OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

E-Verify Vendor Data Security

Special Review

April 21, 2010 **Report 10-15**

Office of the Legislative Auditor
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

April 21, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Tom Hanson, Commissioner
Department of Management and Budget

This report presents the results of our special review of data security concerns related to the vendor, Lookout Services, Inc., selected to help state government implement E-Verify. We initiated the review after learning that a state employee had allegedly detected that E-Verify data could be accessed on Lookout Services' web site without adequate security protection.

We received the full cooperation of officials and staff at the Department of Management and Budget and the Office of Enterprise Technology.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA
Deputy Legislative Auditor

Table of Contents

Report Summary

In January 2008, Governor Pawlenty ordered the state to use E-Verify, a federal Web-based system that allows employers to verify whether newly hired employees are eligible to work in the United States. Use of the system requires the transmission of data—such as social security numbers—classified by law as not public.

The Office of the Legislative Auditor (OLA) conducted a special review of data security concerns related to state government's use of a private vendor, Lookout Services, Inc., to facilitate implementation of E-Verify. Our review focused on the actions of officials and staff in the Department of Employee Relations, which was initially responsible for implementation of E-Verify, and the Department of Management and Budget, which assumed responsibility for E-Verify after the departments of Employee Relations and Finance merged.

Findings

- The Department of Employee Relations conducted a limited assessment of Lookout Services before signing an agreement with the company to be the state's E-Verify vendor, and the agreement did not adequately address data security.

- After becoming responsible for implementing E-Verify and the state's agreement with Lookout Services in June 2008, the Department of Management and Budget left the data security issues unresolved and E-Verify unimplemented for over a year.

- The Department of Management and Budget renewed efforts to implement E-Verify after OLA issued an evaluation report in June 2009, but the department continued to make only limited efforts to obtain additional information about Lookout Services' ability and willingness to protect Minnesota's not public E-Verify data.

- The Department of Management and Budget made a limited response when alerted in November 2009 to possible data security problems at Lookout Services.

- The Department of Management and Budget suspended the state's use of Lookout Services after receiving a second notice in December 2009 that not public data on the company's Web site was not adequately secured. However, the department did not have state information technology staff assess the nature of the problem or the extent of its impact, and its notification letter to people potentially affected by the problem was based on information from Lookout Services.

E-Verify Vendor Data Security

Overview

E-Verify is a Web-based system administered by the Department of Homeland Security in partnership with the Social Security Administration. It was established to help employers comply with the Immigration Reform and Control Act,[1] which requires employers to verify that newly hired employees are eligible to work in the United States.[2] To comply with the law, employers must complete an Employment Eligibility Verification Form, also known as an "I-9," for every employee within three days of being hired. While the form can be completed on paper, E-Verify allows employers to complete it electronically and submit I-9 data over the Internet for analysis by federal data systems. An I-9 form contains personal data, such as an employee's name, address, date of birth, and social security number. Therefore, using E-Verify involves the transmission of not public data over the Internet.[3]

On January 7, 2008, Governor Pawlenty signed an executive order requiring use of E-Verify for newly hired employees in the executive branch of Minnesota state government.[4] Primary responsibility for implementation was assigned to the Department of Employee Relations. The department decided to hire a private company, Lookout Services, Inc., to facilitate implementation.

On December 10, 2009, the State of Minnesota suspended its agreement with Lookout Services. The action came after state officials learned that not public data on the company's Web site could be accessed without adequate security protection. On December 17, 2009, the Office of the Legislative Auditor (OLA) announced a special review of the circumstances that led to the state's action.

We made the decision to conduct a special review for two reasons. First, we wanted to follow up on an E-Verify evaluation report we issued in June 2009. During the evaluation, we learned that data security concerns related to the state's agreement with Lookout Services had stalled implementation of E-Verify. We wanted to determine whether those concerns were adequately resolved before the

[1]8 U.S.C. 1324a(a), *Immigration Reform and Control Act.*

[2]Federal rules prevent employers from using E-Verify to prescreen applicants for employment; data can only be submitted after a person has been offered employment. However, a negative result from E-Verify can be used to terminate an employment offer.

