OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Employment and Economic Development

Unemployment Insurance Program

Information Technology Audit

December 3, 2009 **Report 09-36**

FINANCIAL AUDIT DIVISION
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

Financial Audit Division

The Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division has a staff of forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division, which evaluates topics periodically selected by the Legislative Audit Commission.

Reports issued by both OLA divisions are solely the responsibility of OLA and may not reflect the views of the Legislative Audit Commission, its individual members, or other members of the Minnesota Legislature. For more information about OLA reports, go to:

http://www.auditor.leg.state.mn.us

To obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

To offer comments about our work or suggest an audit, investigation, or evaluation, call 651-296-4708 or e-mail auditor@state.mn.us.

OLA

OFFICE OF THE LEGISLATIVE AUDITOR

State of Minnesota • James Nobles, Legislative Auditor

December 3, 2009

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Dan McElroy, Commissioner
Department of Employment and Economic Development

This report presents the results of our audit of the Department of Employment and Economic Development's controls for the information technology used to administer the state's Unemployment Insurance Program. This report contains eight findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with department staff on November 19, 2009. Management's response to our findings and recommendations is presented in the accompanying section of this report titled, *Agency Response.*

The audit was conducted by Eric Wion (Audit Manager), Carolyn Engstrom (Auditor-in-Charge), John Kelcher (Senior Auditor), Aimee Martin (Senior Auditor), and Bill Betthauser (Senior Auditor).

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Table of Contents

Report Summary

Conclusion

The Department of Employment and Economic Development did not have adequate security controls for the information technology system used to administer the state's Unemployment Insurance Program.

Findings

- The Department of Employment and Economic Development did not have a comprehensive security management program for its information technology systems. (Finding 1, page 5)
- The Department of Employment and Economic Development had not formalized how it would correct vulnerabilities in computers accessible through the Internet, and it had not routinely scanned computers connected to its internal network for vulnerabilities. (Finding 2, page 7)
- The Department of Employment and Economic Development did not have monitoring procedures to detect and promptly respond to security-related events. (Finding 3, page 7)
- The Department of Employment and Economic Development did not adequately restrict some information technology staff from direct access to the Unemployment Insurance Program's database, implement data encryption to mitigate inappropriate access, and monitor activities users performed in the database. (Finding 4, page 8)
- The Department of Employment and Economic Development did not have adequate procedures for managing its firewall and did not sufficiently restrict computer traffic in its internal private network. (Finding 5, page 10)
- The Department of Employment and Economic Development did not enforce strong password controls. (Finding 6, page 12)
- The Department of Employment and Economic Development's change management and software development procedures were not security focused. (Finding 7, page 12)
- The Department of Employment and Economic Development had not established an offsite location to relocate the Unemployment Insurance Program's computer system in the event of a disruption and had not documented a continuity of operations plan. (Finding 8, page 13)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Employment and Economic Development have adequate security controls for the information technology used to administer the state's Unemployment Insurance Program?

We assessed controls as of August 2009.

Department of Employment and Economic Development

Unemployment Insurance Program

Overview

The Department of Employment and Economic Development (the department) administers programs related to business assistance, workforce and community development, international trade, and unemployment insurance. For the state's Unemployment Insurance Program, the department calculates and collects tax revenues from employers, calculates and pays benefits to individuals, and helps resolve disputes concerning tax liability and benefit eligibility. In fiscal year 2009, over 336,000 people applied for unemployment benefits, and the department paid over $1.8 billion in benefits.

In 2007, the department completed the implementation of a $43 million computer system that automated most aspects of the Unemployment Insurance Program. A significant element of the new system is that employers and benefit applicants use the internet or telephone to access the system to make payments and apply for benefits.

The department's information technology unit manages the department's computing environment, including the system that administers the Unemployment Insurance Program. The department relies on the Office of Enterprise Technology to manage some aspects of the Unemployment Insurance Program's database. The database contains the detailed information submitted by employers and benefit recipients.

Objective, Scope, and Methodology

The audit objective was to answer the following question:

- Did the Department of Employment and Economic Development have adequate security controls for the information technology system used to administer the state's Unemployment Insurance Program?

