the internal investigation was a 30 day suspension of Purslow. According to Lawson, termination was considered, but ultimately rejected because DRS determined Purslow's conduct did not warrant termination. Moreover, Lawson testified that based upon her experience with State personnel matters, a termination would not have been sustained when Purslow appealed through the grievance process. Lawson also believed that the 30 day suspension sent a significant message throughout DRS that no matter how good an employee's work history, this incident resulted in Purslow losing 6 weeks pay. A 30 day suspension was much longer than other suspensions typically imposed at DRS according to Lawson. Lawson explained that it was her request that Purslow serve the suspension every other week so he could continue work on projects critical to the agency. (Cheryl Burdick provided no input on what discipline Purslow should receive. Burdick normally does not provide input on those decisions at the conclusion of her investigations.)

4. DRS appears to have conducted a proper and timely internal disciplinary investigation of the loss of the laptop computer.

- **DRS tasked Cheryl Burdick, the DRS Internal Auditor, to investigate the loss of the laptop computer. Although James Norton was her supervisor, and previously held the position of Internal Auditor, and knew the most about this type of security breach, he was not asked to lead the investigation. Instead, he was assigned to assist Burdick.**

Commissioner Pamela Law and her senior staff determined that the internal agency investigation should be reassigned from Human Resources to Internal Audit because the matter raised questions about computers and electronic files that called for technical expertise that personnel in Human Resources did not possess. The Commissioner and her Chief of Staff agreed that Cheryl Burdick, as the agency's designated auditor, should lead the investigation. They also agreed that Burdick's supervisor, James Norton, should assist with, but not lead, the investigation because he was no longer the agency's internal auditor. Also, due to the perception that Norton had already concluded that Purslow committed misconduct prior to the conclusion of the investigation, the Commissioner and her Chief of Staff decided that Norton should not be leading the investigation.

As described above, after James Norton learned of the laptop theft upon returning from vacation on August 23, 2007, he and Cheryl Burdick began an initial *ad hoc* investigation to determine whether taxpayer information had been compromised. After their first meeting with Purslow, Norton was instructed to not question Purslow again because the laptop loss might become a personnel matter and, accordingly, Norton focused on different facets of the agency response to the theft. Norton's understanding was that the DRS Human Resources Office was conducting an internal investigation of the laptop loss to determine what if any personnel action DRS should take.

On or about August 27, 2007, the DRS Human Resources Office was tasked with completing an administrative investigation of the laptop theft. Subsequently, it was determined that Internal Audit should assume responsibility for the investigation because they possessed the expertise to investigate this matter that involved computers and other technical issues.

On or about September 12, 2007, however, Norton learned from an email that Burdick, the agency's Director of Internal Audit and Norton's subordinate, had been tasked with leading the internal investigation.

- **It was alleged that James Norton was removed from the internal DRS investigation because he raised concerns about the investigation and wanted to pursue questions that might subject DRS senior management to criticism. This allegation was not substantiated. According to the testimony from DRS employees presented to this office, Mr. Norton was not assigned to lead the investigation because it was to be a disciplinary investigation and there was concern about the perception that he had already formed opinions as to culpability. Ms. Burdick was therefore directed to lead the investigation with Mr. Norton and others assisting.**

After this investigation by the Auditors of Public Accounts and Attorney General began, additional complaints concerning DRS's internal investigation were received alleging that DRS senior management may have removed James Norton, Chief of DRS IAPD, from the agency's internal investigation because he raised concerns about the handling of the investigation and wanted to pursue questions that might subject DRS senior management to criticism. These allegations were carefully reviewed during the course of the investigation.

In order to understand the organization of the internal agency investigation and reasoning behind certain employees being tasked with the review, this investigation interviewed the senior managers who conceived of, organized and initiated the internal investigation as well as the employees that carried out the agency investigation, including the executive staff of the agency.

Commissioner Law testified that she personally decided, after speaking with her Chief of Staff Christina Lawson, that there should be an internal investigation to put the facts on paper about the laptop theft. Commissioner Law remembered discussing the assignment of the internal investigation with Christina Lawson. The substance of their discussion was that Cheryl Burdick was the Director of Internal Audit and, therefore, she should conduct the investigation. Commissioner Law testified the assignment was her decision, but Lawson may have delivered the news to others in the agency.

Commissioner Law explained that although James Norton was Burdick's supervisor and had served as the agency's internal auditor before Burdick, it was no longer Norton's assignment to conduct internal audit investigations as he was responsible for managing several other important DRS functions. Moreover, Commissioner Law had a reservation about Norton leading the investigation. Based upon a conversation with Norton in the days shortly after the laptop theft, Commissioner Law had a concern that Norton had already reached the conclusion that Purslow was guilty of some misconduct. Norton had suggested to her that Purslow might somehow be involved in the theft of the laptop.

