

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU

LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
Fax No.: (775) 684-6600



LEGISLATIVE COMMISSION (775) 684-6800
JOHN OCEGUERA, *Assemblyman, Chairman*
Lorne J. Malkiewich, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
BERNICE MATHEWS, *Senator, Co-Chair*
STEVEN HORSFORD, *Senator, Co-Chair*
Mark Krmpotic, *Fiscal Analyst*
Rick Combs, *Fiscal Analyst*

LORNE J. MALKIEWICH, *Director*
(775) 684-6800

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
PAUL V. TOWNSEND, *Legislative Auditor* (775) 684-6815
DONALD O. WILLIAMS, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

We have completed an audit of the Department of Business and Industry Information Technology Security. This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions. The results of our audit, including findings, conclusions, recommendations, and the Department's response, are presented in this report.

We wish to express our appreciation to the management and staff of the Department of Business and Industry for their assistance during the audit.

Respectfully presented,

Paul V. Townsend, CPA
Legislative Auditor

November 23, 2010
Carson City, Nevada

STATE OF NEVADA
DEPARTMENT OF BUSINESS AND INDUSTRY
INFORMATION TECHNOLOGY SECURITY

AUDIT REPORT

Table of Contents

	<u>Page</u>
Executive Summary	1
Introduction	6
Background	6
Scope and Objective	7
Findings and Recommendations	8
Sensitive Information Was Not Encrypted	8
Routine Network Maintenance Needs Improvement	10
Virus Protection Was Not Up-To-Date	10
Critical Software Updates Were Not Installed	11
Weaknesses Exist in Managing Network Users	11
Former Employees Had Current Network Access	11
Background Investigations Were Not Conducted	12
Other Security-related Controls	12
Employees Were Not Provided With Ongoing Information Security Awareness Training	13
Servers Were Not Properly Protected	13
A Wireless Network Was Not Properly Secured	13
Web Servers Could Be Made More Secure	14
Appendices	
A. Audit Methodology	15
B. Response from the Department of Business and Industry	17

EXECUTIVE SUMMARY

DEPARTMENT OF BUSINESS AND INDUSTRY INFORMATION TECHNOLOGY SECURITY

Background

The Department of Business and Industry consists of a Director's Office and 14 subordinate agencies, commissions, and programs with a main objective of encouraging and promoting growth, development, and the legal operation of businesses within the State of Nevada. The Department's activities also include regulation of business and industrial enterprises; promotion of worker safety, protection, and rights; and administration of bond programs to encourage growth and development of businesses within the state. The 14 organization subdivisions include:

- Athletic Commission
- Attorney for Injured Workers
- Dairy Commission
- Employee Management Relations Board
- Financial Institutions Division
- Housing Division
- Industrial Relations Division
- Insurance Division
- Labor Commission
- Manufactured Housing Division
- Mortgage Lending Division
- Nevada Transportation Authority
- Real Estate Division
- Taxicab Authority

For fiscal year 2010 the Department was authorized 673 full-time employees statewide and had authorized expenditures of approximately \$144 million.

EXECUTIVE SUMMARY

DEPARTMENT OF BUSINESS AND INDUSTRY INFORMATION TECHNOLOGY SECURITY

Purpose

The purpose of this audit was to determine if the confidentiality, integrity, and availability of the Department's sensitive information and information systems were properly protected. This audit included a review of information technology controls at the Department during fiscal year 2010.

Results in Brief

Weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of the Department's sensitive information and information systems. These weaknesses included computers storing unencrypted sensitive personal identifying information. In addition, computers did not have adequate virus protection and lacked current critical software updates. Furthermore, former employees had current network access and background investigations were not conducted on staff with the greatest access to confidential information.

Other security-related controls need improvement. For example, ongoing security awareness training was not conducted to maintain staff awareness of information security risks. In addition, some servers were not properly protected, a wireless network was not adequately secured, and web servers had vulnerabilities.