To answer this question, we interviewed staff of the department and the Office of Enterprise Technology. We reviewed policies, procedures, and other relevant documentation. We also used a variety of computer-assisted auditing tools and other techniques to analyze the security infrastructure and test controls. We assessed controls as of August 2009.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in *Special Publication 800-53 Recommended Security Controls for Federal Information Systems*, published by the National Institute of Standards and Technology's Computer Security Division. We also used criteria contained in security guidance published by the Defense Information Systems Agency and information published by applicable technology vendors to evaluate select controls. When available, we also used department and state policies to obtain evaluation criteria.

Conclusion

We concluded that the Department of Employment and Economic Development did not have adequate security controls for the information technology system used to administer the state's Unemployment Insurance Program.

The following *Findings and Recommendations* section explains the deficiencies.

Findings and Recommendations

Finding 1

The Department of Employment and Economic Development did not have a comprehensive security management program for its information technology systems.

An information technology security management program is a formal method used by an organization to identify and manage risks and ensure that it has adequate controls in place to help prevent security incidents from occurring and quickly detect and respond to incidents when they occur.

Because the department had not developed a comprehensive security management program for its information technology systems, it had not defined key security objectives, goals, and responsibilities. Staff turnover in the chief information security officer position may have hampered development of the program. The current chief information security officer, hired in July 2009, is the third person to hold that position over the past three years. In addition, the chief information security officer did not have staff to help accomplish the position's duties. Given the size and complexity of the department (about 1,600 employees, 60 workforce centers, about 3,000 laptop and desktop computers, and over 300 computer servers), it is likely that a chief information security officer would need professional security staff to help build a successful information technology security management program at the department.

Implementation of a security management program would also require input from other individuals and groups in the department, particularly those involved in developing and operating the department's information technology systems. However, the department did not clearly define the security roles and responsibilities for these individuals and groups. For example, most information technology position descriptions lacked security-related requirements or tasks. Key governance committees (the Information Steering Committee, the Change Advisory Board, and the Architecture Planning Team) lacked defined responsibilities and outcomes related to security. The service level agreement between the department's management and its information technology division did not define the roles and responsibilities for security, and the department had not updated the agreement since 2007. The department could potentially overlook critical tasks if it does not clearly define security expectations and responsibilities for individuals and groups. Much responsibility for security rests with employees who also must support daily operations. Without clear documentation of the employee's security duties, daily operational tasks typically take priority and may be at odds with good security practices.

Finally, the department did not have written policies, standards, and procedures addressing information technology risks and security. These are critical because they outline management's security expectations. They also help define employees' roles and responsibilities. Employees cannot make consistent security decisions without policies and standards to refer to as guidance. Had the department proactively defined and communicated its security expectations, it may have averted the findings in this report.

While the department should have a comprehensive security management program that covers all of its information technology systems, it is particularly important for the department to address security for the system it uses to administer the state's Unemployment Insurance Program. That system annually processes millions of dollars in tax revenues and benefit payments; it contains a large amount of private data; and it is available through the Internet. It is one of the state's most important information technology systems. The findings of this report indicate that the department has not adequately addressed the system's risks and vulnerabilities.

Recommendation

- *The department should develop a comprehensive security management program for its information technology systems.*

  - *It should define the program's scope, objectives, goals, and responsibilities and assess whether it has sufficient security staff to design, implement, and monitor the effectiveness of the security program.*

  - *It should define and document the roles and responsibilities of individuals and groups that play a vital role in security and develop a training program to communicate their security responsibilities and to improve awareness of key risks and controls.*

  - *It should develop risk assessment methodologies and perform periodic assessments.*

  - *It should develop written security policies, standards, and procedures and monitor compliance with them.*

Finding 2

The Department of Employment and Economic Development had not formalized how it would correct vulnerabilities identified in computers accessible through the Internet, and it had not routinely scanned computers connected to its internal network for vulnerabilities.