[3]According to *Minnesota Statutes* 2009, 13.02, subd. 8a, "not public data" include any government data which is classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic.

[4]The governor's executive order also required state contract vendors and certain employers receiving state subsidies to certify their compliance with federal immigration laws.

state moved forward to use Lookout Services as an E-Verify vendor. Second, we wanted to assess how state officials responded when informed that not public data on Lookout Services' Web site could be accessed without adequate security protection.

Scope and Methodology

Our review focused on the actions of executive officials in Minnesota state government and addressed the following questions:

- Did the Department of Employee Relations adequately assess Lookout Services before selecting the company to be the state's E-Verify vendor, and did the agreement it signed with the company adequately address data security?

- After assuming the responsibilities of the Department of Employee Relations in a merger, did the Department of Management and Budget[5] adequately resolve concerns about the state's agreement with Lookout Services before requiring state agencies to begin using Lookout Services to implement E-Verify?

- Did the Department of Management and Budget respond adequately when notified of possible data security problems related to Lookout Services?

To answer these questions, we interviewed officials and staff involved in implementing E-Verify, hiring Lookout Services, and responding to notifications of possible security problems at the company. In addition, we interviewed the state employee who first detected the data security problem at Lookout Services. We also reviewed documents, including e-mails, related to implementing E-Verify, hiring Lookout Services, and responding to reports of security problems at the company's E-Verify Web site. Finally, we reviewed information sent to us by Lookout Services.

[5]The department is also referred to as Minnesota Management and Budget (MMB).

Findings and Recommendations

Finding 1

The Department of Employee Relations conducted a limited assessment of Lookout Services before signing an agreement with the company to be the state's E-Verify vendor, and the agreement did not adequately address data security.

To implement the governor's executive order, state agencies could have been allowed to connect directly to E-Verify through the Web site administered by the U.S. Department of Homeland Security. However, the Department of Employee Relations decided to require agencies to connect through a private E-Verify vendor. E-Verify vendors provide Web-based services designed to enhance the use of E-Verify. For example, the department thought an E-Verify vendor's software would help ensure the accuracy of the state's I-9 data and compliance with federal requirements. In addition, the department wanted a vendor to provide a central electronic storage site for the state's I-9 data. Without a central data storage site, I-9 data would be maintained by individual agencies and would, therefore, not be readily available for use by state government or for review by federal authorities.

As with other types of information technology services that principally involve software, E-Verify vendors typically sell their services through a service agreement (also referred to as a "subscription"). The service agreement normally includes a license to use the vendor's software and provisions related to other services, such as training and a "help desk."

To identify potential E-Verify vendors, a Department of Employee Relations program manager working on implementation of E-Verify conducted an Internet search and identified several companies to consider. Shortly thereafter, program managers in the department selected Lookout Services, a company based in Bellaire, Texas, as the most promising possibility based on criteria established by the department and agencies that were going to use E-Verify.

According to the program managers involved, Lookout Services was selected based on four criteria: (1) Lookout Services was a U.S. Department of Homeland Security "designated agent" for E-Verify;[6] (2) Lookout Services had the ability to

[6]Although department officials and program managers thought being a Homeland Security "designated agent" was significant, the designation can be attained simply through a registration process that does not involve a substantive certification by the federal government. For E-Verify, the federal government defines a "designated agent" as any U.S. company, corporation, or business entity acting as a service provider using E-Verify to verify the employment eligibility of clients' new hires. Like other E-Verify users, designated agents must enroll in E-Verify and sign a memorandum of understanding agreeing to abide by system rules and responsibilities.

provide centralized electronic storage through its contract with a second company, Adhost, based in Seattle, Washington; (3) Lookout Services' software was deemed to have "good functionality" and seemed relatively easy to use; and (4) Lookout Services offered the lowest price.