Commissioner Law made clear during her testimony that Norton is a very bright, experienced and valuable manager, but that in this instance she did not want him leading the investigation because he seemed to have prematurely jumped to a conclusion about what Purslow did. Commissioner Law wanted the investigation to gather all the facts unconstrained by any preconceived opinions or conclusions.

Deputy Commissioner Richard Nicholson remembered speaking with Commissioner Law about the investigation to raise the question of whether Human Resources personnel may not have the resources and background to conduct the investigation. Nicholson made contact with Linda Yelmini, Director of the Office of Labor Relations, to obtain her advice on how best to proceed with an investigation of the laptop theft. Yelmini recommended that DRS conduct an internal investigation of the theft and use that investigation for any disciplinary proceeding against Purslow. According to Nicholson, Yelmini had no role in assigning the investigation to particular employees within DRS.

Deputy Commissioner Nicholson recalled that Commissioner Law wanted Burdick to lead the internal investigation because she was the Director of Internal Auditor and seen as a more focused and structured interrogator than Norton. Nicholson did not take part in deciding whether Norton or Burdick would lead the internal investigation and did not have an opinion about who should lead the investigation.

Chief of Staff Christina Lawson recalled a meeting at which it was decided that Internal Audit, not Human Resources, would investigate and provide a report of the facts to Human Resources for disposition. According to Lawson, Linda Yelmini recommended assigning the investigation to Internal Audit instead of Human Resources, but did not have input as to which personnel within Internal Audit should handle the investigation. The reason behind assigning the investigation to Internal Audit was that they possessed the technical expertise to investigate this matter involving computers.

Lawson explained that Burdick was assigned to conduct the internal investigation because she was the Director of Internal Audit at that time. Lawson acknowledged that Norton had more experience than Burdick because he preceded her in that position and that Norton had continued to work on internal audit projects after Burdick's arrival. Burdick had been the Director of Internal Audit for a number of years and, moreover, as the Chief of IAPD Norton had a number of other responsibilities beyond Internal Audit. Lawson recalled further discussions between herself, Commissioner Law, and Deputy Commissioner Richard Nicholson to the effect that Burdick did good work and the investigation should be assigned to her as Director of Internal Audit. Lawson also agreed with Commissioner Law's concern that Norton may have "jumped the gun" by reaching conclusions before the investigation was complete.

Lawson went on to explain that she contributed to the internal investigation by deciding how to organize the report and by providing Burdick with information on due process and guidance on misconduct by State employees.

Lawson later provided information on State regulations and the definition of "willful neglect" as part of the process of reviewing and editing the draft report with Burdick. Lawson took part in discussions about whether the facts Burdick found supported the conclusion that Purslow committed "willful neglect" or violations of agency policy. Lawson believed that there must have been some debate about whether or not the facts proved willful neglect and Lawson provided the regulatory citations to Burdick to assist in resolving that question. (Cheryl Burdick recalled that Law provided her with the regulations after Burdick requested information on policies that might be implicated by the loss of State property.)

Cheryl Burdick testified that she reports to and receives direction from James Norton, who as her supervisor sets priorities for the Internal Audit unit within DRS. After initially helping to identify and notify affected taxpayers, Burdick provided some assistance to the Human Resources Office with the internal administrative investigation. Burdick first learned that she would be tasked with leading the internal investigation upon receiving an email from Christina Lawson that outlined a proposed approach to the internal investigation. Burdick initially believed that her assignment to lead the investigation was a typo in the outline Lawson sent because, Burdick assumed, Norton would lead the investigation. In a conversation with

Christina Lawson, Burdick received clarification that Norton would assist her, but as Director of Internal Audit she should lead the investigation.

Burdick testified that she proceeded to lead the internal investigation, but Norton provided her constant guidance, mentoring, and technical expertise. Burdick explained that in the ordinary course of business on other internal audit projects Norton would fill the same role by providing guidance, suggestions and supervision to Burdick. As her work on the internal investigation progressed, Norton continued to provide guidance, technical assistance and edits to drafts of the report.

- **James Norton directly raised a concern with senior managers, including the Commissioner, Deputy Commissioner, and Chief of Staff about whether Burdick should be leading the internal agency investigation instead of Norton.**

Norton testified that he disagreed with the decision to assign Burdick to lead the internal investigation. Norton did not believe Burdick had the experience with computers or witness interviews to take on this type of investigation. Norton stated that he had more experience than Burdick with internal audit and internal investigation assignments. Norton had conducted internal audits of the agency for over a decade at the time of the laptop theft. Norton was involved in Burdick's prior investigation work and observed that it took Burdick longer than necessary to conclude investigations. According to Norton, Burdick agreed that she was not ready to lead this type of investigation. Norton testified that he did not know why Burdick was made the leader of the internal investigation, but during his testimony he explained he believed that there was some concern that he would pressure witnesses too much during interviews or not work well with the Office of Labor Relations.