Principal Findings

- Confidential personal information was stored unencrypted on Department computers. Six Department divisions had application databases

EXECUTIVE SUMMARY

DEPARTMENT OF BUSINESS AND INDUSTRY INFORMATION TECHNOLOGY SECURITY

containing substantial amounts of unencrypted personal information such as social security numbers. In addition, we identified 23 other computers storing unencrypted personal information. This included 7 servers and 16 individual desktop computers that contained this personal information. If this information is inadvertently accessed or released, the Department would be required to contact all of the affected persons. (page 8)

- Virus protection software was not current or not installed on some Department computers. Of the 161 individual desktop computers sampled, we found 24 computers or 15% of our sample that lacked adequate antivirus protection. We also found additional computers without virus protection during other audit tests. In all, we found 29 computers without adequate virus protection. Virus definition ages averaged over 206 days old on these computers. State security standards require that all computers have antivirus software installed and current virus definition files. Without current virus protection, there is increased risk that computers will become infected. (page 10)
- Seven computers were missing critical software security patches. This included four desktop computers and three servers. One computer had not been updated for 438 days. If critical software security updates are not installed, there is increased risk that computers will be vulnerable to various hacker attacks and exploits. (page 11)
- Five former employees' network access had not been disabled in a timely manner. The duration these five accounts remained enabled after the employee had left the agency ranged from 102 days to 7.5 years. State security standards require the prompt removal of users who are no longer in the Department's service in order to reduce the risk of someone gaining

EXECUTIVE SUMMARY

DEPARTMENT OF BUSINESS AND INDUSTRY INFORMATION TECHNOLOGY SECURITY

unauthorized access to the state's network and data. (page 11)

- Background investigations are not conducted throughout the Department. State security standards require that state employees in positions identified as sensitive have background investigations conducted. Without conducting background investigations on staff with the greatest access to sensitive information and systems, the risk increases that a person with an unsuitable background could be hired or granted access to these systems. (page 12)
- Ongoing security awareness training was not being conducted throughout the Department. The intent of this training is to ensure that all new and existing employees, consultants, and contractors are aware of their responsibilities in protecting the state's information systems and information processed through them. Without annual information security refresher training, there is greater risk that employees will not adequately protect state information systems and data. (page 13)
- Six of the 26 (23%) network servers or server rooms were not adequately protected. This included unrestricted access to equipment and one room with a leaky roof. Unrestricted physical access to network servers increases the risk of accidental damage and theft or vandalism. Such problems could also result in the release of confidential data or the loss of use of the computer network. (page 13)
- One division had an improperly secured wireless access point. The wireless access point could allow access to the state's network. Improperly secured wireless network configurations represent "backdoors" into an otherwise secure computer network. These backdoors can allow unauthorized access to state information technology resources and confidential data. (page 13)

EXECUTIVE SUMMARY

DEPARTMENT OF BUSINESS AND INDUSTRY INFORMATION TECHNOLOGY SECURITY

- We identified three web servers whose configurations could be made more secure. Scans of these web servers revealed several vulnerabilities in their configurations. These vulnerabilities could allow hackers to modify the web servers and cause them to malfunction. Staff indicated they had not previously conducted vulnerability scans on these web servers. (page 14)

Recommendations

This audit report contains 11 recommendations to improve the information security at the Department of Business and Industry. These recommendations address controls over security of confidential information. In addition, these recommendations address controls over managing network users, network maintenance, and other security-related controls. (page 25)

Agency Response

The Department, in response to the audit report, accepted the 11 recommendations. (page 17)

Introduction

Background

The Department of Business and Industry consists of a Director's Office and 14 agencies, commissions, and programs with a main objective of encouraging and promoting growth, development, and legal operation of businesses within the State of Nevada. The Department's activities also include regulation of business and industrial enterprises; promotion of worker safety, protection, and rights; and administration of bond programs to encourage growth and development of businesses within the State. The 14 subordinate entities include:

- Athletic Commission
- Attorney for Injured Workers
- Dairy Commission
- Employee Management Relations Board
- Financial Institutions Division
- Housing Division
- Industrial Relations Division
- Insurance Division
- Labor Commission
- Manufactured Housing Division
- Mortgage Lending Division
- Nevada Transportation Authority
- Real Estate Division
- Taxicab Authority

For fiscal year 2010 the Department was authorized 673 full-time employees statewide and had authorized expenditures of approximately \$144 million. The Department has over 30 offices statewide with primary locations in Las Vegas, Carson City, Reno, and Henderson.

Scope and Objective

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to the provisions of NRS 218G.010 to 218G.350. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This audit included a review of information technology controls at the Department of Business and Industry during fiscal year 2010. The objective of our audit was to determine if the Department's information security controls were adequate to protect the confidentiality, integrity, and availability of its sensitive information and information systems.

Findings and Recommendations

Weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of the Department's sensitive information and information systems. These weaknesses included computers storing unencrypted sensitive personal identifying information. In addition, computers did not have adequate virus protection and lacked critical software updates. Furthermore, former employees had current network access and background investigations were not conducted on staff with the greatest access to confidential information.