In an e-mail dated February 14, 2008, the program manager that selected Lookout Services said:

> After reviewing a number of vendors, Lookout meets our requirements and has offered best pricing. They are the likely choice unless we identify major concerns with their ability to handle the state structure and how we do business.

In a later e-mail, another program manager said: "This vendor [Lookout Services] is too good to be true. I like their pricing approach." In fact, price was the deciding factor in the department's choice of Lookout Services to be the state's E-Verify vendor. Lookout Services proposed a price of $1.25 per I-9 transaction, which was four to five times lower than other vendors.[7] In addition, Lookout Services was willing to waive its "set-up fee." The program manager working on implementation of E-Verify estimated that the total annual cost of an agreement with Lookout Services would be $8,750.

One of the program managers involved in the selection of Lookout Services described the decision to hire the company as follows:

> We had minimum criteria. You know, they've got to be a designated agent, you've got to do this, that and the other thing, you've got to have checking, you have to produce -- you have to do reminder kinds of things for people who need re-verification. But …among the people that we demo'd, other than a couple that we just kind of rejected out of hand for various reasons, among what I would consider the finalists, it really came down to cost.

Program managers were concerned about cost in part because the department had not established a budget for the E-Verify vendor services it was seeking. One of the program managers involved in the search for a vendor told us:

> I was not given a budget at all, no. What we were trying to do is beg, borrow, and steal to try and do something to solve this need. And what we were hoping is that we could come forward with a solution that we could manage somehow.

[7]According to department documents, it received quotes from other vendors that ranged from $3.50 to $7.50 per I-9 transaction. When asked why Lookout Services was willing to price its services so much lower than other vendors, one of the department program mangers involved in selecting Lookout Services said it was because E-Verify was a "sideline" business of Morley and Morley, a small law firm that specialized in immigration law.

In addition to not having a budget for implementation of E-Verify, the department did not conduct a formal assessment of the data security risks involved with using an E-Verify vendor and did not conduct an independent security review of Lookout Services. In fact, information technology staff at the Office of Enterprise Technology and within the Department of Employee Relations were involved only to a limited degree in the selection of an E-Verify vendor.

According to an e-mail dated January 10, 2008, from an information technology manager within the department to other department staff working on implementation of E-Verify, the state's chief information security officer was contacted about the use of a vendor to implement E-Verify. According to the e-mail, the state's chief information security officer told the department official that his information security team was "swamped" with other projects and would not be able to participate in the selection process. Again, according to the e-mail:

> He [the state's chief information security officer] stated it is common practice to enter into contracts with vendors regarding services that require them to store nonpublic data, and he sees the State continuing to do that more and more as we realize the benefits of outsourcing rather than building or maintaining systems internally.
>
> To him, the most important aspect is ensuring we have a strong contractual agreement with the selected vendor. He strongly encourages us to review the contract DOER [the Department of Employee Relations] has with Blue Cross Blue Shield. He recalls looking at that language as it is strong in many areas, such as adequate controls, security (audit) requirements, and liability. He is willing to answer questions as needed.

The department's information security staff did participate in teleconference interviews with potential vendors and were asked to raise questions and listen for any information that caused "red flags." They also reviewed documents provided by Lookout Services. However, the documents they were given to review were limited. One information security staff person who reviewed the documents told us the documents were the "advertising version" of what companies claim to have as security. He also told us he was surprised at how little he was asked to be involved in the selection process given that the vendor would receive, transmit, and store not public data provided by Minnesota state agencies. He suggested the department could have taken several additional steps to assess a vendor's security controls, but it did not. For example, he said the department could have obtained documentation of the vendor's security policies and procedures and evidence that they were being followed. He also suggested the department could have done some testing of Web-based applications.

Despite these concerns and reservations, the consensus conclusion of the department's information technology staff about Lookout Services was positive. It was conveyed in an e-mail dated February 26, 2008, which said: "Overall, it looks like the vendor [Lookout Services] has a secure environment and good security practices. We don't have specific concerns."