Cheryl Burdick also recalled a conversation with Norton about who should lead the internal investigation. Burdick sensed that Norton felt his role in the investigation had been diminished. Burdick testified that at the time she agreed with Norton when he said that he should lead the internal investigation because he had more expertise and experience. That being said, Burdick testified to her belief that the end result of the investigation she led was comparable to what an investigation led by Norton would have produced -- in large part because Norton was assisting and guiding her work on the project. Burdick spoke with Commissioner Law and Christina Lawson, both of whom told her that as Director of Internal Audit the investigation was her task and Norton was there to support her.

Norton testified that he also discussed his concern about Burdick leading the investigation as well as his concern about conference call participants taking part in the internal investigation with Deputy Commissioner Richard Nicholson. According to Norton, Nicholson shared Norton's concerns about the handling of the investigation and agreed that Norton should be leading the work.

Nicholson stated that he was aware of Norton's concerns about the conduct of the internal investigation and spoke with Norton about Commissioner Law's decision that Burdick would lead the internal investigation. Nicholson denied telling Norton that it should be Norton leading the investigation. Rather, Nicholson believed that he shared the reasoning of the Commissioner

with Norton, but also encouraged Norton to speak directly with Commissioner Law about the situation.

According to Norton, he asked to meet with Commissioner Law and told her that Burdick was not ready to run the investigation. Norton recalls that Commissioner Law indicated she did not want him leading the investigation because he "knew too much" about what DRS had and had not done in response to the laptop theft.

Commissioner Law testified that she told Norton that Burdick would lead the investigation because Law thought he had already reached a conclusion on the matter. Law stated that Norton did not say much in response to that explanation. Law also emphasized to Norton that as Burdick's supervisor it was his job to support Burdick and help her succeed with the project. Law did not recall telling Norton he "knows too much" or having a concern about Norton interacting with the Office of Labor Relations. Law knew that Linda Yelmini, Director of the Office of Labor Relations, had spoken with others at DRS about the internal investigation, but Law did not know what input Yelmini provided and indicated that whatever input Yelmini offered did not play a role in Law's decision that Burdick should lead the internal investigation.

- **Norton also directly raised his concern that members of senior management, such as Chief of Staff Christina Lawson and Executive Assistant Donna Pomeroy, who heard about the laptop theft during the Saturday conference call, but failed to act, should not have control over the internal investigation because the potential for perceived culpability might affect the investigation.**

During their conversation about whether Burdick should lead the investigation, Norton recalls that he also advised Commissioner Law that it was his opinion that any employee that took part in the Saturday conference call with Purslow should not be involved in the internal investigation. This included Chief of Staff Christina Lawson as well as the Commissioner's Executive Assistant Donna Pomeroy. Norton feared that the involvement of the conference call participants could taint the internal investigation. As he explained during his testimony, by "taint" Norton meant that because the conference call participants took no action when Purslow told them the laptop had been stolen they might have some culpability for the loss and, therefore, could not be independent when working on the investigation. Norton believed that the conference call participants' fear—founded or unfounded—of criticism or even some culpability for the loss of taxpayer information could compromise their work on the internal investigation. Norton was also concerned that should questions be asked about DRS's inaction after the conference call, the fact that conference call participants took part in the planning, organization and conduct of the internal investigation would make DRS vulnerable to criticism. Norton does not remember Commissioner Law giving him a response to this concern. Norton believed that Law took the matter under advisement.

Commissioner Law does not remember Norton or anyone else suggesting that the conference call participants, including Lawson and Pomeroy, should not be involved in the investigation because of a risk of tainting the investigation.

Deputy Commissioner Richard Nicholson recalled that on or about September 14, 2007 James Norton approached him with concerns that all relevant information would not be revealed by the internal investigation. According to Nicholson, Norton was concerned that Purslow had stated his laptop was stolen during the Saturday conference call, but apparently none of the senior staff and managers taking part in the call acted to address the possible loss of taxpayer information at that time. Norton suggested that conference call participants bore some responsibility for the consequences of the theft as a result. Norton also expressed to Nicholson the concern that Chief of Staff Christina Lawson should not be involved in the internal investigation because she had taken part in the conference call and worked with Jason Purslow on projects.

The fact that Norton had such concerns caused Nicholson concern. Nicholson testified that although he did not share Norton's view that all the relevant facts would not be revealed, he wanted to make sure he understood the reasons for Norton's concern. As a result, Nicholson counseled Norton to prepare detailed notes of Norton's recent conversations related to his concerns with Commissioner Law, Nicholson, Chief of Staff Lawson, and Cheryl Burdick. Nicholson also asked Norton to answer a series of questions that Nicholson sent him via their personal email accounts on Saturday, September 15, 2007. By questioning Norton, Nicholson attempted to obtain a better understanding of the source of Norton's concerns.