Other security-related controls need improvement. For example, ongoing security awareness training was not conducted to maintain staff awareness of information security risks. In addition, some servers were not properly protected, a wireless network was not adequately secured, and web servers had vulnerabilities.

Sensitive Information Was Not Encrypted

The Department stored unencrypted personal identifying information (PII) in several application databases, several servers used for file storage, and on individual user desktop computers. Personal identifying information is often collected and stored on state computers in the course of doing business. Such information can include names, social security numbers, driver's license numbers, and other confidential personal information that, if not protected, could lead to identity theft.

We identified six Department agencies that collected and stored personal identifying information such as unencrypted social security numbers (SSNs) in their application databases. For example, the Industrial Relations Division uses a Claims Indexing database to help detect workers compensation fraud. That database contains personal records that include SSNs. The data is not encrypted as required by state security standards.

We also identified 23 other computers storing unencrypted licensee social security numbers. This included 7 servers and 16 individual desktop computers that contained this information. This information was contained in spreadsheets, tables, and

other user created documents. This information also was not encrypted as required by state security standards.

In addition, one division was not authorized to collect the personal information stored in its database. NRS 239B.030 requires agencies to be specifically authorized to collect personal information from the public. While several Department divisions collect personal information with such specific NRS authority, the Housing Division collected SSNs without such authorization. Prior to completion of our audit, the division indicated it is now only collecting the final four digits of program participant SSNs as allowed by NRS 239B.030 and it has replaced the five leading digits of all SSNs in its database with zeros.

Collecting and storing PII such as unencrypted social security numbers puts the agency at risk of losing sensitive data and then making the time consuming and expensive notifications of affected persons. Some agency staff indicated they were unaware of the requirement to encrypt sensitive information. Users with PII on their individual desktop computers stated they were often unaware that such data resided on their hard drives. The sensitive data was sometimes from previous computer users.

Management indicated that the Department was testing a data storage appliance which encrypts data to address the data stored on file servers and individual desktop computers. In addition, management indicated it would work with each agency to remove the unneeded sensitive data, which currently resides on file servers and desktop computers. The application databases, containing the largest amount of unencrypted personal information, remain the greatest risk to unauthorized access and should be encrypted as software upgrades make this capability available.

In addition to encryption, there are other short-term options. For example, one division indicated it has taken steps to remove the five leading digits of the social security number in accordance with NRS 603A.040. Another division is in the process of masking or hiding social security numbers so employees cannot view them. While these solutions are not as ideal as encryption, they offer some protection.

Recommendations

1. Discontinue collection of SSNs where not authorized by law.

2. Remove or mask the five leading digits of all existing SSNs in agency databases where possible.
3. Develop a plan to encrypt sensitive data as hardware and software upgrades make this capability available.

Routine Network Maintenance Needs Improvement

Routine maintenance needs greater attention to ensure adequate security is maintained. This includes ensuring virus protection is current and that operating system security updates are installed.

Virus Protection Was Not Up-To-Date

We found that 24 of 161 (15%) desktop computers we sampled at Department locations throughout the state lacked adequate virus protection. In addition, we identified five other computers without adequate virus protection while examining servers and agency virus management software. In all, we identified a total of 29 Department computers that did not have adequate virus protection. Some computers did not have antivirus software installed while others were missing current virus definitions. Virus definition ages averaged about 206 days old on these computers.

State security standards require that all agencies' computers have virus protection software installed and that they should update virus protection software and definition files as new releases and updates become available. Computers without current virus protection are at risk of being corrupted by computer viruses from the Internet or other sources. Employees with infected computers will lose productive time while their computers are purged of the infected files.

Management indicated that the Department was taking actions to address the issues causing the virus problems. These actions included modification of the network infrastructure to support centralized virus software updates across all agencies, informing contractors who provide PC support of the need to re-install antivirus software when they rebuild computers, and requesting funding to procure virus protection software for all PCs and servers.

Critical Software Updates Were Not Installed

Seven computers were missing critical software security updates, or patches. This included four desktop computers and three servers. One computer had not been updated for 438 days. State security standards indicate that agencies must demonstrate a process in progress to install critical security patches within 72 hours (3 working days) from the date of release by the vendor.

Computers without current software security patches represent a weakness in the agency's computer network defense system. These weaknesses can be exploited by hackers to gain unauthorized access to the Department's information systems.