The department did not have processes in place to correct computer vulnerabilities identified by the Office of Enterprise Technology when the office scanned the department's computers that were accessible from the Internet. The Office of Enterprise Technology uses an Enterprise Vulnerability Management System to assist state agencies in identifying vulnerable computer systems. The Office of Enterprise Technology conducts monthly external scans of Internet accessible state computers to find exploitable security vulnerabilities, such as a flaw in a commercial software product that a hacker could use to force a computer program to perform an unauthorized operation. Department staff had not resolved some vulnerabilities identified by the Office of Enterprise Technology's scans in a timely manner. It is important for the agency to correct these vulnerabilities because hackers often take advantage of them. In addition, the department did not routinely scan other computers accessible from inside the department for vulnerabilities. State policy requires each agency to manage and monitor their computers for vulnerabilities and implement and maintain vulnerability remediation processes.[1]

Recommendation

- *The department should develop a formal vulnerability and threat management program to ensure it routinely scans computers and corrects critical vulnerabilities in a timely manner.*

Finding 3

The Department of Employment and Economic Development did not have effective monitoring procedures to detect and promptly respond to security-related events.

The department's monitoring procedures were not sufficient to detect and appropriately respond to important security-related events, such as potential external attacks, unauthorized attempts to access computers, employee system misuse, changes to critical computer settings, access to sensitive files, and exceptions to defined policies and procedures.

The department's monitoring efforts were not effective because it had not assessed which security-related events put the system at highest risk and had not customized its computers to log those high-risk events. The logs for some of the department's computers included all security-related events, while other logs did

[1] *Office of Enterprise Technology: Enterprise Security Vulnerability Management Policy 2008-04.*

not include some rudimentary, but critical, security events. Department staff was not regularly and proactively reviewing any of its logs. The department had not assigned the review of the logs to specific staff, identified how often they should review the logs, or prescribed the action they should take in response to suspicious activity. The department did not have software to assist in the gathering and analyzing of security logs to identify events that require attention.

Finally, the department did not develop and implement a strategy to ensure it maintained, backed up, and archived all security log records. It is important to have historic log information available should the department or law enforcement need to conduct an investigation.

Without an adequate monitoring system, the department would be unable to take timely and appropriate action to protect the system and its data if an attack occurred.

Recommendations

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the review. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.*

- *The department should define procedures for employees to follow when a security incident is identified.*

- *The department should define and follow its records retention requirements for security log records.*

Finding 4

The Department of Employment and Economic Development did not adequately restrict some information technology staff from direct access to the Unemployment Insurance Program's database, implement data encryption to mitigate inappropriate access, and monitor activities users performed in the database.

The department did not adequately limit access to the database containing the Unemployment Insurance Program's data. It did not have a process to periodically review and recertify employees' database access privileges. Furthermore, department staff often did not document the security decisions, making security administration difficult. The department and the Office of Enterprise Technology jointly managed the database; however, they had not documented, through a service level agreement, each agency's security roles and responsibilities.

Some employees had incompatible or unnecessary access to the database without the department establishing effective mitigating controls. For example, 15 software developers, 4 business analysts, and a system architect had the ability to connect directly to the database, and read significant amounts of data, including not public data such as applicant's social security numbers and banking information. Several people, including software developers, shared four passwords that could modify or delete virtually any data. Also, over 30 people had access to the unencrypted passwords that were stored in a poorly secured electronic file. Two Office of Enterprise Technology employees had database privileges that allowed them to read, update, and delete any data that they did not need for their day-to-day job duties. The ability to connect directly to the database and read or modify data should be restricted to a few individuals.[2] Furthermore, software developers should not have the ability to modify data because they have intimate knowledge of the system's functions and would be in a position to perpetrate and hide fraudulent transactions. Finally, individual accountability is lost when people share passwords.

The department did not ensure that the Office of Enterprise Technology adequately restricted the connection of external computers directly to the database. An Office of Enterprise Technology managed firewall allowed any computer on the state's network to pass traffic through the firewall and attempt to connect directly to the database. In general, these connections should be limited to very few people and computers at the department and the Office of Enterprise Technology.