Nicholson did not subsequently develop the concern that all the relevant facts would not be revealed by the internal investigation and does not believe that the investigation was tainted or compromised. Nicholson explained that he questioned Norton about his views because Nicholson wanted to understand Norton's concern and be assured that all the relevant facts were obtained through the internal investigation.

The only reference to a possible taint of the investigation Chief of Staff Christina Lawson remembered was during a discussion with Commissioner Law, in which Law indicated her concern that Norton would jump the gun by reaching conclusions before completing an investigation of the facts.

Deputy Commissioner Richard Nicholson does not recall discussing with anyone the concern Norton characterized as a risk the investigation might be tainted. Nicholson believed he told Commissioner Law that Norton was concerned that conference call participants had not been more proactive when hearing that Purslow's laptop was stolen. According to Nicholson, Commissioner Law expressed disagreement with Norton's view based upon her understanding that Purslow gave no indication during the call that it was a DRS laptop. Nicholson recalled some discussion between senior staff—perhaps just Nicholson and Commissioner Law—expressing disagreement with the idea that the investigation might become tainted.

- **Chief of Staff Christina Lawson directed that Norton not attend an investigative interview of Jason Purslow; however, the evidence obtained does not substantiate that Lawson gave this directive to exert improper influence over the investigation.**

Although Burdick had been tasked with leading the internal investigation, Norton believed that he and Burdick would conduct an interview of Jason Purslow on September 19,

2007. Approximately fifteen minutes before the interview was scheduled to begin, Norton received an email from Christina Lawson directing that Mary Kate Speer would attend the interview instead of Norton. Norton notified Deputy Commissioner Nicholson of this development, which, at the time, Norton apparently perceived as supporting his concern that the internal investigation could be compromised.

Cheryl Burdick explained what led to Lawson giving the direction that Norton should not attend the investigative interview of Jason Purslow. Burdick remembers feeling conflicted about the issue. Burdick described Norton as an aggressive interviewer who got answers quickly, but sometimes made people feel "attacked." Burdick indicated her preference for a less aggressive approach to interviews. When preparing for the Purslow interview Burdick realized that she did not want Purslow to feel threatened and stop answering her because that would hinder the investigation she was leading.

Contributing to this was Burdick's perception that there was an adversarial relationship and tension between Norton and Purslow. From the point of view of Burdick, Norton thought that Purslow did not respect security. Burdick recalled Norton saying something to the effect, "this is what happens when you think of security afterwards," in reference to Purslow and the theft of his laptop. As the time of the Purslow interview approached, Burdick recognized that there was a presumption that Norton would attend the interview and that brought her concern about Norton and Purslow to the forefront.

Burdick went on to explain that this was a very difficult time to work with Norton because he felt very slighted when Burdick was tasked with leading the internal investigation instead of him. Burdick said she was also under significant stress having recently been assigned the investigation and felt she did not have the courage or time to tell Norton he should not attend the Purslow interview. Burdick approached Christina Lawson and discussed the "pros and cons" of Norton taking part in the interview. Following that discussion, Lawson communicated to Norton that Mary Kate Speer would be attending the Purslow interview. Burdick felt she needed someone above her to essentially back her up and tell Norton that he would not attend the interview. Burdick did not consider Norton's absence unusual because Norton would often provide guidance but not attend her investigative interviews. Moreover, Burdick recalled that there was a subsequent interview, at which time Norton attended and had the opportunity to question Purslow. Norton confirmed that he and Burdick conducted another investigative interview of Purslow subsequent to the September 19th interview.

Chief of Staff Christina Lawson recalled questions about whether Norton should attend an interview of Purslow as part of the internal investigation. Lawson recalled a high stress level within the agency at the time and that Cheryl Burdick had called her to indicate that Burdick did not want Norton attending the interview. As a result, Lawson directed that Mary-Kate Speer attend the interview with Burdick instead of Norton. Lawson believes Burdick sought her assistance because it was Norton's nature to take charge and lead, but at this time Burdick was supposed to lead this investigation and, therefore, she wanted to be able to lead Purslow's interview. If Norton were present, it would have been hard for Burdick to lead the interview. Lawson did not know whether Burdick addressed this issue with Norton, but remembered that Norton wanted to attend. Lawson did not remember giving any prior indication that Norton

should attend the interview and understood that in the ordinary course of business Norton did not attend this sort of interview, but rather left them for Burdick to handle. Lawson testified that she did not direct the internal investigation, but took this action to assist Burdick. Although Norton was and is Burdick's direct superior, Lawson explained that DRS employees can contact senior staff for resolution of issues when the employee believes they cannot resolve it through their normal chain of command.