Recommendations

4. Develop procedures to identify computers without current virus protection.
5. Develop a procedure to periodically check software update installations to detect failed or missing update installations.

Weaknesses Exist in Managing Network Users

The Department did not always remove former employees' network access. In addition, background investigations were not conducted on employees with the greatest access to sensitive information and systems as required by state security standards.

Former Employees Had Current Network Access

Five former employees' network access had not been disabled in a timely manner. The duration these five accounts remained enabled after the employees had left the agency ranged from 102 days to 7.5 years. Allowing former employees to have network access increases the risk that the network could be accessed by non-authorized personnel.

State security standards indicate the Information Security Officer (ISO) shall review the user list quarterly to verify accuracy and document the results. If the Department had conducted such a review, it could have identified these former employees with current network access.

Background Investigations Were Not Conducted

Background investigations are not conducted throughout the Department. State security standards require that state employees in positions identified as sensitive have background investigations conducted. An example of a sensitive position is one that has a major responsibility for the development, planning, direction, or implementation of a computer security program.

Without conducting background investigations on staff with the greatest access to sensitive information and systems, the risk increases that a person with an unsuitable background could be hired or granted access to these systems. Management and staff indicated they were not aware of the requirement for background investigations until the requirement was identified during our audit.

Management indicated they would consider performing background checks when funding specifically for background checks was made available. Due to current funding constraints, our discussions with Department management focused on initially conducting background investigations on a limited number of IT staff with high-level access to sensitive data and systems. However, future plans should include a risk-based approach to conducting background investigations on the remainder of employees with access to sensitive information and systems.

Recommendations

6. Follow state security standards by conducting quarterly reviews of user lists.
7. Conduct background investigations on employees with the greatest access to sensitive information or systems.

Other Security-related Controls

We found several other areas where security could be improved. For example, ongoing security awareness training for computer users was not always conducted. In addition, mission critical servers and the sensitive information they contained were not always properly protected. One wireless network was not properly configured. Finally, web servers could be made more secure.

Employees Were Not Provided With Ongoing Information Security Awareness Training

Ongoing security awareness training was not being conducted throughout the Department. State security standards direct each state agency to conduct security awareness training at least annually with all employees.

The intent of this training is to ensure that all new and existing employees, consultants, and contractors are aware of their responsibilities in protecting the state's information systems and information processed through them. Agency staff indicated they had been working on such an IT security awareness training program but they had not yet implemented it. Management indicated that the Department was implementing a quarterly security awareness news letter to address this deficiency.

Servers Were Not Properly Protected

Six of the 26 (23%) network servers or server rooms we examined were not adequately protected. This included unrestricted access to equipment and one room with a leaky roof. The server room with a leaky roof had already resulted in water damaged computer equipment.

State security standards require network servers be installed in physically secure and environmentally sound facilities. Unrestricted physical access to network servers increases the risk of accidental damage, theft, or vandalism and could result in the release of confidential data or the loss of use of the computer network.

A Wireless Network Was Not Properly Secured

One division had an improperly secured wireless access point. The wireless access point could allow access to the state's network. This wireless access point was periodically used by non-state employees while visiting the Housing Division's office in Carson City.

Improperly secured wireless network configurations represent "backdoors" into an otherwise secure computer network. These backdoors can allow unauthorized access to state information technology resources and confidential data.

Discussions had occurred between DoIT staff and Housing Division staff regarding segregating this network on DoIT's isolated Guest Net. However, follow through did not occur and the wireless network was not connected to the isolated Guest

Net. The Housing Division indicated it has since corrected this issue by connecting the wireless access point to DoIT's Guest Net and has instructed staff to only turn on the device when it is necessary.

Web Servers Could Be Made More Secure

We identified three web servers whose configurations could be made more secure. Scans of these web servers revealed several vulnerabilities in their configurations. These included services which should be disabled to prevent attacks against the servers. These vulnerabilities could allow hackers to modify the web servers and cause them to malfunction or allow unauthorized disclosure of information. Staff indicated they had not previously conducted vulnerability scans on these web servers.

Recommendations

8. Implement a program to provide IT security awareness training at least annually for all employees.
9. Develop a plan to properly secure all servers in accordance with state security standards.
10. Coordinate with DoIT to ensure the wireless network grants access only to the Internet by isolating it on DoIT's Guest Net.
11. Disable unneeded services on web servers.

