State of Ohio
Office of the Inspector General
THOMAS P. CHARLES, Inspector General

REPORT OF INVESTIGATION

FILE ID NUMBER:	2007190
AGENCIES:	Ohio Department of Administrative Services, Office of Information Technology, Office of Budget and Management
BASIS FOR INVESTIGATION:	Governor's Office Referral
ALLEGATION:	Mismanagement, Failure to Protect Confidential Information, Failure to Properly Report Loss
INITIATED:	June 15, 2007
DATE OF REPORT:	July 20, 2007

EXECUTIVE SUMMARY

File ID No. 2007190

On June 15, 2007, Governor Ted Strickland announced that a computer backup tape containing Social Security numbers and other confidential data on more than 64,000 state employees had been stolen from the car of an intern assigned to the state's integrated Ohio Administrative Knowledge System ("OAKS") project. The governor asked the Office of the Inspector General ("OIG") to initiate an investigation on the same day.

The theft, which occurred in the Columbus suburb of Hilliard on the evening of June 10, 2007, or early the following morning, exposed a questionable but longstanding practice in which OAKS supervisors, contractors and, eventually, college interns took backup tapes to their homes on a daily basis. The instructions, reduced to policy in an OAKS Business Continuity Plan published April 30, 2002, were to return the tapes on the following workday.

Numerous studies published by Gartner Inc. and other leading authorities on information technology security best practices recommend that administrators of large IT systems encrypt sensitive portable data maintained on backup tapes and laptops. They also advise that backup tapes be treated like cash and either taken off-site via a physically secure method of transportation such as armored car or by secure site-to-site electronic transmission.

Although OAKS is a $158 million IT project and the State of Ohio is a $52 billion business enterprise, OAKS administrators had not encrypted the data on the stolen backup tape and had authorized a succession of interns to take the tapes home for the previous two years with only an admonition to store the tapes in a safe place. For approximately six weeks before the theft, that task had fallen on the OAKS intern with the least seniority – Jared Ilovar, a 22-year-old, $10.50-an-hour employee hired on March

5, 2007. Ilovar received this assignment not from an OAKS supervisor, but from a fellow intern who had that responsibility before him.

This practice violates not only basic tenets of IT security but common sense as well. Nevertheless, we discovered that the same practice was in place at the state Office of Budget and Management ("OBM") – albeit not involving the use of interns as couriers. Until the theft of the OAKS backup tape last month, two OBM network administrators had shared the duty of taking home OBM backup tapes since 1999. They no longer do so.

Our investigation determined that following the theft, OAKS Project Manager David White compounded problems by instructing Ilovar not to inform Hilliard police that the tape contained confidential data after Ilovar discovered on the morning of Monday, June 11, that the tape had been stolen. White disputes this allegation, but both Ilovar and Compuware consultant Avadhut Kulkarni, who were present when White instructed Ilovar to file a police report early Monday afternoon, contradict him.

White also did not report to his superiors that the tape contained sensitive data until 2 p.m. on Tuesday, June 12, 2007, even though Ilovar's fellow intern, Brian Ring, said he and other OAKS personnel had determined that the tape contained state employees' Social Security numbers almost 24 hours earlier. White maintains that he didn't sound the alarm sooner because OAKS employees were still examining another version of the tape, but all of the evidence we reviewed leads us to conclude that it was apparent almost from the outset that the stolen tape contained a large amount of confidential data.

With Hilliard police having been given no reason to consider the theft an urgent matter, administrators at OAKS, OBM and the Office of Information Technology ("OIT") lost another opportunity to possibly recover the tape by failing to notify the State Highway Patrol until 3:30 p.m. on Thursday, June 14. Interviews and records make it clear that the delay occurred because state officials were focused more on determining the volume of sensitive data on the tape than in recovering the device, even though both goals could

have been achieved. In hindsight, administrators we interviewed universally agreed that they should have notified the patrol and other authorities at least 48 hours earlier.

Contributing to this communication and supervision breakdown was a reporting structure at OAKS in which contractors were given supervisory authority over Ilovar and the other OAKS interns. Although a gubernatorial transition report had warned that OIT was over-reliant on contract employees, we found that contractors were so embedded in the culture at OAKS that the OAKS project manager, a state employee, turned to them for advice and guidance following the theft of the data tape.

Finally, we note that the theft would never have compromised the identities of hundreds of thousands of state employees, taxpayers, public assistance recipients and others had OAKS administrators responded appropriately to a call they received from an assistant state auditor in late February 2007. The auditor warned that access to Social Security numbers and other sensitive data was readily available on a shared drive on the OAKS intranet. Four months later, state officials would learn that the stolen backup tape contained a massive quantity of data that had been stored on that drive.

White and other OAKS administrators initially took the auditor's warning seriously, restricting access to the shared folder referred to as the I: drive and ordering that Social Security numbers and other sensitive data be removed and placed in a more secure location on OAKS servers. Those orders, however, were never relayed to the database analysts who were working with the data, and they soon repopulated the I: drive with large files containing Social Security numbers, banking information and other sensitive data. One OAKS analyst admitted to us that she transferred multiple copies of a file containing the names and Social Security numbers of all 64,000 state employees onto the I: drive and had been working on the files on the Friday before the theft.

Given the complexity of the OAKS conversion and the enormous pressure nearly 300 state employees and contractors have been under to meet tight delivery schedules, it is clear that security and confidentiality were secondary concerns at OAKS. Consequently,

we found that all OAKS personnel – from the program manager to the administrative assistants – had unfettered access to reams of sensitive data on the OAKS intranet, whether they had a need for that access or not. We also found system "loopholes" that permitted human resources officials in agencies across the state to access Social Security numbers, banking information and other private information on employees in other state agencies.

Our findings include one instance in which a wrongful act occurred, two instances in which a wrongful act or omission occurred and one instance in which two acts of omission occurred.

This investigation was conducted parallel with a criminal investigation by the State Highway Patrol and the Hilliard Police Department. Although the Highway Patrol has established a tip line and Hilliard police have offered a $500 reward for its recovery, the tape is still missing and the criminal probe remains open.

Based on the results of our investigation, we have made seven recommendations and are asking the appropriate agencies to respond to this office within the next 60 days with a plan outlining how these recommendations will be implemented.