Commissioner Pamela Law recalled discussing and agreeing with Christina Lawson that Cheryl Burdick and Mary-Kate Speer should conduct the investigative interview of Jason Purslow. Law did not want Norton taking part because his personality was such that if he attended the interview he would take charge and Law wanted Burdick to lead this interview and investigation. Also, Law was concerned that Norton's opinions might affect the fact-gathering process during the interview.

Deputy Commissioner Richard Nicholson first learned that Speer would attend the interview of Purslow instead of Norton upon receiving an email from Norton to that effect. Nicholson had no part in deciding who should attend the interview, but recalled hearing about Burdick having some discomfort or disagreement with Norton's anticipated approach to the interview and that being what led Lawson to send Speer instead of Norton.

- **The evidence obtained supports the conclusion that while DRS senior management deliberately limited the role of Norton they had justifiable managerial reasons for doing so. Further, they allowed Norton to provide input and advice on the investigation.**

Norton testified that he was effectively removed from the internal investigation insofar as Chief of Staff Christina Lawson indicated that his role in the internal investigation should be limited to providing input and assistance only when Burdick sought his help.

Commissioner Pamela Law testified, however, that Norton was not removed from the internal investigation because it was never assigned to him. Moreover, Law testified that she explained that Norton was told to contribute to the internal investigation by helping Burdick with the investigation itself as well as the drafting of the report.

Deputy Commissioner Richard Nicholson did not remember any discussion about removing James Norton from the chain of command concerning the internal investigation. Nicholson was aware that Commissioner Law took the position that it was most appropriate for Cheryl Burdick as internal auditor to conduct the internal investigation. However, Nicholson believed that Commissioner Law wanted Norton to supervise Burdick's work. Nicholson believed that Norton continued to provide input and advice on the investigation and subsequently helped edit the report. Nicholson was not aware of restrictions being placed on Norton's participation in the internal investigation.

Christina Lawson also testified that Norton was not removed from the internal investigation. Lawson recalled telling Norton it was his job to support his subordinates and help

them succeed. Lawson stated that Norton provided this support and guidance to Burdick during the investigation.

Finally, Cheryl Burdick did not believe that James Norton was removed from the investigation. Burdick described how she was in constant communication with Norton and constantly asking him questions as she worked on the internal investigation. Burdick recalled that Norton reviewed everything she did during the investigation.

In conclusion, based upon the evidence obtained, the concern that James Norton had prematurely reached a conclusion about Purslow's conduct, as well as the fact that Cheryl Burdick had been hired to serve as the agency's Director of Internal Audit when Norton was promoted out of that position, justified the decisions Commissioner Law made concerning the assignment of the internal investigation and the role of Norton.

- **The DRS internal investigation did not pursue the question of whether DRS management properly handled the theft of the laptop computer. DRS's investigation focused only on the loss of the laptop computer. Subsequent actions of DRS management were not directly relevant to that inquiry. DRS management assumed that the Auditors of Public Accounts and the Office of the Attorney General would investigate those issues**.

Norton testified to his opinion that the response or lack of response by the conference call participants, including several DRS managers, to Purslow stating his laptop was stolen should have been investigated. As part of that inquiry, Norton testified that the internal investigation should have looked into whether, as Gary Cyr claimed, Cyr's phone disconnected from the conference call at the moment Purslow stated his laptop had been stolen. Norton's perspective was that nearly a week passed and nothing was done about the laptop theft. Norton believed that this inaction should have been scrutinized.

Commissioner Law did not remember any proposed objectives of the internal investigation being "vetoed" during these discussions. Since receiving the final report of the internal investigation, nothing has come to the attention of Law that calls into question the findings of the report. Law testified that she did not know of any unanswered questions about the laptop theft. Law did, however, remember that at some point during the investigation Norton proposed that Purslow's 14 year old son should be interviewed. Norton proposed this during a conversation with Law in which he also suggested that Purslow might be involved in the theft of the laptop. Law told Norton and reiterated in her testimony that it would be inappropriate to interview a 14-year-old as part of the agency's internal investigation.

Deputy Commissioner Richard Nicholson testified that he does not know of any unanswered questions concerning the laptop theft or suggestions by others that there are unanswered questions or doubts about the conclusions of the internal investigation. Nicholson recalled a discussion about whether Purslow's son should be interviewed that ended with Commissioner Law indicating that the agency would not pursue the interview. Nicholson also recalled a meeting between Nicholson, Norton, and Calvin Mellor at which doubts were raised about the accuracy of Purslow's account of the theft, but believes these questions were put to rest

before the DRS finalized its report. Other than the disagreement about whether James Norton or Cheryl Burdick should lead the investigation, Nicholson testified that he was not aware of any disagreement over the course of the investigation or areas of proposed inquiry.