As an alternative to obtaining more information about security at Lookout Services, information technology staff emphasized the need for security-related provisions in the service agreement. For example, the February 26, 2008, e-mail quoted above also recommended that there should be specific language in the service agreement regarding the role of the data storage company, Adhost, and how security breaches would be handled by both Lookout Services and Adhost. The recommendation reflected the advice reportedly given in January by the state's chief information security officer.

On March 16, 2008, the commissioner of Employee Relations approved having the department move forward with Lookout Services as the state's E-Verify vendor, saying in an e-mail, "Let's get this done." The commissioner signed a service agreement with Lookout Services on April 4, 2008. It was Lookout Services' "Standard Service Agreement," and the commissioner signed it without additions, amendments, or restrictions that reflected the state's data security interests.

On April 10, 2008, the staff person who had emphasized the need for strong data security provisions in the state's E-Verify vendor agreement sent an e-mail to a colleague, which said, "Thanks for sending me a copy [of the Lookout Services agreement] …it's the first time I've seen it." She went on to express numerous concerns about deficiencies in the agreement. One of the most significant deficiencies involved what the agreement said about the company's lack of responsibility for encrypted data. She called the company's position "unacceptable." She was referencing the following language in the agreement:

> Licensor [Lookout Services] assumes no responsibility for Licensee's [State of Minnesota's] encrypted data that is sent to, stored on, or retrieved off of a Licensor's server. The SSL technology used to encrypt data being transmitted to or from Licensor's secure server, if any, is licensed by Licensor and Licensor makes no claims or warranties regarding the viability, integrity, quality, endurance, sturdiness, strength, or robustness of the encryption used. Further, Licensor is not responsible for any failure of the secure server to properly encrypt data. By using the secure server, Licensee assumes the risk that the encryption algorithm may be broken so that the data being transmitted is visible to others.

She also pointed out that the agreement had "no mention of Licensor liability in the event of a security breach," and noted that the state's chief information security officer had strongly recommended that any information technology agreement should include language that clearly defined responsibility for security breaches.

Because of these concerns, the Department of Employee Relations put the state's agreement with Lookout Services and implementation of E-Verify on hold. State agencies continued to use their existing—largely paper-based—methods of completing I-9 forms and storing I-9 data to comply with the federal Immigration Reform and Control Act.

Finding 2

After becoming responsible for implementing E-Verify and the state's agreement with Lookout Services in June 2008, the Department of Management and Budget left the data security issues unresolved and E-Verify unimplemented for over a year.

On June 1, 2008, the departments of Employee Relations and Finance merged into the Department of Management and Budget. As a result, issues related to the state's agreement with Lookout Services and implementation of E-Verify became the responsibility of the Department of Management and Budget. However, several department officials we interviewed acknowledged they had many immediate and pressing issues to address in the months following the merger, and issues related to the Lookout Services agreement and E-Verify implementation were not among their highest priorities.

Department officials did ask the Attorney General's Office to draft an addendum to the state's agreement with Lookout Services aimed at correcting the deficiencies that had stalled implementation of E-Verify. The communications that occurred between the representative of the Attorney General's Office and Lookout Services during this time demonstrated that there was a clear connection between security and the company's pricing of its services. For example, in an e-mail to a representative of the Attorney General's Office dated September 10, 2008, an official at Lookout Services acknowledged the company had priced its agreement with the State of Minnesota to exclude liability for some security concerns. The e-mail said:

> Yes… security and liability are significant pricing issues. The language currently in the contract absolves us of liability for the use of the Internet and security through encryption because we don't control this aspect of the transfer.

Despite the importance of security and the link between security and Lookout Services' approach to pricing its services, the department considered, but did not propose, to pay more if the company would assume more responsibility for the

security of Minnesota's E-Verify data. In fact, the data security concerns related to the state's agreement with Lookout Services received little additional attention within the Department of Management and Budget until OLA issued a report on E-Verify in June 2009 noting the lack of progress in implementing the governor's E-Verify executive order.