TABLE OF CONTENTS

I. BASIS FOR INVESTIGATION

On June 15, 2007, the Office of the Inspector General ("OIG") opened an investigation at the request of Governor Ted Strickland after the governor revealed at a news conference that a backup data tape containing the Social Security numbers of more than 64,000 State of Ohio employees and other confidential information had been stolen from the car of an Ohio Administrative Knowledge System ("OAKS") intern on the evening of June 10, 2007, or early the following day. In addition to reviewing the work culture, policies and procedures that permitted a 22-year-old part-time employee to take home such a large volume of sensitive information, we also investigated two related allegations and two other data-breach incidents.

II. ACTION TAKEN IN FURTHERANCE OF INVESTIGATION

We reviewed emails and other written correspondence sent by supervisors and employees at OAKS, the Office of Budget and Management ("OBM"), the Department of Administrative Services ("DAS"), the Office of Information Technology ("OIT") and other agencies. We also conducted interviews with the directors of OBM and DAS; the governor's chief of staff and cabinet secretary; the state chief information officer; the state chief privacy officer; the OAKS project manager; and other officials and employees at OBM, DAS and other state agencies. We additionally interviewed the chief executive of Interhack Corporation, the private firm hired to conduct an independent security analysis of OAKS, and reviewed state policies and procedures, reports on other government data thefts, and analyses of best practices published by Gartner Inc. and other leading IT security sources.

III. DISCUSSION

Five years in the making, OAKS is a $158 million Enterprise Resource Planning system that, when fully rolled out in July 2008, will integrate all state agency capital improvements, finance, fixed assets, human resources and procurement functions.

The project is managed jointly by OBM and DAS, which, along with numerous other state agencies, have assigned a total of 119 employees to the project. Another 167 contract workers are detailed to the project, 117 of whom work for Accenture LLP, the company hired in April 2005 to implement the OAKS system integration. Five consultants from Compuware Corporation have been assisting the state in ensuring that Accenture meets its contract specifications.

OAKS utilized a 20-tape backup rotation in the building in which the stolen data was stored. Interhack Corporation, the firm hired by the State of Ohio to perform a security analysis of OAKS and determine what data was on the tape stolen from Ilovar's car, is examining day-before and day-after tapes {Tape 6 and Tape 8} to determine what data was on the stolen device {Tape 7}.

Allegation 1: OAKS administrators failed to protect confidential information by authorizing state employees, including college interns, to take backup tapes containing sensitive data to their homes for overnight storage.

On Monday, June 11, 2007, Jared Ilovar, a college intern assigned to the OAKS project, reported that an unencrypted backup tape he had been assigned to take home for safekeeping over the weekend had been stolen from his car in the Columbus suburb of Hilliard. According to Ilovar, the theft occurred either late Sunday, June 10, or early Monday morning.

Subsequent analysis revealed that the tape included the names, Social Security numbers and check amounts for more than 770,000 Ohio taxpayers with uncashed personal

income tax or school district income tax refund checks; pharmacy benefits information on policy holders and their dependents that is protected from disclosure under the Health Insurance Portability and Accountability Act of 1996; confidential information pertaining to Medicaid providers and Temporary Assistance to Needy Families recipients; and other sensitive data protected under state or federal laws (Exhibit A).

Under questioning, Ilovar acknowledged that this was not the first time he had left the backup tapes in his car, estimating that he remembered to bring them into his apartment approximately 85 percent of the time. On those occasions, he said he placed the tapes on top of his TV so that he would remember to bring them back on the following day.

Hired to help OAKS administrators meet a grueling series of deadlines, Ilovar and his fellow interns also were given other security responsibilities. They included programming key cards for access to OAKS offices and providing new employees with user rights to the OAKS network.

Although OAKS administrators from Project Manager David White on down acknowledged that they were aware that Ilovar and the other interns were taking backup tapes home, the person who assigned Ilovar this task was not White or another OAKS administrator but Brian Ring, a fellow intern. This, however, was not an example of Ring exercising authority that he lacked; it was an example of OAKS interns making management decisions because managers had ceded their authority.

OAKS interns had shared the responsibility of taking backup tapes home for two years prior to the theft – a practice that OAKS intern Aron Rogers referred to as "the passing of the torch." Previously, OAKS supervisors, including both state staff and contractors, had taken the tapes home. OAKS officials even went so far as to memorialize this practice in

a Business Continuity Plan published on April 30, 2002.[1]

Taking home backup tapes is a common practice suitable perhaps for the proprietor of the corner drugstore, but not for major enterprises with large amounts of sensitive data. Where an elevated level of risk exists, Gartner and other experts on IT security best practices recommend that backup tapes be treated like cash – sent off-site for secure storage and encrypted in case of loss or theft.[2] Gartner also claims that IT security-awareness training will result in a 25 percent productivity savings by avoiding security incidents that could have been prevented.

As the state's technology leader, Ohio's chief information officer ("CIO") typically would be the person responsible for responding to a data-security breach such as the one that occurred at OAKS. For several reasons, that did not happen.

Under the previous administration, OAKS operated independently of OIT and OIT lacked statewide enforcement authority of its standards. Consequently, OAKS administrators did not follow the state's IT Security Incident Response policy,[3] which had been adopted on June 14, 2006. Our investigation found that OAKS had no incident response point-of-contact, no incident response team and no incident response plan.

Although he has been Ohio's CIO only since February 12, Steve Edmonson revealed a surprising lack of familiarity with state IT policy. During our interview, he repeatedly insisted, incorrectly, that state IT policy prior to the theft did not call for agencies to

[1]Section 4.3 of the OAKS Business Continuity Plan, "Storage of Back-up Tapes," says, "The previous day's back-up tapes are removed from the PMO {Project Management Office} and taken to the Network Administrator's residence." OAKS administrators claim that Ilovar and the other interns "functionally" served as network administrators.

[2] See the following Gartner publications: "Management Update: Predicts 2006: Storage Technology Evolves Along With Demand," November 30, 2005, ID Number G00136682; "Missing Bank of America Tapes Underscore Encryption Need," March 1, 2005, ID Number G00126581; "Management Update: Best Practices for Secure Data Tapes, 2005," July 27, 2005, ID Number G00130112; and "Management Update: Data Protection Is Less Costly Than Data Breaches," September 28, 2005, ID Number G001131331.

[3] http://www.oit.ohio.gov/IGD/policy/pdfs_policy/ITP-B.7.pdf

establish an incident response point-of-contact. He also claimed – and pledged to provide documentation – that state IT policy prior to the theft forbade employees from taking backup tapes home. Asked three different times over the next four days to provide that documentation, Edmonson finally conceded that he had been wrong.