The department did not encrypt some not public data during transmission and storage. Although the department properly encrypted not public data when someone used the Unemployment Insurance Program's computer system, it did not encrypt data when employees connected directly to the database. Also, it did not encrypt not public data, such as social security numbers and banking information, stored in the database. Encryption converts data into a format that cannot be read and is an important control to help protect data from unauthorized disclosure.

The department did not limit the amount and type of not public data used in its test environment by software developers and others; it used a complete copy of the unemployment insurance database. Because test environments typically have less rigorous controls, the database's substantial amounts of not public data may have been subjected to more risk of inappropriate use or access. Although, the department sometimes needed to use original not public data to test certain aspects of the system, it did not minimize the volume of data, specify the period of time it retained the data, and implement strong security controls to protect the not public data from unauthorized disclosure.

[2] Defense Information Systems Agency's Database Security Technical Implementation Guide, Section 3.3.11.

Finally, the department did not have any database monitoring controls to identify security-related events, such as unauthorized changes to data or employee misuse of not public data.

Recommendations

- *The department should periodically review and recertify that it appropriately limits database user's access.*

- *The department should further restrict who can access not public data and prohibit software developers from modifying or deleting system data or establish effective mitigating controls.*

- *The department should prohibit the sharing of passwords.*

- *The department should work with the Office of Enterprise Technology to develop firewall rules that adequately restrict access to the database.*

- *The department should encrypt not public data during transmission between internal servers. The department should also implement appropriate encryption of data stored in the database.*

- *The department should limit the amount of not public data in its test environment. It should minimize the volume of data, specify the period of time it is retained, and implement strong security controls to protect it from unauthorized disclosure.*

- *The department should develop and implement database-monitoring controls.*

Finding 5

The Department of Employment and Economic Development did not have adequate procedures for managing its firewall and did not sufficiently restrict computer traffic in its internal private network.

The department lacked formal firewall management procedures and it did not define who had primary responsibility for managing the firewall. A firewall typically is an organization's first line of defense against external threats from hackers. A firewall is a computer that separates an organization's private internal network from the public Internet. Serving as gatekeeper, a firewall examines all traffic that attempts to enter or leave an organization's private network. Traffic that does not meet certain conditions, defined in firewall rules, cannot pass in or out of the private network.

The department did not have adequate documentation of its firewall's extensive rules. The department did not have documentation of the business purpose of the rules and had not periodically reviewed the rules to ensure that they were still appropriate. The department did not require staff to document and obtain authorization for rule changes. A formal change management process would include request, review, and approval procedures. Without adequate documentation, staff was not sure about the purpose of some rules. Staff identified some of the rules they reviewed for our audit as unnecessary or outdated and believed others to be more restrictive than they actually were.

In addition, the department did not delegate primary firewall management responsibilities to specific employees who would coordinate and manage changes to the firewall. With seven employees who could independently make changes to the firewall, the department could not ensure that all changes were necessary or appropriate. In addition, these seven employees also had powerful and incompatible access to the department's computer servers, including web servers and application servers.

Finally, the department did not sufficiently restrict computer traffic between portions or segments of its internal private network. Internal network segmentation and filtering improves control by only allowing authorized traffic in or out of each segment on the private internal network. Without adequate filtering, someone who gained unauthorized access to portions of the department's private internal network could freely move throughout the network and attempt to access any computer and software on them. Segmentation and filtering also help prevent the spread of malicious software, such as viruses, worms, and trojans.

Recommendations

- *The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.*

- *The department should conduct a complete review of its firewall rules. It should remove redundant or unneeded rules and further restrict excessively permissive rules.*

- *The department should filter computer traffic between segments on its internal network to only allow authorized traffic between each segment.*

Finding 6

The Department of Employment and Economic Development did not enforce strong password controls.

The department did not use customizable features to enforce strong password controls on some computers. Employees use passwords to prevent unauthorized access to their system accounts. The department could set the customizable features to prevent employees from selecting easy to guess passwords, like dictionary words, and to require that employees periodically change their passwords. The features could also disable accounts employees had not used for prolonged periods or that had repeated failed logon attempts, which might be an indication of someone trying to get unauthorized access. Also, some "administrator" accounts, which generally allowed changes to security settings, installation of software and hardware, and access to files, had inadequate passwords, and some staff shared log on identification and passwords to these powerful accounts.