Finding 3

The Department of Management and Budget renewed efforts to implement E-Verify after OLA issued an evaluation report in June 2009, but the department continued to make only limited efforts to obtain additional information about Lookout Services' ability and willingness to protect Minnesota's not public E-Verify data.

On June 10, 2009, OLA issued its evaluation report on E-Verify noting the department's lack of progress in implementing the governor's executive order.[8] Shortly after the report was released, the governor's chief of staff told department officials to make implementation a high priority. In response, there were renewed efforts to amend the state's agreement with Lookout Services.

During this time, department officials focused on obtaining more information about Adhost, the Seattle-based company Lookout Services was using to store I-9 data. Officials at the Department of Management and Budget thought the state's agreement with Lookout Services had been put on hold largely because it had not included enough information about Adhost and its relationship with Lookout Services.

On June 25, 2009, the department's deputy commissioner asked the department's chief information officer to "keep an eye on [the addendum to the Lookout Services agreement] to be sure that it's moving along." In response, the deputy commissioner was given assurance that the department had adequate information about security at Adhost. For example, one e-mail to the deputy commissioner dated June 25, 2009, said:

> We haven't seen the [addendum], but saw some evidence that the hosting vendor [Adhost] has a secure site based on audit information sent to us. One of the issues in the previous contract was that there was no evidence that there was any commitment from hosting vendor [Adhost] with our vendor to provide a secure site. The documentation of any agreement was not part of our contract, even though we believed it existed. Another issue raised by AG [the Attorney General's Office] last year was the liability limit is an insignificant amount. However, given the small size of the contract and the urgency to move forward, I am not sure how much more we can do.

[8]Minnesota Office of the Legislative Auditor, Program Evaluation Division, *E-Verify*, June 2009.

The department officials we interviewed acknowledged they knew very little about the audit information that was being used as assurance that the state's data would be stored at a secure site. And, at the time the information was being used to reassure the department's deputy commissioner, one department information security staff questioned its value. In an e-mail dated June 24, 2009, he said to his supervisor:

> This document [the audit report] doesn't have any descriptions of the controls they have in place, just whether or not the auditor believes the controls meet the control objectives… I can only say they appear to have a favorable SAS70 [audit] report based on some unknown set of control objectives.

Beyond the audit report on Adhost, the department did not seek additional information about security at either Lookout Services or Adhost. The only change to the agreement resulted from the addendum prepared by a representative of the Attorney General's Office. One amendment in the addendum deleted a section of the agreement that absolved Lookout Services of any obligation for encrypted data provided by the State of Minnesota. But the addendum did not contain an affirmative statement concerning the obligation of Lookout Services (or Adhost) to protect encrypted data provided by the State of Minnesota. Rather, it did contain two amendments that required Lookout Services to protect Minnesota's "confidential information" consistent with the *Minnesota Government Data Practices Act*.[9] The addendum was effective on June 30, 2009.

Finding 4

The Department of Management and Budget made a limited response when alerted in November 2009 to possible data security problems at Lookout Services.

After the addendum was effective, the Department of Management and Budget moved forward with the implementation of E-Verify by having state employees participate in training hosted on Lookout Service's Web site. During a training event that occurred on October 29, 2009, an employee of the Minnesota State Colleges and Universities (MnSCU) system was concerned that the computer screen being used in the training appeared to be displaying a Lookout Services Web site that contained not public data on individuals. After the training, the employee used her work computer to go back into Lookout Services' Web site where the data had been displayed, and she was again able to see not public data—names, birth dates, and social security numbers. The employee reported what had occurred to her supervisor, who verified that the data was accessible

[9] *Minnesota Statutes* 2009, Chapter 13.

without proper controls. The supervisor reported the issue to an official at the MnSCU System Office, and he notified the Department of Management and Budget.