Related Management Issues

The reporting structure (Exhibit B) under which OAKS interns worked shows that Ilovar and fellow interns Ring, Rogers and Steve Karaffa reported to Compuware consultant Avadhut Kulkarni, whose services are billed to the state at a rate of $125 an hour. Kulkarni reports to Assistant OAKS Program Manager Brian Welch – another Compuware contractor – whose services Compuware bills at $200 an hour. In turn, Welch reports to Phil Rowe, the data solutions team lead, who reports to White, the OAKS project manager.[4]

This unorthodox reporting structure and lack of management controls was clearly evidenced in Ilovar's actions on the morning that he discovered the break-in. Ilovar first reported the theft to Ring. The interns then sought out Kulkarni instead of his state supervisor, Rowe. In fact, Ilovar said he did not have his first conversation about the stolen tape with Rowe until Thursday, June 14, three days after the theft. Ilovar said Rowe apologized to him that day and told him responsibility for the backup tapes "shouldn't have been on my shoulders."

State Budget Director Pari Sabety said she learned "to my horror" after taking office in December 2006 that White's top aide, Welch, was a contractor with no fiduciary responsibility to the state. White's predecessor as OAKS program manager, Nola Haug, also worked for Compuware.

[4] Rowe replaced Carl Miller, who retired on May 31.

Our investigation found that White became so reliant on Compuware that it was Welch who directed the remaining interns' analysis of duplicate backup tapes after the theft, and it was Kulkarni to whom White turned when the state's chief privacy officer, Sol Bermann, emailed a series of questions about whether OAKS had a data-breach policy and whether the policy had been followed. Although White claimed during two interviews that he knew the answers to most of Bermann's questions, the answers he provided came from Kulkarni.

The dependence on contractors was one of the "major issues" identified in the gubernatorial transition report for OIT (Exhibit C). "There are serious issues with over-reliance on vendors/contractors in long-term or mission-critical roles," the report says, adding that "too often, they become fixtures at great expense and questionable ROI {return on investment} to the taxpayers." The report went on to all but predict a data-security calamity, saying, "Ohio's lack of a robust, unified privacy/security capacity lays it open to the type of data spills and breaches that have been plaguing the government and corporate sectors in increasing numbers over the past few years."

White discontinued the practice of taking home backup tapes shortly after the theft and assigned Rowe and Kulkarni to rewrite that section of the Business Continuity Plan. At the same time, state officials discovered and put a halt to an identical practice at OBM, where two network administrators had been taking home backup tapes since 1999. We are aware of no security breaches that occurred as a result.

Given the strenuous pace at which OAKS personnel have been working, the absence of a security plan and the loose supervision of the intern staff at OAKS, the OIT gubernatorial transition report appears to have been prescient.

Accordingly, we find reasonable cause to believe a wrongful act occurred in this instance.

Allegation 2: OAKS, OIT and OBM officials failed to report the theft of confidential information to state and law enforcement officials in a timely manner.

On the day of the theft, Ilovar actually had two OAKS backup tapes stored in a compartment in the driver's side door of his car. Only one was stolen.

Ilovar reported to work on Monday, June 11, 2007 – the morning he discovered that the tape was missing – and immediately reported the theft to Ring, a fellow OAKS intern. OAKS supervisors were off-site at the time and it was not until 11:30 a.m. that morning that Ilovar and Ring found Kulkarni and told him the tape was missing. In turn, Kulkarni and Ilovar sought out and reported the theft to White.

The three men agree that White instructed Ilovar to return home and file a theft report with Hilliard police. Thereafter, their stories diverge. Both Ilovar and Kulkarni contend that White told Ilovar not to tell police that the tape contained sensitive data. White contends that he gave Ilovar no specific instructions about what to tell police, but added: "I wanted to make sure we were dealing with what we knew and not something that we didn't know."

This strikes us as akin to waiting to put out the fire until you discover the cause of the flames. Informing law enforcement authorities of the potential risk and continuing to analyze a copy of the tape were not contradictory actions.

The report Ilovar filed with Hilliard police (Exhibit D) on June 11 at 12:43 p.m. is remarkable less for what it says than what it does not say. Ilovar told us he realized immediately that the stolen tape contained confidential human resources data, and the failure to inform Hilliard police of its significance may have cost authorities their best chance of recovering it. Many people are convinced that the thief tossed the tape in an area trash receptacle, either because he didn't realize the potential value of what he'd stolen or because the data were not easily accessible. Waste Management Inc. picks up

refuse at the Crystal Lake Apartment complex, where Ilovar lives, between 8 a.m. and noon on Tuesdays and Fridays, meaning authorities would have had nearly 24 hours after Ilovar filed his report to find the tape if this theory is correct.

Unfortunately, Ilovar's sketchy report to the Hilliard police was the last time any state official would raise a question about the involvement of law enforcement authorities until Thursday, June 14, nearly three days later. In an email she sent that day at 10:07 a.m., informing various state officials that she had given the governor's office a second briefing on the theft, Sabety wrote, "What police force is handling the incident? . . . Has anyone considered involving the Highway Patrol?"

Contributing to the failure to notify the Highway Patrol and other state officials in a timely manner was a complete breakdown in the reporting chain, beginning with White. Although White and Edmonson had ample reason to suspect immediately that the tape contained confidential data, a timeline of events (Exhibit E) we compiled shows that Edmonson did not notify Sabety of the theft until 3 p.m. on Tuesday, June 12, about 27 hours after Ilovar reported it to White.

White said he informed Edmonson that the tape contained sensitive data at a regularly scheduled meeting at 2 p.m. on Tuesday. By 3:39 p.m. that afternoon, Edmonson had that confirmation from White in writing. "Unfortunately, upon further investigation," White wrote, "we did discover some files that did contain SSNs and names."

Sabety provided the first briefing to Governor Strickland's senior staff on the morning of Wednesday, June 13, 2007. Nonetheless, Edmonson still had not informed Sabety that the tape contained sensitive data, and the governor, his chief of staff, John Haseley, and his chief legal counsel, Kent Markus, were meeting that morning with the House speaker and Senate president and thus were not at Sabety's briefing. With no apparent cause for alarm at that point, Sabety and Cabinet Secretary Jan Allen said they felt no need to notify Governor Strickland, Haseley or Markus of the theft later that day.

Perhaps the most astonishing aspect of this reporting breakdown was the failure of anyone to notify DAS Director Hugh Quill of the theft until Thursday, June 14, 2007. DAS and OBM share ownership of the OAKS project, but Quill said he did not learn about the theft until his communications chief, Ron Sylvester, mentioned it at 11 a.m. on June 14. By then, the governor's staff had been briefed, the administration had begun drafting plans to inform the public and provide potential victims with identity-theft protection, the OAKS Business Continuity Plan had been rewritten, and the administration had begun assembling a team and drafting talking points on how to deal with the media.