Strong password controls are important because they help prevent employees and hackers from assuming the identity of legitimate system users. When employees share log on identification and passwords, the department is unable to determine which employee is responsible for specific actions.

Recommendation

- *The department should implement and enforce strong passwords and should not allow employees to share log on identification.*

Finding 7

The Department of Employment and Economic Development's change management and software development procedures were not security focused.

Computer systems often require frequent changes. Those changes can vary widely and often include developing new or modifying existing software, installing vendor-provided security and software fixes, changing critical computer settings, modifying data to correct errors in the database, and upgrading software versions. Change management is a formal process of managing and controlling all changes to the technology infrastructure. Its purpose is to implement only appropriate and authorized changes into the business environment.

The department's change management procedures were not security focused. The department had some computers that were running outdated versions of commercial software, some of which were no longer supported by the vendor. In some instances, there was justification for delaying software upgrades, but the agency lacked documented strategies for determining when and how they would apply the updates in the future.

The department's software development program did not adequately focus on security. It had not established software development standards to document how staff should code software to ensure adequate security. The department lacked a security-focused training program for its software developers. The department lacked procedures to review and test newly written software to ensure it did not contain security vulnerabilities prior to implementing it. The Unemployment Insurance Program's computer system is a custom-developed application that requires significant ongoing development. The system is a web-based system that is accessible from the Internet. The overall security of the system relies on a well-developed software code. Failure to follow stringent change management procedures and secure software development and testing procedures may result in unauthorized changes, computer disruption, or security vulnerabilities.

Recommendations

- *The department should develop adequate change management procedures to ensure computer-related changes are appropriate and authorized.*

- *The department should develop security-focused software development standards.*

- *The department should develop procedures to review and test newly written software to ensure it does not contain security vulnerabilities prior to implementing it.*

- *The department should develop a training program to ensure its software developers have adequate security-focused training.*

Finding 8

The Department of Employment and Economic Development had not established an offsite location to relocate the Unemployment Insurance Program's computer system in the event of a disruption and had not documented a technology recovery plan.

The department did not have a documented and tested plan to recover the Unemployment Insurance Program's computer system should a significant event cause it to be unavailable. When the department approved the project to develop the system, the project's scope and budget did not include an adequate recovery strategy even though the department defined the system as a mission critical system that needed high availability and a short recovery timeframe.

Many events could cause the system to be unavailable, such as natural disasters like tornadoes, floods, or fires; computer viruses or computer failures; or terrorism. Having an up-to-date, documented, tested plan increases the likelihood the department could recover from a disruption and continue to provide unemployment insurance services.

Recommendations

- *The department should document and test a recovery plan for the Unemployment Insurance Program's computer system following accepted project management methodologies.*

- *The department should assess the impact of any significant project so technology recovery plans do not become outdated.*

positively Minnesota Department of Employment and Economic Development

November 30, 2009

Mr. James R. Nobles
Legislative Auditor
First Floor, Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

The Minnesota Office of the Legislative Auditor (OLA) conducted a thorough audit of the Department of Employment and Economic Development (DEED) Unemployment Insurance (UI) system during the summer of 2009. The DEED Business and Information Technology team has reviewed the auditor's findings in-depth and has provided formal responses to each finding in the attached document.

The findings have led DEED to develop more formalized information security programs based on new information security standards adopted by the state of Minnesota. These new standards will reduce or eliminate security vulnerabilities and ensure that data and information about Minnesota citizens are protected from unauthorized access. We would like to point out that to date there has been no loss of data, nor has data about Minnesota citizens been compromised.

We take seriously our security controls and are working with internal business leaders and the Office of Enterprise Technology (OET) to prioritize the auditor's findings, reduce or eliminate vulnerabilities, implement sound technical controls and develop security documentation. Our efforts will help ensure that DEED information assets are safeguarded against unauthorized access, modification, disclosure, theft, and breach from either internal or external sources.

The auditor's findings and recommendations are among several information security, technical control and risk management improvements that are under way at DEED. It is my priority to maintain the confidentiality, availability and integrity of the information that is entrusted to us for serving the people of Minnesota.