Upon receiving the notice, a program manager at the Department of Management and Budget contacted the supervisor of the employee who discovered the alleged security problem to obtain additional information. However, based on information obtained from the supervisor, the program manager was not able to replicate access to the data in question. The program manager then contacted Lookout Services to discuss the alleged security problem and was given repeated assurances that the data in question was only "test data" that was part of a training database. However, the program manager who talked with Lookout Services was not an information technology specialist and did not involve the department's information security staff in an assessment of the alleged security problem. After several conversations with Lookout Services about what had been reported, the program manager was satisfied that a data security breach either had not occurred or, if it had occurred, it had been fixed. In addition, the program manager acknowledged being less concerned because the alleged breach did not involve State of Minnesota government data. The program manager told us:

> The fact that we couldn't get into anything. The fact that whatever had happened was corrected. And the fact that through at least five phone calls with this vendor I never thought that the vendor would not be truthful with me…. After the last phone call, I have to say that I didn't have any more concerns.

The department continued to move forward with training and implementation of E-Verify using Lookout Services.

Finding 5

The Department of Management and Budget suspended the state's use of Lookout Services after receiving a second notice in December 2009 that not public data on the company's Web site was not adequately secured. However, the department did not have state information technology staff assess the nature of the problem or the extent of its impact, and its notification letter to people potentially affected by the problem was based on information from Lookout Services.

The state employee who detected the data security problem at Lookout Services told us she was still concerned about Lookout Services several weeks after detecting the problem in late October. As a result, in mid-November and early December she sought additional information about Lookout Services through a Web search. During one search (using the standard Google search function), a Web link appeared that allowed the state employee unprotected access into individual and company-specific not public data on Lookout Services' Web site. The following events then occurred:

- On December 2, 2009, the employee notified her supervisor about what had occurred, and the supervisor was able to use the information provided by the employee to access not public data (names, social security numbers, birthdays, and other personal data). The information about these events was conveyed to an official at the Department of Management and Budget.

- On December 3, 2009, department program managers were able to use the information they were given to gain unprotected access into Lookout Services' Web site and viewed what they immediately thought was not public data, but noted that none of the data was Minnesota government data.

- On December 7, 2009, the program managers demonstrated to department officials how not public data could be accessed on the Lookout Services' Web site and discussed their concerns with officials at Lookout Services.

- On December 9, 2009, a reporter from Minnesota Public Radio contacted the department about an alleged data security breach at Lookout Services and met with the commissioner. Department officials again noted that Minnesota data was not involved.

- On December 10, 2009, a reporter from Minnesota Public Radio provided the department with not public data on an employee in Governor Pawlenty's office, allegedly obtained through accessing Lookout Services' E-Verify Web site.

- On December 10, 2009, the department directed Lookout Services to delete all State of Minnesota government data from the company's Web site and directed state agencies to stop using Lookout Services for E-Verify verifications.

- On December 14, 2009, Lookout Services filed a lawsuit against the State of Minnesota in the District Court of Harris County, Texas. The filing cited eight causes of action, including breach of contract and various violations of federal laws involving unauthorized intrusions ("hacking") into electronic data systems.

- On December 15, 2009, the department sent a letter notifying approximately 500 people that not public data related to them might have been inappropriately accessed on Lookout Services' Web site, but the letter minimized the likelihood and extent of any adverse impact.

The notification letter cited a statement from Lookout Services that "attempts" had been made against the company's Web site from "…computers with [Internet] addresses belonging to the State of Minnesota and Minnesota Public

Radio." Using this assertion, the department's notification letter concluded that only two individuals—a state employee and a Minnesota Public Radio reporter—had accessed not public data on Lookout Services' Web site. The letter said, "We do not believe that any personal information was stolen, nor do we believe it was accessed by anyone other than those two individuals."

The department made this assertion despite the fact that department officials told us they were able to easily access not public data on Lookout Services' Web site using a Web address obtained from a Google search. As one of the department officials involved told us:

> Googling Lookout Services, a number of sites came up on the Google page, going down to one and clicking on something. I don't recall that there was a whole lot of activity required to access the site. It was pretty enormously easy.

They also told us they ended the state's relationship with Lookout Services because they had become increasingly distrustful of information the company was offering in response to the state's concerns.