As for the governor, we determined that he was not notified of the data theft until 1:30 p.m. on Thursday, June 14. The patrol was formally called in at 3:30 p.m., and a patrol supervisor informed Hilliard police of the significance of the tape shortly thereafter. By then, more than four days had elapsed since Ilovar had reported the theft to White.

It is clear that OAKS, OIT and OBM officials were more fixated on analyzing the tape and assessing the level of risk than they were in recovering the stolen tape, even though they should have been pursuing both goals. Sabety said she wasn't initially alarmed because the information "percolating up from the OAKS types" was that "this isn't really serious because it's some high school kid that's taken it, and he doesn't know what he has." Given the passage of time, Sabety is now convinced that White withheld information until he had a large body of evidence that confirmed his early suspicions about the tape's contents.

White vehemently denies this, maintaining that although he knew "there was a potential for sensitive data on the tape," he acted appropriately by waiting to notify his superiors until he got "solid information." Nevertheless, White conceded to us that "the biggest mistake that I think I made is that I didn't escalate or notify people sooner." We agree.

Accordingly, we find reasonable cause to believe a wrongful act or omission occurred in this instance.

Allegation 3: OAKS administrators failed to protect confidential information by allowing personnel to store sensitive data in an unsecured folder on the OAKS intranet.

On February 26, 2007, Carl Miller, then the OAKS technical manager, received a call from an assistant state auditor. Using an old password and ID number, the auditor had just gained access to the OAKS intranet from a remote location and with a few keystrokes had been able to find the Social Security numbers of Miller and other OAKS personnel. The auditor wanted to know why.

Miller said he took this information to White, who ordered that all sensitive data be removed from the OAKS I: drive, the shared folder in which the assistant auditor had been trolling. Miller said he ordered a lockdown of the I: drive that day and instructed three college interns who had been hired as network administrators to begin combing the drive for Social Security numbers and other sensitive data.

Brian Ring, one of the interns to whom Miller gave this task, estimated that over the course of the next few weeks he and his colleagues moved 2,000 files containing confidential personal information off of the I: drive and into a more secure location. However, despite their efforts, "a lot of the data kept coming back," Ring said.

White received enough resistance to his order that he finally issued a memo to OAKS team supervisors on April 4, 2007: "I think that we have been discussing what we are going to do with the I: drive long enough. I want all files that can be identified with SSN data put into a secure directory today. All new discoveries will be put into the directory also. I want this done today and access reestablished to our end user."

For reasons that White, Miller and others have been unable to explain, Miller's previous oral orders and White's written order were never relayed to the database analysts who were running tests on large files containing sensitive data on the I: drive. White conceded

that he did not issue any orders to the analysts, nor did he order his team supervisors to do so. And, despite White's order to them, the team supervisors did not on their own initiative relay White's directive to their employees. So, although there was a temporary push to remove sensitive data from the I: drive, OAKS analysts continued to put the data back onto the drive. One analyst told us she placed multiple copies of a quarterly wage report containing the Social Security numbers of all state employees on the I: drive and had been working on it during the first week of June. Those files were backed up on the tape taken from Ilovar's car.

Even more confounding is a claim that Jerry Miller, one of White's team supervisors, made to us that White knew his directive was being ignored. Miller, who is not related to Carl Miller, said he permitted the 25 OAKS employees who report to him to continue to work on sensitive files on the I: drive because they had signed pledges not to reveal or otherwise misuse confidential data and needed to be able to access data in a shared environment. Consequently, Miller conceded, he did not feel a need to relay White's "I want this done today" directive to members of his team.

Carl Miller claims that Ring and the other interns assured him that the I: drive was purged of all sensitive data by May 31, 2007, the day he retired. However, this is unlikely. "There was never a point where I believed it was completely clean," Ring told us, "because every time we checked there was more."

As for White, he insists that his instructions were clear and should have been followed. If there is fault to be found, he said, it is a shared fault – with Carl Miller for not ensuring that the I: drive was scrubbed of all sensitive data, and with him for not following up.

Accordingly, we find reasonable cause to believe a wrongful act or omission occurred in this instance.

III. OTHER INCIDENTS

In the course of our investigation, we also became aware of two other data breaches involving OAKS.

The more serious of the two was the discovery by human resources personnel at the Ohio Court of Claims in May that they could access the Social Security numbers, dates of birth, bank account numbers and health care information of employees working in other state agencies. A court fiscal officer said she inadvertently found this information on the OAKS intranet while trying to determine why one of her employees had not received a paycheck. She then checked with human resources colleagues at the Ohio Supreme Court to ask whether they could pull up the same information. They could.

Nancy Kelly, deputy director of the Human Resources Division at DAS, said she immediately brought this "loophole" in OAKS to the attention of officials at Accenture, the company hired to do the system integration for OAKS. Kelly said she told Accenture officials that it "was unacceptable and that we needed to look to ways to tighten up the security." She said Accenture has assured her that the loophole is now closed and the Court of Claims fiscal officer confirmed that she no longer has access to the data.

The other breach occurred last December, when a DAS supervisor sent an email to 70 state employees working in various state agencies, informing them that they did not have email addresses in the OAKS system. The supervisor attached an Excel spreadsheet containing the employees' names and Social Security numbers and asked them to contact the OAKS Help Desk to obtain a user ID and password. A recipient of the email angrily contacted the DAS supervisor, asking her why she was sharing confidential information in such a cavalier manner. The supervisor subsequently recalled the email and asked all recipients to delete it.

Accordingly, we find reasonable cause to believe acts of omission occurred in both instances.

IV. CONCLUSION

One of the unfortunate ironies of this theft is that OAKS administrators allowed callow interns to take home backup tapes in order to protect the data in the event of a disaster at the OAKS facility and to save money. Instead, the policy – coupled with one intern's carelessness – created a potential disaster that may well cost the state more than $2 million in identity-theft prevention and protective services.

Fully informing law enforcement and other state authorities and continuing to analyze a duplicate of the stolen tape were not contradictory actions, and both should have been pursued with equal vigor. Nevertheless, Hilliard police were given virtually no information about the tape and its contents, White and Edmonson did not act with an appropriate sense of urgency and fully inform their superiors until too much time had elapsed, and no one asked the State Highway Patrol to investigate until four days after the theft was reported.