If you have any questions or need additional information, please contact Henry May at henry.may@state.mn.us or 651-259–7007.

Sincerely,

Dan McElroy
Commissioner

DEED AUDIT FINDINGS, RECOMMENDATIONS AND REPSONSES -

Audit Finding 1: The Department of Employment and Economic Development did not have a comprehensive security management program for its information technology systems.

Recommendations:

- *It should define the program's scope, objectives, goals and responsibilities and assess whether it has sufficient security staff to design, implement and monitor the effectiveness of the security program.*
- *It should define and document the roles and responsibilities of individuals and groups that play a vital role in security and develop a training program to communicate their security responsibilities and to improve awareness of key risks and controls.*
- *It should develop written security policies, standards and procedures, and monitor compliance with them.*

Response: The department agrees with the finding and recommendations. While DEED maintains internal controls, generally they have not been well-documented and monitored. DEED has now created a strategic information security charter and policies, a risk control policy, security standards and processes to deliver an effective information security management program. In addition, we developed a three-year plan and budget, which includes additional resources. The DEED Information Security Management Plan is on-going and will adapt to future risk and vulnerabilities. Reginald Williams, chief information security officer (CISO), will be responsible for the mitigation of this finding by Dec. 31, 2009.

Audit Finding 2: The Department of Employment and Economic Development had not formalized how it would correct vulnerabilities identified in computers accessible through the Internet, and it had not routinely scanned computers connected to its internal network for vulnerabilities.

Recommendations:

- *The department should develop a formal vulnerability and threat management program to ensure it routinely scans computers and corrects critical vulnerabilities in a timely manner.*

Response: The department agrees with the finding and recommendation. DEED has created network vulnerability technical controls and documentation to perform network vulnerability scan assessments weekly, and on a monthly basis on DEED internal networks, VLANS, servers, remote sites, workstations, resource rooms and multiple network devices. Plans include vulnerability remediation for current and future internal network vulnerability findings. OET has jurisdiction of DEED's external network vulnerabilities. The CISO obtains periodic reports and coordinates with OET Information Security on potential external network vulnerabilities. Henry May, chief information officer (CIO), will oversee the resolution of this finding by Dec. 31, 2009.

Audit Finding 3: The Department of Employment and Economic Development did not have effective monitoring procedures to detect and promptly respond to security-related events.

Recommendations:

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the review. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.*
- *The department should define procedures for employees to follow when a security incident is identified.*
- *The department should define and follow its records retention requirements for security log records.*

Response: The department agrees with the finding and recommendations. DEED does not have a monitoring and detection program because a technical security infrastructure must be in place prior to the implementation of file integrity or an intrusion detection program. A policy and process have been created to monitor and review information risk, perform risk analysis and perform mitigation based upon the risk factors and probabilities. DEED has a work plan under way to purchase an appliance to monitor and detect authorized access to sensitive files. The CIO will oversee the implementation of the file integrity, monitoring and detection technology plan by Oct. 31, 2010.

Audit Finding 4: The Department of Employment and Economic Development did not adequately restrict some information technology staff from direct access to the Unemployment Insurance Program's database, implement data encryption to mitigate inappropriate access, and monitor activities users performed in the database.

Recommendations:

- *The department should periodically review and recertify that it appropriately limits database users' access.*
- *The department should further restrict who can access not-public data and prohibit software developers from modifying or deleting system data or establish effective mitigating controls.*
- *The department should prohibit the sharing of passwords.*
- *The department should work with the Office of Enterprise Technology to develop firewall rules that adequately restrict access to the database.*
- *The department should encrypt not-public data during transmission between internal servers. The department should also implement appropriate encryption of data stored in the database.*
- *The department should limit the amount of not-public data in its test environment. It should minimize the volume of data, specify the period of time it is retained, and implement strong security controls to protect it from unauthorized disclosure.*
- *The department should develop and implement database- monitoring controls.*

Response: The department agrees with the finding but does not fully agree with the recommendations. A DEED process is under way to strengthen the controls around account access to the database. These controls include additional tracking and monitoring of database changes. DEED will accept the risk of having privileged staff with direct access to the database and will have an exception signed by the UI director and the CIO. DEED will also establish compensating controls within the process to strengthen the account access to the database.