Officials at the Department of Management and Budget did not involve information security staff in the data security events that occurred in December. Both the department's chief information security officer and the state's chief information security officer told us they learned about the security problems at Lookout Services through actions of the Office of the Legislative Auditor.

We contacted the state's chief information security officer to request that the Office of Enterprise Technology conduct a forensic examination of the state computer used to detect the security problem at Lookout Services. The request was accepted and the examination was promptly conducted. It showed that E-Verify data on Lookout Services' Web site had been accessed from the state computer using a normal Web browser. Contrary to the assertion of Lookout Services, the forensic examination found no evidence of "hacking."

Finally, we note that after the department told state agencies to stop using Lookout Services, department officials did not consider using another E-Verify vendor as an intermediary. State agencies were told to register with the U.S. Department of Homeland Security and enter data directly onto E-Verify.

Recommendations

This report highlighted the problems two state agencies experienced implementing E-Verify by using an information technology vendor. The most serious problem—a data security breach—was the responsibility of the vendor, Lookout Services. But the state agencies also bear responsibility for some of the problems that occurred during the process of implementing E-Verify.

The state officials and program managers we talked with acknowledged their responsibilities and offered helpful insights into how the problems occurred. They pointed to such factors as the small amount of money that was involved, the nature of the service that was being purchased, the type of agreement that was used to purchase the service, and the disruptions and miscommunications that occurred during the merger of the departments of Employee Relations and Finance into the Department of Management and Budget.

We agree that all of these factors had an impact, but we think the limited involvement of information security staff was also important. Although using an E-Verify vendor cost a relatively small amount of money, it involves the transmission of not public data through a complex web of information technology. Yet, the process used to obtain and manage the E-Verify vendor was handled almost completely by officials and program managers who had limited expertise or experience with complex information technology systems.

We recommend:

- **When seeking services from an information technology vendor that involve the vendor obtaining, processing, transmitting, or storing not public data, the Department of Management and Budget should conduct and document an assessment of the security risks and how those risks will be addressed. The department should also ensure that information security specialists are fully involved in the process of identifying, selecting, contracting with, and monitoring the performance of the vendor.**

In addition, the Office of Enterprise Technology needs to take action. We recommend:

- **The Office of Enterprise Technology should establish policies and procedures state agencies must follow when seeking services from an information technology vendor that involve the vendor obtaining, processing, transmitting, or storing not public data. The office should also establish policies and procedures that ensure that information security specialists are fully involved in the process of identifying, selecting, contracting with, and monitoring the performance of the vendor.**

During our review, we learned that the officials and program managers involved in selecting Lookout Services were unable to avail themselves of state established data security standards in selecting and managing an E-Verify vendor because state standards have not been established. They all agreed that standards would have been helpful.

The responsibility to establish statewide data security standards rests with the Office of Enterprise Technology. *Minnesota Statutes* 2009, 16E.01, says, "The office [of Enterprise Technology] shall provide oversight, leadership, and direction for information and telecommunications technology policy and the management, delivery, accessibility, and security of information and telecommunications technology systems and services in Minnesota." It also says the office has a duty to "ensure overall security of the state's information and technology systems and services."

As part of our review, we interviewed the state's chief information security officer, and he strongly endorsed the need for a comprehensive set of security standards for state agencies to follow in selecting and managing information technology vendors, especially when not public data are involved. He indicated that development of the standards has been part of the Office of Enterprise Technology's work plan since the office was created in 2006. However, he told us that other projects and limited resources have made it impossible for the office to complete the standards. He also pointed out that the office is monitoring the development of national standards and efforts in private companies to address issues related to vendor security. He said the office is scheduled to have standards for state agencies to use by the middle of 2011. While we appreciate the many challenges the Office of Enterprise Technology has had to address with limited resources and its deliberative approach to establishing policies and standards, this report demonstrates there is an urgent need for the Office of Enterprise Technology to act more quickly to address issues related to vendor selection and management in state government.