Large IT systems face numerous security threats, ranging from viruses to unauthorized access to data theft and abuse by insiders. A recent data-security brief issued by the National Association of State Chief Information Officers warns that "it is not a question of if a data breach will occur; it is only a question of when and how." Since January 2006 alone, 275 incidents have been reported nationwide in which a total of 155 million records containing sensitive information have been stolen, lost or improperly accessed.[5]

Given the elevated level of risk, it defies common sense that OAKS officials allowed state workers, contractors and interns to take backup tapes home. It also seems incongruous to us that OAKS officials considered the backup tapes important enough to

[5] "Chronology of Data Breaches," compiled by Sol Bermann, Ohio Chief Privacy Officer.

be shuttled back and forth between offices and homes, yet gave virtually no thought to trying to find one of the tapes after learning that it had been stolen.

Although we have identified numerous mistakes made by state officials and employees, there is shared blame here. A Compuware Corporation contract employee was a key member of the OAKS Configuration Management Team, which drafted the policy that permitted employees to take backup tapes home. That employee also was involved in the rewriting of the policy following the theft, and he directly supervised the intern who had the tape stolen from his car.

If there is a silver lining to be found in this matter, it is that despite the many poor decisions that were made, there appears to be little risk to state employees, taxpayers and vendors. Based on our interviews with data-security experts, the technical complexity of retrieving the data makes the possibility that it will be used for criminal purposes remote.

VI. RECOMMENDATIONS

Based on the results of our investigation, we are making the following recommendations:

1. OBM, DAS and OIT should take appropriate disciplinary action against individuals responsible for losing the data tape; failing to ensure that Hilliard police were apprised of the potential seriousness of the theft; downplaying the seriousness of the theft to superiors; and failing to ensure that sensitive information was removed from the OAKS I: drive.
2. OBM, DAS and OIT should conduct an administrative review of all state agencies, boards and commissions to determine whether they have authorized employees to take home backup tapes for storage and, if so, order them to cease.
3. OBM, DAS and OIT should ensure that all state agencies, boards and commissions utilize a secure method of storage for sensitive computerized data.
4. OBM, DAS and OIT should ensure that the OAKS project is brought under the jurisdiction of OIT's Security Incident Response policy.

5. OBM, DAS and OIT should ensure that a thorough security analysis of the OAKS project is conducted. We understand that Interhack Corporation is including this analysis in its scope of work. In addition, regular third-party security audits should be conducted to ensure the confidentiality, reliability and integrity of OAKS data. Policy reviews should be included as part of these regular audits.
6. OAKS should designate a chief security officer who is responsible for performing data security-related duties. This person, who should not be a contract employee, should be granted authority to make decisions regarding all information-security issues.
7. OBM, DAS and OIT should determine whether there is shared liability with contractors assigned to the OAKS project for costs associated with the theft of the tape.

We request that the appropriate agency respond to this office within the next 60 days with a plan explaining how these recommendations will be implemented.

EXHIBITS

EXHIBIT A

DATA CONTAINED ON STOLEN OAKS BACKUP TAPE

FILE	DESCRIPTION	PERSONAL IDENTIFIERS
Payroll	65,280 state workers	Names, SSNs
Pharmacy Benefits Participants and Vendors	53,797 policy holders 75,532 dependents	Names, SSNs
Electronic Funds Transfer Reimbursements	28,362 state workers and vendors	Addresses, phone numbers and banking information
State Teachers Retirement System Payments	467 STRS retirees (includes duplicates)	Names, SSNs, STRS account numbers
Medicaid	171,445 providers	Names, tax ID numbers, addresses, banking information
School Districts and Local Government	2,685 school districts and local governments	Names and bank account information
Payroll Vendors	1,200 vendors	Names, federal tax ID numbers, banking information
Temporary Assistance for Needy Families	153,517 records pertaining to uncashed TANF payments (includes duplicates)	Names, TANF case ID numbers
Uncashed State Personal Income Tax Refunds	771,126 taxpayers issued checks between 2005 and 2007	Names, SSNs, check amounts
Ohio Lottery	421 people and 25 businesses with uncashed checks (includes duplicates)	Names, SSNs
Unclaimed Funds Payments	1,531 people and 73 businesses with uncashed checks (includes duplicates)	Names, SSNs
Rejected Electronic Funds Transfers	388 people with EFT transactions bounced back from the banking institution (includes duplicates)	Names, bank account numbers

Total Number of Affected People, Employees, Dependants and Businesses – 1,194,732 (Source: Office of Budget and Management, as of July 13, 2007)

EXHIBIT B

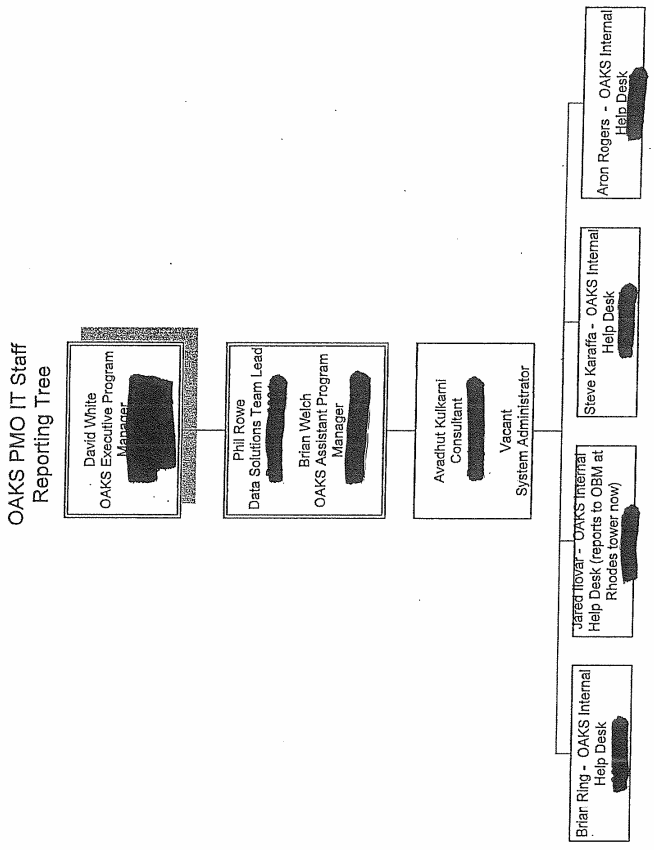
OAKS PMO IT Staff
Reporting Tree
David White
OAKS Executive Program
Manager
Phil Rowe
Data Solutions Team Lead
Brian Welch
OAKS Assistant Program
Manager
Avadhut Kulkarni
Consultant
Vacant
System Administrator
Briar Ring - OAKS Internal
Help Desk
Jared Tovar - OAKS Internal
Help Desk (reports to OBM at
Rhodes tower now)
Steve Karaffa - OAKS Internal
Help Desk
Aron Rogers - OAKS Internal
Help Desk