DEED will take under advisement the recommendation to encrypt data on the database and to limit the amount of data on the test database. Both these recommendations need to be analyzed to determine the business impacts. DEED will work with OET to determine the best approach for adding additional encryption to internal data transmissions and the impacts to the business. DEED will work with OET to determine if the firewall rules need further restrictions and the impacts to the business. The CIO will oversee the resolution of this finding by March 31, 2010.

Audit Finding 5: The Department of Employment and Economic Development did not have adequate procedures for managing its firewall and did not sufficiently restrict computer traffic in its internal private network.

Recommendations:

- *The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.*
- *The department should conduct a complete review of its firewall rules. It should remove redundant or unneeded rules and further restrict excessively permissive rules.*
- *The department should filter computer traffic between segments on its internal network to only allow authorized traffic between each segment.*

Response: The department agrees with the finding and recommendations. A DEED process is under way to create a firewall policy to request, review and approval firewall rule changes. A contractor has been selected to perform rule analysis, recertify rules, upgrade the firewall operating system, close idle ports and services, and remove unused or unverifiable firewall rule sets. DEED will accept the risk of network employees performing multiple roles (firewall, network and server administration) simultaneously with elevated account privileges. In addition, DEED will accept the risk of employees' non-segregation roles because of limited resources; however, compensating controls will be implemented. The CIO will oversee the resolution of this finding by Feb. 28, 2010.

Audit Finding 6: The Department of Employment and Economic Development did not enforce strong password controls.

Recommendation:

- *The department should implement and enforce strong passwords and should not allow employees to share log on identification.*

Response: The department agrees with the finding and recommendation. DEED has created a security standard to establish, implement and enforce complex password parameters on servers, domains and workstations. A DEED security standard indicates that user passwords will not be shared unless expressly approved and documented by the CISO. Technical password controls shall be implemented on servers, domains, laptops and workstations. The CIO will oversee the resolution of this finding by March 31, 2010.

Audit Finding 7: The Department of Employment and Economic Development's change management and software development procedures were not security focused.

Recommendations:

- *The department should develop adequate change management procedures to ensure computer-related changes are appropriate and authorized.*
- *The department should develop security-focused software development standards.*
- *The department should develop procedures to review and test newly written software to ensure it does not contain security vulnerabilities prior to implementing it.*
- *The department should develop a training program to ensure its software developers have adequate security-focused training.*

Response: Technical Support –The department agrees that formal change management procedures need to be implemented to ensure computer-related changes are appropriately reviewed and approved. DEED is currently assessing tools to assist with the tracking and approval of such changes, refining current processes and establishing a formal Change Advisory Board. The CIO will oversee the resolution of this finding by March 31, 2010.

Application Development – The department does not fully agree with the finding and recommendations. DEED has a software development standards document for the UI application that includes sections that are focused on security. The DEED application is built in a security-focused framework so software testing inherently uses the security rules that are built into the application. The developers will attend the OET software security training by March 31, 2010.

Audit Finding 8: The Department of Employment and Economic Development had not established an off-site location to relocate the Unemployment Insurance Program's computer system in the event of a disruption and had not documented a technology recovery plan.

Recommendations:

- *The department should document and test a recovery plan for the Unemployment Insurance Program's computer system following accepted project management methodologies.*
- *The department should assess the impact of any significant project so technology recovery plans do not become outdated.*

Response: The department agrees with the finding and recommendations. DEED has created a Statement of Work (SOW) to solicit a contractor to develop and create the UI Disaster Recovery (DR) program documentation in coordination with the DEED Business Continuity program. An initial UI DR funding allocation has been established by the federal government and a process is under way to select a contractor by Jan. 12, 2010. The UI DR project will be ongoing and requires additional funding and business commitment. Work will commence in January 2010 related to the UI DR planning, development and documentation. The CISO will oversee the resolution of this finding by June 2010 and address future resource commitments.