From Christina Lawson's perspective, there were no questions left unanswered or avenues of investigation neglected by the conclusion of the internal investigation and no one has suggested to Lawson that such questions remain. Lawson did not take part in any discussions about interviews of Purslow's wife or son.

Lawson strongly felt that DRS should not attempt to answer the question of whether the agency "appropriately responded" to the theft. Lawson thought that other agencies, such as the Auditors of Public Accounts and Attorney General, would likely take on that inquiry. However, she is not aware of anyone at DRS flagging that issue for the Auditors of Public Accounts to review. Instead, the purpose of the internal investigation was to determine the contents of the laptop and whether disciplinary action was warranted. Lawson took part in discussions about the overall objectives for the investigation, but was not involved in deciding how to obtain information.

Cheryl Burdick testified that, to her knowledge, no avenues of investigation were vetoed. No one suggested or directed Burdick to not question a particular witness or examine particular evidence. Burdick did not recall any communication about interviewing Purslow's wife and child. However, she did recall attending a staff meeting to discuss an outline of the objectives of the internal investigation. The staff at the meeting discussed including the question "whether DRS appropriately responded" to the theft in the investigation. According to Burdick, the consensus at that meeting was that although DRS had responded appropriately to the theft, it would not be appropriate for the agency to attempt to investigate that aspect of events and judge its own performance. Furthermore, Burdick noted that because she was closely involved in the initial response to the theft she felt she would not be able to perform an independent investigation of the agency response. Instead, Burdick understood that the investigation should focus on Purslow's loss of the laptop.

Burdick did recall Norton expressing a concern about what he perceived as the inaction of the conference call participants after learning Purslow's laptop was stolen. As a result, Burdick interviewed all the conference call participants as well as Commissioner Law to inquire into what if any response followed the news of the laptop theft. (Commissioner Law confirmed that she was also interviewed as part of the internal agency investigation and questioned about the circumstances of her learning of the laptop theft from Donna Pomeroy.) Based upon Burdick's inquiry into the conference call, not all of the conference call participants heard Purslow say his laptop was stolen because not all the callers had joined the call at that time. Most of those that did hear it did not know Purslow was referring to a DRS laptop. Burdick did not include her findings regarding the conference call in her report because it did not fit into the report. According to Burdick, the purpose of the report was to document events to enable the Human Resources Office to complete a disciplinary review of the matter.

Norton also testified that in his opinion some questions remained unanswered at the conclusion of the internal investigation. According to Norton, Purslow's wife, son, and former

wife, who also attended the hockey tournament in Islandia that weekend, should have been interviewed by DRS to find out what they knew about the laptop theft. Norton recalled that Commissioner Law indicated that those interviews would not be pursued.

In conclusion, although Commissioner Law did not approve Norton's recommendation to interview Purslow's family members and DRS itself did not pursue the question of whether its management properly handled the theft of the laptop, the totality of the evidence obtained does not substantiate that DRS's internal investigation was deficient or compromised in a material respect. Rather, the evidence supports the conclusion that DRS deliberately limited the scope of its internal investigation to its stated purpose—ascertaining the facts surrounding the Purslow's loss of the laptop so that management could determine whether discipline of Purslow was warranted.

5. Since the laptop theft, DRS has identified and taken corrective actions to provide greater protection to taxpayers' confidential information.

- **DRS has implemented greater restriction on taxpayer information access and storage.**

Calvin Mellor described the changes to security measures for taxpayer information in electronic form subsequent to the laptop theft. Laptops are now encrypted and physically secured with cable locks. Taxpayer information is tracked when it is moved to and from laptops. DRS policy now requires that return information be stored on the secure network. Now all employees, managers, supervisors, and internal audit personnel are responsible for tracking the movement of taxpayer information within the agency.

Deputy Commissioner Richard Nicholson also testified that DRS has changed how taxpayer information in electronic form is handled within the agency. Taxpayer information is no longer stored on desktops, but is kept on the agency network. Taxpayer information is moved from the network to a laptop only when a business purpose makes the transfer necessary. Furthermore, a log is kept of that movement of information. All laptops are protected by encryption. At the time of his testimony, Nicholson confirmed that DRS was pursuing the acquisition of a data loss prevention system. Subsequently, this investigation determined that DRS has purchased and begun to install the system.

Jason Purslow testified that since the laptop theft significant changes have been made to the handling of taxpayer information in electronic form. No taxpayer information is stored on desktops and employees store only what is necessary in their portion of the network. Laptops are now encrypted. Purslow recalls meetings at which these new procedures were explained.

- **DRS established more comprehensive procedures to protect taxpayer information.**

In addition to the new policies concerning storage and access described above, DRS implemented a process for systemically tracking taxpayer information when it was necessary to transfer the information from the DRS network to mobile electronic storage devices such as laptops. DRS implemented a process that involved a series of affirmative steps by individual

employees handling taxpayer information, the employees' supervisors, and the agency's internal audit staff to systemically track this movement of taxpayer information. This process was used in addition to the logging of access to taxpayer information already used at DRS.