EXHIBIT C

GOVERNOR-ELECT TRANSITION DOCUMENT
OFFICE OF INFORMATION TECHNOLOGY

MAJOR ISSUES

Issue #1: Management & Governance

- **Project management:**
  - Project management competency at all levels is questionable. OIT management staff is noticeably lacking in management, organizational and operations skill sets.
- **Role of the CIO:**
  - Overall, the CIO's authority and mission are vague, as are the reporting structure and mechanisms of evaluation and accountability.
    - The CIO position states that it will advise the Governor on IT hardware, software, security, but there is little evidence this is occurring
    - The CIO position is a Cabinet-level position, but there is no discussion of the relationship of the CIO to other cabinet members.
  - Legislative Affairs and Communications are necessary components for the Office of the CIO.
    - Regular and consistent interaction at the most senior levels with the legislative branch does not occur. Does the legislature consider that position as one that is accountable for security, privacy, delivering projects on time, prioritizing IT investments, etc?
- **Influence over other Agencies:**
  - OIT has limited influence over agencies, except for process approval for agency purchases.
    - OIT is so far behind from a technology perspective that they have little credibility with other agencies (many individual agencies have their own CIOs; *also see Issue #2: Capacity & Planning*).
    - OIT has no compliance authority or mechanisms (carrot or stick) to compel agency and vendor accountability.
    - OIT lacks performance metrics and/or Service Level Agreements, which are a key element in a shared services environment.
- **Staffing:**
  - The number of people and the stand-alone nature of procurement and contract management are questionable. Monitoring and Audit seem to not take advantage of centralized offerings in other parts of government. OIT has not made the necessary investment in new technology or relevant training for their staff.

Issue #2: Capacity & Planning

- **OIT competency:**
  - OIT's advice and consul on technology and planning are rarely sought by other agencies as they feel they can do it cheaper and better by themselves or through vendors, consequently consultants are brought in for more challenging projects.

- Nearly all the agencies have surpassed OIT's technical capability leading to individual agency implementation in such areas as; Security (firewalls, intrusion detection/prevention), IP Telephony, networking, wireless, switching, and Application Development.
- The development and deployment of technology systems (software, hardware, business process reengineering) are conspicuously absent from the Executive Order, the Summary, the Implementation Plan, and all documentation generated thus far from the Office of Information Technology.

- **Enterprise Project Management Office**:
  - OIT has no true Enterprise Architecture in place. The EPMO does not function as a real Enterprise Program or Project Management Office; rather it supplies, through various arms of OIT, services and resources, but does not truly manage the program or project.
- **Strategic Plan/Future Planning**:
  - Overall, there is a dearth of future OIT planning, for example, the Strategic Plan on the OIT website lacks definitive goals or measurable objectives.
- **Standards Development**:
  - There is little evidence of publicly available standards and architecture; this may reflect poor standards development and/or the reality that agencies act independently.
- **OIT usage of FT consultants:**
  - There are serious issues with over-reliance on vendors/contractors in long term or mission critical roles. Judicious use (fixed length engagement with clear sunset guidelines, etc.) of consultants can be productive but too often, they become fixtures at great expense and questionable ROI to the taxpayers.

Issue #3: Privacy & Security

- OIT offers little-to-no policy guidance or standards in the areas of privacy and security.
  - No Chief Privacy Officer or Chief Security Officer for this, or any other, agency.
  - There is no evidence of PIA or SIA/STA usage.
  - Interagency data-sharing is imperative, but this is dangerously problematic without centralized privacy and security policies and standards throughout each agency. Without such policies and standards the chances of significant data breaches and spills are greatly increased.
  - There is no interaction with the legislature on privacy or security policy issues.

MAJOR BUDGET & PROCUREMENT ISSUES

- A $750m spend on an enterprise of $37Bis a technology spend of about 2%, a low number.
- The 10% payroll surcharge to pay for DAS administrative support offices (legal counsel, finance, human resources, and, ironically enough, desktop support) causes OIT to overcharge agencies for their services. Adding a surcharge to OIT's already weak services and then asking them to execute the shared services mission is a non-starter for many agencies, thus giving them another reason to seek IT services elsewhere..

- Procurement should play a role in compliance with enterprise architecture; this will allow for acquisition by statewide cross-agency needs instead of multiple, independent, agency solutions for the same functional requirements. This will, in turn, produce benefits in economies of scale, interoperability, business continuity, training/peer support and will discourage over-reliance on temporary staff/contractors.
- The State Term Schedule's (STS) process should be streamlined so that the time spent negotiating a new STS is condensed. It currently takes approximately three weeks to get an order through the DAS/OIT process.

REGULATORY REVIEW
The State as a whole lacks significant regulation/legislation in the areas of privacy and security.

INTERAGENCY IT PROJECTS
OAKS (covered by another team); MARCS; e-payment; centralized collection and disseminated forms all seem to reflect better planning and more successful governance, but was OIT the lead on any of these projects?.

STAKEHOLDERS

Agencies:
- Agencies see little value in OIT, leading to numerous agency level CIOs; 12 private networks throughout the State; and individual implementation of agency security policies, firewalls, intrusion prevention and desktop anti-virus software.
    - The only agencies using OIT do so because they are either too small to support a staff or they are in the planning stages to breakaway.

Vendors:
- Most vendors spend the majority of their time calling on the individual agencies, viewing OIT as necessary entity so they will not block purchases from other agencies.
- Contractors are often inappropriately used in internal (agency-to-agency) project/relationship management. Vendors without authority, knowledge of the process and political relationships, historical perspective and long-term stakes cannot effectively deliver top quality services. In addition, contractors are often not required to provide knowledge transfer plans and complete documentation of all systems and process work.
    - There is little evidence of how OIT evaluates the performance of vendors/service providers.
- Some standard procurement contract language is overly burdensome and prohibitive (ex: vendor unlimited liability). This language discourages best solution offerings from many of the most competent companies.

Business:
- The Ohio Business Gateway is successful in providing valuable and efficient services.

JOB-CREATION OPPORTUNITIES

An overall improvement in OIT's performance could streamline state government and allow for other agencies to better concentrate on their core missions, rather then spending duplicative efforts on IT.