Appendices

Appendix A

Audit Methodology

To gain an understanding of the Department of Business and Industry, we interviewed Department management and staff. We reviewed legislation, committee minutes, and state and Department policies. We interviewed the Department's information technology staff to gain a broad understanding of the Department's network resources and how they are managed and utilized. We discussed how the Department interconnects and interacts with the Department of Information Technology, other state agencies, and third party service providers.

To ensure our audit tests were representative of the Department's statewide operations, we conducted tests at 26 of the Department's offices located throughout the state. During our audit, we examined adherence to the state's IT security standards as well as the Department's own IT security policies and procedures.

To determine if controls over desktop computer security were adequate, we tested a judgmental sample of 161 of the Department desktop computers to ensure they had the latest operating system updates as well as having current antivirus protection. In addition, these same computers' hard drives were examined to determine if they contained unencrypted confidential information. Computers selected were based on location throughout the State. We also examined the Department's network user accounts to determine if only current employees had access to the network. We then determined if the Department's computer network users with access to sensitive information had background investigations conducted and if they had signed security awareness statements.

To assess the security of the Department's network servers, we tested their security settings. Specifically, we tested to ensure they were configured to enforce state password standards for all accounts, that they had adequate virus protection and that software security updates were installed. We also examined the physical security

over the network servers at each of the 26 locations we visited. Web servers were scanned to identify any high-risk vulnerabilities.

In addition, we tested a wireless access point to determine if it was properly configured.

Finally, we identified and tested controls over sensitive data the Department collects to determine if access to the data was appropriately restricted.

Our audit work was conducted from March to October 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Director of the Department of Business and Industry. On November 1, 2010, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B which begins on page 17.

Contributors to this report included:

Jeff Rauh, CIA, CISA
Deputy Legislative Auditor

S. Douglas Peterson, CISA
Information Systems Audit Supervisor

Appendix B
Response from the Department of Business and Industry

Jim Gibbons
Governor

Dianne Cornwall
Director

STATE OF NEVADA



DEPARTMENT OF BUSINESS AND INDUSTRY
OFFICE OF THE DIRECTOR

November 12, 2010

Paul V. Townsend
Legislative Counsel Bureau
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Townsend:

Attached is the Department of Business and Industry's repose to the preliminary audit report on the Department's Information Technology Security (dated October 25, 2010).

Information technology security is vitally important to the Department, and to the constituents that we serve. The Department appreciates the Legislative Counsel Bureau's (LCB's) professional and thorough approach relative to this important issue and in the execution of the audit. The Department staff has been very pleased with LCB's clear and open communication throughout the course of the audit.

Overall the Department accepts all eleven of the recommendations in the report. The Department has already implemented of some of the recommendations while others will take time to be fully implement due to financial and technical constraints. The details are articulated in our response.

The Department of Business and Industry consists of a Director's Office and fourteen divisions with approximately thirty office locations. The Department contributes a significant amount of net revenue to the State of Nevada. In FY2010, the Department contributed approximately \$258 million to the state General Fund after operational expenses. Exhibit 1, below, summarizes the revenues and expenditures for the Department of Business and Industry and illustrates the fiscal importance of the department to the State.

Carson City: 901 South Stewart Street, Suite 1003 Carson City, Nevada 89701 Telephone (775) 684-2999 Fax (775) 684-2998


Las Vegas: 555 E. Washington Avenue, Suite 4900 Las Vegas, Nevada 89101 Telephone (702) 486-2750 Fax (702) 486-2758
www.biinfo.dbi.state.nv.us

Exhibit 1 – Estimated Revenue & Expenditures for FY2010

Revenue/Expenditure Items	Approx. Amount (\$ Millions)
Revenue (Primarily fees collected to support agency operations, plus revenues from Highway Fund and General Fund) *	\$125
Additional Revenues posted directly to the General Fund (includes direct agency fee receipts, insurance premium tax and insurance retaliatory tax)	\$258
Total Revenue	\$383
Less Authorized Expenditures for Operations	(\$125)
Net Contribution to State General Fund	<u>\$258</u>
<i>* Source: State budgeting system (NEBS)</i>	

If you have any questions or need additional information please contact Grant Reynolds directly at (775) 684-2994.