In addition, during this investigation investigators questioned DRS employees about whether a Data Loss Prevention computer program had been considered as a means of tracking and securing taxpayer information. Investigators learned that, subsequent to their questioning, DRS recently acquired a Data Loss Prevention ("DLP") application to protect and track taxpayers' information at the agency.

In early 2009, DRS purchased the DLP application and began the process of integrating the application into agency systems and procedures. The DLP application will prevent any unauthorized movement of taxpayer information in electronic form, limit the amount of taxpayer information that authorized employees can access or move, it will maintain records of what taxpayer information has been accessed or moved by employees and, in the event taxpayer information is lost or breached, this application will enable the agency to recreate the lost information. Once installed, this application will provide these protections to all agency computers including laptops.

- **Laptops and electronic mobile storage devices are now encrypted.**

After the laptop theft in August 2007, all laptops were encrypted at the direction of Governor Rell.

CONCLUSIONS

1. The failure of DRS to implement effective security and tracking measures to protect taxpayer information contributed to the loss of the confidential information of 106,000 taxpayers.

2. The laptop should not have contained the taxpayer information transferred from Purslow's desktop. If there were a legitimate need to store taxpayer information on the laptop, it should have been encrypted.

3. The failure of DRS to immediately investigate whether the laptop contained confidential taxpayer information exposed taxpayers to an additional five days of possible identity theft and financial harm. After that initial failure, DRS management properly and quickly took steps to protect taxpayers whose information was compromised.

4. DRS conducted a proper disciplinary internal review, assigning its personnel in a manner to avoid possible issues in taking future disciplinary action. It was reasonable for DRS to leave the question of management fault for the loss of taxpayer information to an independent review by the Auditors of Public Accounts and the Attorney General.

5. Since the theft of the laptop computer, DRS has taken significant steps to increase the security of taxpayer information, including establishment of greater restrictions on taxpayer information access, storage and protection, as well as encryption of laptops and other mobile electronic devices.

6. DRS should take additional measures to ensure that all of its employees understand the seriousness of data breaches and to further safeguard confidential taxpayer information.

RECOMMENDATIONS

This investigation identified changes necessary to adequately protect taxpayer information in electronic form at DRS:

1. **DRS should train all employees to spot data breaches and teach them what to do if they happen. DRS should hold employees accountable if they fail to follow data breach protocols and procedures.**

Government agencies like DRS that must maintain large computer systems storing sensitive information in order to carry out their essential functions today face numerous threats. From computer viruses to unauthorized employee access, there are many ways in which citizens' personal information could be jeopardized. As with any means of storing valuables, risks of loss or theft can be significantly minimized, but never eliminated altogether.

Therefore, it is recommended that DRS establish and promulgate a clear and concise policy on safeguarding taxpayer information in electronic form that specifically addresses what procedure to follow during incidents of potential information loss, ensure that all employees are advised of the policy, and that employees are held accountable for non-compliance.

2. **DRS should continue ongoing efforts to update its computer networks so that all confidential taxpayer information stored is tracked and secured.**

Before the laptop theft, DRS had established a process of maintaining records of all access to taxpayers' information.

Subsequent to the theft, a process was implemented to track all taxpayer information moving from network storage to temporary laptop storage within the agency. This was a step in the right direction. However, this manual process suffers from the inherent flaw that it is dependent upon the employees taking affirmative steps to record their use of taxpayer information. Should an employee, for whatever reason, neglect to take those steps, the record of their use and movement of taxpayer information may be incomplete.

After investigators questioned Commissioner Law and other senior staff about whether a DLP system could be used at DRS, the agency acquired and began the process of installing a DLP application that will provide substantially greater ability to track and prevent the misuse of taxpayer information at the agency.

Therefore, it is recommended that DRS continue to implement procedures and technical improvements, including the agency wide data loss prevention system, to systemically track the use and movement of all taxpayers' information. This process should periodically review the current state of the art, reflecting technical advancements to ensure that DRS continues to adopt best practices for the foreseeable future.

3. **DRS should study how other states and federal entities such as the Social Security Administration and the Internal Revenue Service test new computer systems, and then reduce as much as possible use of taxpayer "test subjects" in designing and testing new computer systems.**

As described above, the issue of whether real taxpayers' return information should be used to test DRS systems has been the subject of some discussion within DRS. DRS has created fictitious taxpayer information for some testing purposes, but real taxpayers continue to be used as unwitting test subjects for DRS systems.

The evidence obtained during this review indicates that there is no active and organized effort towards decreasing and minimizing the use of real taxpayers' information for test purposes.