Given the size, complexity, and decentralized operations of Minnesota state government, we recognize that the security of not public data will not be ensured simply by having the Office of Enterprise Technology establish policies and procedures. The many state agencies that sign contracts and service agreements with information technology vendors will have to rigorously apply the policies and procedures developed by the Office of Enterprise Technology. In addition, for some kinds of information technology services, agencies will need to go beyond general policies and procedures and develop more specific requirements and expectations. Nevertheless, the Office of Enterprise Technology was created and given specific responsibilities related to the security of information technology and data systems. Our review demonstrated that there is a clear need for the office to fulfill those responsibilities.

MINNESOTA Management & Budget

April 19, 2010

Mr. James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street, Room 140
St. Paul, MN 55155

Dear Mr. Nobles:

Thank you for the opportunity to discuss your review and recommendations regarding the department's agreement with Lookout Services, Inc. MMB is committed to proper and secure data management and this retrospective is helpful. In that spirit, we will continue to improve our own standards and advocate for comprehensive enterprise-wide guidelines.

This department, and all other state departments, must balance risks, resources, and performance on a daily basis in a complex, dynamic environment. The report provides a useful chronology of events that highlights the on-going need for statewide data security standards and review. I appreciate the efforts of all state employees to address the issues that arose in this project while having to work with rapidly changing information.

MMB deals with many technology projects but at the outset this subscription contract had seemed to be more of a programmatic activity. With this review in place, we see that there is no distinction. From the onset of the project, multiple factors impacted the department's approach:

- The project was for a subscription service, an increasingly common method of delivery, but one that has not been the norm for state contracts in the past.
- The project was small in cost – the anticipated yearly expenditure would have been less than $8,750. The actual total spent by the state on this contract was $753.
- Security standards do not exist for the review, selection and monitoring of these small IT subscription service projects.

The experience with this project has increased our appreciation that even the smallest IT project requires extensive review to reduce risk. To that end, we have commenced discussions to clarify expectations and roles regarding information security for future projects, and to assure that projects currently underway have had robust security reviews.

We fully support the recommendation that Office of Enterprise Technology establish standards to guide contracting decisions and monitoring activities for contracts such as this one, and further that those standards be communicated widely to state program managers who likely will be the initiators of such purchases in their agencies.

Sincerely,

Tom J. Hanson

Tom J. Hanson
Commissioner

400 Centennial Building • 658 Cedar Street • St. Paul, Minnesota 55155
Voice: (651) 201-8000 • Fax: (651) 296-8685 • TTY: 1-800-627-3529
An Equal Opportunity Employer

THE OFFICE OF
ENTERPRISE TECHNOLOGY
STATE OF MINNESOTA

April 19, 2010

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street 140
Centennial Office Building
St. Paul, MN 55 155-4708

Dear Mr. Nobles:

Thank you for the opportunity to respond to the E-Verify Special Investigation Report.

We concur that the Office of Enterprise Technology should take a leadership role in the assessment of managed service provider security controls. As this report clearly illustrates, even agencies with large information technology departments and experienced security professionals have difficulty understanding and assessing the pertinent security risks.

Our new Enterprise Security Program has provided agencies with industry best practice documents to help them understand and assess managed service provider risks. However, it is important to go one step further and develop formal standards that all agencies must follow. Entering into agreements with managed service providers without first doing a rigorous information security control validation can no longer be an acceptable business practice.

When we started the Enterprise Security Office about three years ago, we hoped that we would have sufficient resources for a team of security professionals to provide direct assistance to agencies in this area. However, due to limited resources, we were forced to make difficult decisions to focus on other more pressing issues, such as enterprise vulnerability management, security monitoring, and access controls. OET's recently submitted Comprehensive Information Security Funding Strategy discusses in greater depths the benefits and limitations of the current IT security funding. In light of the E-Verify report and the Security Funding report, OET is open to again discussing the need for more central security professionals to help agencies with third-party assessments and other security needs.

Finally, I would like to thank the talented members of the audit team who conducted this difficult assignment. Their efforts and recommendations will make the Office of Enterprise Technology a more effective agency.

Sincerely,

Gopal Khanna
State Chief Information Officer