CLOSING THOUGHTS & QUESTIONS TO CONSIDER

OIT was created to provide centralized standards, services and solutions, but their lack of capacity (especially managerial) and authority to implement the solutions exacerbates the very problem they were created to address. Under the current model, OIT does not proactively acquire, build or provide offerings needed by the agencies; therefore, there is no incentive for research and development of new/better solutions. This, in turn prevents OIT from offering useful services at a competitive cost, especially when burdened with the DAS surcharge. Ultimately, agencies are offered little incentive (carrot or stick) to use OIT services over outsourcing.

E-government: To quote one of the team, "E-government should be declared dead." Instead, it should be part of improved business processes embedded in the agencies, with an enterprise work management engine. In addition, benchmarking one state government against another is a meaningless indicator of success when a constituent's real life experience is Amazon or Yahoo.

Privacy & Security: Ohio's lack of a robust, unified privacy/security capacity lays it open to the type of data spills and breaches that have been plaguing the government and the corporate sectors in increasing numbers over the past few years. Without a comprehensive program that includes promulgation of policies, standards, tool usage, rule enforcement, monitoring and auditing, and legislative interaction, the danger of breaches similar to those experienced by Secretary of State Blackwell's office, the federal VA, Ohio University, and others, will continue to grow. Team members suggest an independent body outside OIT would be best suited to develop and lead such a comprehensive program. At the federal level, a model was developed under the Clinton Administration giving OMB the agency lead for programmatic development.

EXHIBIT D

OFFENSE REPORT
Hilliard Division of Police
3800 Municipal Way - Hilliard, OH 43026
614-876-2429

Incident # 507155	Call For Service # 25683	Record #(S) 38601
Offense Classification: Attempted Offense ☐ THEFT		Charges Filed? Yes ☐ No ☒
Location Occurred (and Business Name) [redacted] (PARKING LOT)		# Of Victims: 1
Date Occurred-Earliest 06-10-07	Date Occurred-Latest 06.11.07	Date Reported 06.11.07
Time Occurred-Earliest 2000	Time Occurred-Latest 0800	Time Reported 1243

Complainant: Last ILOVAR First JARED Middle

Address [redacted] City HILLIARD State OHIO Zip 43026

Home Phone	Work Phone	Other Number/Email Address
[redacted]	SAME	

Sex	Race	DOB	Age	SSN or OLN/STATE
M	W	[redacted]	22	

Victim #1 Same ☒ Last (Or Business Name) First Middle

Address City State Zip

Home Phone	Work Phone	Other Number/Email Address

Sex	Race	DOB	Age	SSN or OLN/STATE

Parent/Guardian If Victim is Juvenile Same ☐ Home # Work #

Address City State Zip

Facts: COMPLAINANT STATES UNKNOWN PERSON(S) GAINED ENTRY TO HIS VEHICLE AND REMOVED PROPERTY

Total Theft $ Loss For This Victim: 215.00

The above report is true and correct to the best of my knowledge.

X [signature] Complainant's Signature

Reporting Officer [signature] Badge # [redacted] Approving Officer [signature] Badge #

Hilliard, Ohio Division of Police
Stolen / Recovered Property Form

Incident# 85755	Copy to Incident#	Date and Time 06-11-07
Victim: JARED ADAM ILOVAR		Original Report ☒ Follow-Up ☐
*Property Status: S=Stolen R=Recovered		Page 1 of 1

QTY	Description: Make/Brand:	Model	Size/Cal.
1	RADAR DETECTOR	BEL TRONICS 955	
Status* S	Serial # AW0A8239	Each Item $	Total $ 200.00
LEADS/NCIC#	Date/Time:	Tech:	

QTY	Description: Make/Brand:	Model	Size/Cal.
1	H.D COMPUTER BACK UP TAPE IN CASE, FOR STOLE COMPUTER		
Status* S	Serial #	Each Item $	Total $ 15.00
LEADS /NCIC#	Date/Time:	Tech:	

QTY	Description: Make/Brand:	Model	Size/Cal.
Status*			
	Serial #	Each Item $	Total $
LEADS /NCIC#	Date/Time:	Tech:	

QTY	Description: Make/Brand:	Model	Size/Cal.
Status*			
	Serial #	Each Item $	Total $
LEADS /NCIC#	Date/Time:	Tech:	

QTY	Description: Make/Brand:	Model	Size/Cal.
Status*			
	Serial #	Each Item $	Total $
LEADS /NCIC#	Date/Time:	Tech:	

TOTAL $ AMOUNTS FOR PAGE	
STOLEN	$ 215.00
RECOVERED	$

Reporting Officer RD Quigley II	Badge #	Approving Officer	Badge#

EXHIBIT E

OAKS TIMELINE

Sunday, June 10

OAKS data tape containing backup data from Friday, June 8, is stolen from car of OAKS intern Jared Ilovar in Hilliard.

Monday, June 11

8-9 a.m. – Ilovar discovers that his car has been broken into. He goes to work and reports the theft to fellow intern Brian Ring (Sources: Ilovar and Ring interviews).

~11:30 a.m. – Ilovar reports theft to Compuware consultant Avadhut Kulkarni. They immediately report theft to OAKS Project Manager David White, who directs Ilovar to file a police report. (Sources: Ilovar, Kulkarni and White interviews).

12:43 p.m. – Ilovar files report with Hilliard police. White instructs him not to tell police that the tape contains sensitive data (White disputes this). (Sources: Ilovar and Kulkarni interviews).

1-1:30 p.m. – White informs Chief Information Officer Steve Edmonson of tape theft. White says he is unsure whether tape contains confidential data (Sources: White and Edmonson interviews).

4 p.m. – White calls Edmonson and tells him that he doesn't think the backup tape contained sensitive information. (Source: White interview).

4-4:30 p.m. – OAKS personnel determine that the stolen tape contains state employees' SSNs and sensitive data on all 65,000 state employees (Source: Ring interview).

6:28 p.m. – Kulkarni sends email to White, informing him that he found SSNs on the shared I: drive, where much of the data on the stolen tape was stored.

Tuesday, June 12

9:14 a.m. – Chief Privacy Officer Sol Bermann sends email to White, thanking him for bringing the theft to his attention. He asks for information on policies and procedures, including whether OAKS/DAS has a breach/incident policy.

10:35 a.m. – White sends email with Bermann's questions to Kulkarni, asking whether OAKS has a data-breach policy and whether it was followed.

12:16 p.m. – Kulkarni emails White a detailed response to Bermann's questions, which includes a listing of the confidential data on the stolen tape.

2 p.m. – At regularly scheduled meeting, White tells Edmonson and Bermann that tape may contain confidential data (Sources: White, Edmonson interviews).