It is important to note that it may not be possible or appropriate to completely eliminate this use of taxpayers' information. For example, when an individual taxpayer calls DRS to complain that they were unable to interface with a DRS Internet-based system, the first reasonable step for DRS to take is to run an internal test using that individual's information in order to ascertain the source of the problem. That being said, greater efforts to minimize this use of taxpayers' information are warranted.

Any use, transfer or manipulation of a taxpayer's information increases the risk that the information might be misplaced or misused. Although State law permits DRS to use taxpayers' information for testing purposes, it would be reasonable and prudent for DRS to accelerate its efforts to minimize this practice based upon its evaluation of the practices of other states and federal entities.

Therefore, it is recommended that DRS minimize the use of taxpayers as "test subjects" by accelerating its effort to reduce the use of taxpayers' information for testing purposes based upon its evaluation of the practices of other states and federal entities, such as the Social Security Administration and Internal Revenue Service.

4. **DRS should notify affected taxpayers and law enforcement agencies if a DRS employee improperly accesses taxpayers' information so judgments can be made whether a criminal investigation or other action is warranted.**

As described above, it has been the practice at DRS to treat incidents of employees improperly accessing taxpayers' confidential information, referred to within the agency as

"browsing," exclusively as a personnel matter. DRS does not notify the taxpayers whose information was improperly accessed or alert outside law enforcement agencies to the incident.

State laws concerning DRS's inspection and disclosure of taxpayer information, Conn. Gen. Stat. §§ 12-15(a), 12-15(b), 12-15(b)(12), and 12-15(f), indicate that DRS employees may inspect and disclose taxpayer information only to the extent necessary for the purposes of tax administration or their other official duties. (State law, Conn. Gen. Stat. § 12-15(b)(12), recognizes "testing" and "maintenance" of DRS equipment as part of tax administration.) Put another way, unless a bona fide business purposes requires inspection or disclosure of taxpayer information, State law prohibits DRS employees from accessing the information. Pursuant to Conn. Gen. Stat. § 12-15(g), violation of the State statute controlling inspection and disclosure of taxpayer information can be punished by imprisonment for one year and a one thousand dollar fine.

Unauthorized inspection and disclosure of taxpayer information may violate other State laws such as Conn. Gen. Stat. § 53-451(b), which makes Unauthorized Use of a Computer or Computer Network a criminal offense. Evidence of this conduct could also establish that other crimes, such as Identity Theft contrary to Conn. Gen. Stat. § 53a-129a, were committed based upon the particular circumstances.

Moreover, Federal law, 26 USCS § 7213A, also makes unauthorized inspection of taxpayer information by Federal employees, or State or local employees in receipt of Federal taxpayer information, a criminal offense punishable by imprisonment for one year and a one thousand dollar fine. Furthermore, when an individual is charged with a criminal violation for unauthorized inspection or disclosure of taxpayer information 26 USCS § 7431 requires that the Internal Revenue Service notify the affected taxpayer.

In sum, the practice of treating unauthorized access to taxpayer information as solely a personnel matter for disposition by DRS may not comply with State and Federal law or the intent behind the statutes described above.

Moreover, the current treatment of unauthorized access as an internal agency matter that at worst may result in personnel disciplinary action may contribute to more instances of unauthorized access because employees do not understand the potential consequences of their conduct. The use of the colloquialism "browsing" may also contribute to this perception because it does not adequately convey the impropriety of accessing taxpayers' confidential information without authorization or a legitimate business purpose.

DRS should notify outside law enforcement agencies of any instances of unauthorized inspection, access or disclosure of taxpayer information by the agency's employees. The outside law enforcement agency would determine whether the facts and circumstances warranted further investigation as a possible criminal matter. Also, if as State law apparently indicates, unauthorized access to taxpayer information by a DRS employee is a crime, this conduct could also constitute just cause for dismissal of that employee in that it is commission of a misdemeanor while performing work duties.

DRS should also notify taxpayers when their information has been the subject of unauthorized inspection, access or disclosure. Taxpayers have the most at stake and are in the best position to determine whether instances of unauthorized inspection or disclosure may lead to identity theft or misuse. Although DRS may see unauthorized access to taxpayer information as an agency problem to be dealt with internally, it is possible that it could result in identity theft or other misuse of the taxpayers' confidential information. DRS may not know whether an instance of unauthorized access has resulted in identity theft or other misuse of the information. If the taxpayer is not notified by DRS about the unauthorized access, the taxpayer may know that he or she has been the victim of identity theft, but will have no way of knowing that the source of the identity theft was at DRS and the taxpayer's attempts to rectify the situation and protect themselves will be hampered.

Therefore, it is recommended that when a DRS employee has improperly accessed taxpayers' information the agency should notify the affected taxpayers and allow outside law enforcement agencies to determine whether the employee's misconduct is a criminal offense or otherwise warrants further action.