3 p.m. – Edmonson reports theft to OBM Director Pari Sabety. He tells her he doesn't know whether it contained sensitive information (Sources: Edmonson, Sabety interviews, Administration timeline).

3:39 p.m. – White informs Bermann, Edmonson and OAKS Supervisor Phil Rowe in an email that "unfortunately, upon further investigation, we did discover some files that did contain SSN's and names."

4:57 p.m. – Bermann sends email saying he briefly sat down with Edmonson and Sabety "and we have begun discussing next steps."

5:02 p.m. – Kevin Brown emails Bermann and Daren Arnold a proposed Sensitive Data Security rule.

5:18 p.m. – Bermann sends email to Sabety and Edmonson re: "latest iteration" of proposed rule. Bermann says he has someone doing research on what other states are doing and is researching the importance of adopting encryption technology.

Wednesday, June 13

9 a.m. – Sabety informs Jan Allen, Jess Goode and other senior staff in governor's office of the theft but says she has no information about whether the tape contained SSNs or other sensitive data. Governor and Chief of Staff John Haseley are not present. (Sources: Sabety, Allen and Haseley interviews, Administration timeline).

9 p.m. – Sabety asks Bermann about status of inquiry (Sources: Sabety interview, Administration timeline).

9:43 p.m. – Sabety sends email to Bermann and Edmonson, saying she wants to brief governor's office on case status "tomw AM."

10:46 p.m. – Bermann responds in email to Sabety that he hasn't received any additional information about the backup tape and that "we are at the same place we were when we last talked." He says he will contact OAKS officials in the morning.

Thursday, June 14

6:33 a.m. – Bermann sends email to Sabety saying that OAKS was, "due to their unique position . . . not following any specific security incident response plan." He adds that

OAKS also was not following "relevant statewide security policies," adding, "I would recommend this changes." He adds that he is looking into encryption options.

9 a.m. – Sabety briefs senior staff in governor's office (Sources: Sabety, Allen and Haseley interviews, Administration timeline).

10:04 a.m. – White sends email to Edmonson saying OAKS has changed daily backup procedure and that backup tapes are now taken from building PM01 and stored in a locked communications room in building PM02.

10:07 a.m. – Sabety sends email to Rowe, Edmonson, White, Bermann and DAS spokesman Ron Sylvester saying she has briefed the governor's office on the tape incident. She poses several questions, including, "What police force is handling the incident? . . . Has anyone considered involving the Highway Patrol?"

10:22 a.m. – Kulkarni sends email to Bermann and copied to White, giving Bermann an update as to what data are on the stolen tapes.

10:47 a.m. – White informs Edmonson and Bermann that all state employees' SSNs are on the stolen tape (Source: Administration timeline).

11 a.m. – Sabety calls governor's office to update senior staff on latest development (Sources: Sabety interview, Administration timeline). DAS Director Hugh Quill is informed of the theft for the first time (Source: Quill interview).

11:23 a.m. – Sylvester sends email to White saying he's been asked "to walk point with the media on this issue" and needs copies of policies and procedures, including information on the backup process. Says "since this occurred Monday night/Tues. a.m., we're probably going to have to open up about it today or nlt (no later than) than tomorrow a.m."

11:49 a.m. – White sends email to Sylvester with attached copy of new OAKS backup plan. The new plan indicates that employees no longer take tapes home.

Noon – Sabety briefs DAS Director Hugh Quill and Edmonson (Sources: Sabety interview, Administration timeline).

1:30 p.m. – Strickland is notified of data theft (Source: Administration timeline).

2:30 p.m. – Governor orders State Highway Patrol to investigate (Source: Administration timeline).

3:30 p.m. – Highway Patrol formally notified of theft (Source: SHP).

4:57 p.m. – Sabety sends email to governor's Chief Legal Counsel Kent Markus, Allen and Sylvester, saying that while she acknowledges that "the potential data breach is the

story today . . . we also need to factor in the impact on the legitimacy of the OAKS 'go live' as a whole, and our competence." She adds: "I did not mean to be defensive, or participate in a 'blame game.' "

5:17 p.m. – Edmonson sends email to Sabety saying he has authorized a security review of OAKS "ASAP."

7:44 p.m. – Haseley sends email to Sabety, asking whether she has provided "some reassurance" to Ilovar.

8:04 p.m. – Sabety responds to Haseley in email that she has reassured Ilovar but that there may be a need for disciplinary action.

8:48 p.m. – Edmonson sends email to Allen, correcting timeline she is compiling. He says White first mentioned the stolen tape on Monday morning but didn't know whether it contained sensitive information. He adds that White informed him on Tuesday that it did contain sensitive information.

9:22 p.m. – Sabety sends email to various people in governor's office and DAS/OAKS, informing them that her records show that they all knew at 10:48 a.m. this morning that all state employees could be at risk. She congratulates them for being able to announce an executive order on security and privacy within 24 hours.

Friday, June 15

8 a.m. – Emails indicate that governor's office gets briefing on latest information pertaining to data theft.

10 a.m. – Governor publicly announces the theft. He signs Executive Order 2007-013S, putting the state chief privacy officer in charge of all data security; orders all agencies to designate a data-privacy point-of-contact within seven days; orders a third-party security assessment of OAKS; and orders the CPO to develop an encryption protocol within 75 days.

1:43 p.m. – OAKS supervisor Sheryl Harrington sends email to OAKS users, informing them that all media inquiries are to be directed to Sylvester.

2:38 p.m. – White sends email to Sabety, Rowe and Edmonson, attaching his 4/4/07 email ordering all sensitive data to be removed from a shared folder on the OAKS intranet known as the I: drive. Sabety responds: "Pretty clear instruction."

2:44 p.m. – White forwards another email string to Sabety, White and Rowe about the I: drive security issue.

2:47 p.m. – Sabety responds to White's email, saying, "Sounds like it has been a persistent problem. What were people supposed to do with their sensitive data? How was that treated?"

2:53 p.m. – White responds in email to Sabety that sensitive data was to be stored in secure directories on the network and that printouts were to be bagged for transport to a shredder.

3:10 p.m. – Governor's spokesman Keith Daily sends email to Sabety, Allen and Sylvester saying media are requesting the name of the employee who told intern to take the tape home.

3:56 p.m. – Responding to Daily's question, White sends email to Sabety, Rowe, Edmonson, Sylvester and Allen, saying that Ilovar was supervised by Carl Miller until May 31. He says Ilovar is now supervised by Rowe and worked closely with Kulkarni.

4:09 p.m. – Kulkarni sends email to White and Rowe with copy of updated Business Continuity Plan, which changes procedure for storage of backup tapes.