Sincerely,

By *Todd Riehl, Deputy Director* 

Dianne Cornwall

Carson City: 901 South Stewart Street, Suite 1003 Carson City, Nevada 89701 Telephone (775) 684-2999 Fax (775) 684-2998

Las Vegas: 555 E. Washington Avenue, Suite 4900 Las Vegas, Nevada 89101 Telephone (702) 486-2750 Fax (702) 486-2758
www.biinfo.dbi.state.nv.us

Department of Business and Industry’s Response to Audit Recommendations

Introduction

Department accepts all eleven of the recommendations in the audit report. The Department has already started implementing some of the recommendations while others will be phased in over time as the Department works under financial and technological constraints.

This document is organized as follows:

- Response to LCB’s Recommendations – Business and Industry’s response is documented for each of the eleven (11) recommendations
- Response to Recommendations (Summary Matrix) – One page Check list that summarizes which recommendations were accepted and which were rejected.

Response to LCB’s Recommendations

Recommendation #1: Discontinue collection of SSNs where not authorized by law.

The Department accepts this recommendation. The Department will work with each division to verify their legal authority to collect Social Security Numbers (SSNs). We will also determine if there is a valid business/program need to collect this information. In situations where it is not appropriate to collect SSNs we will:

- Discontinue the collection of SSN, and/or collect only the last four (4) digits of the SSN; and
- Purge SSNs that are currently stored in databases or in electronic documents.

Recommendation #2: Remove or mask the five leading digits of all existing SSNs in agency databases where possible.

The Department accepts this recommendation. The Department is implementing this solution where technically and fiscally feasible. We are in the process of implementing data masking in the Real Estate Division’s database system. In addition the Housing Division has removed the five leading digits of SSNs stored in one of their database systems. The Department will continue reviewing each division that has a need to collect and store SSNs in databases and either mask or truncate the SSN field where feasible.

Recommendation #3: Develop a plan to encrypt sensitive data as hardware and software upgrades make this capability available.

The Department accepts this recommendation; however, it will likely need to be phased in over time due to fiscal and technical constraints. The Department is evaluating two types of encryption technologies:

- Encrypt document files
- Encrypt database records

Encrypt document files

This involves encrypting document files, in formats such as Word, Excel, PDF, etc. These documents are typically stored on a desktop PC or shared file server. The Director’s Office is currently testing/piloting a data storage “appliance” which encrypts files. This appliance has a web interface and user access security (based on user profiles and credentials). Once we complete the evaluation of the appliance and it meets our business and security requirements we will roll it out for Department-wide use. We will host and manage the device from the B&I Director’s Office.

The Director’s Office will work with the individual agencies to move their sensitive information to the appliance. The Director’s Office will also work with the agencies to establish roles, polices and procedures related to managing sensitive data.

Encrypt Database Records

This involves encrypting database applications using encryption features available in the database software. The primary database software used in the Department is Oracle, SQL Server, and Access. Implementing database encryption will require upgrades and additional expenditures. The Department will assess the feasibility and cost/benefits of implementing database encryption for those systems that store sensitive data.

Summary of Encryption Options to be Evaluated

Format	Device	Protection Method
Documents (e.g. Word, Excel, etc.)	PCs & Shared File Servers	<ul style="list-style-type: none"> • Store sensitive documents on encrypted NAS appliance
Database records (e.g. SQL Server, Oracle)	Application Servers	<ul style="list-style-type: none"> • Mask SSNs on user screens • Encryption features in database software

Recommendation #4: Develop procedures to identify computers without current virus protection.

The Department accepts this recommendation. The Department will establish formal processes to ensure computers are running the current versions of virus protection software. This includes the following:

- Modify the Department’s server/network infrastructure to more effectively support centralized automatic virus software updates across all agencies (this includes evaluating features available in upgraded versions of Symantec’s server software)
- Establish business processes to validate that updates are being properly made (include the State MSA contractor, who provides periodic IT services to some divisions, as part of the process)
- Educate users, through security awareness training on how to check for virus protection software on their PCs and how to download updates

Recommendation #5: Develop a procedure to periodically check software update installations to detect failed or missing update installations.

The Department accepts this recommendation. The Department will establish a formal process to ensure software updates are being properly made to PCs and servers. This will be implemented similar to how the Department is addressing #4 above – through network/server infrastructure, formal business processes, and user education.

Recommendation #6: Follow state security standards by conducting quarterly reviews of user lists.

The Department accepts this recommendation. The Department will establish procedures to perform quarterly reviews of user lists to ensure former employee accounts are disabled. This includes user accounts for network access as well as access to business applications.

Recommendation #7: Conduct background investigations on employees with the greatest access to sensitive information or systems.

The Department accepts this recommendation; however, it will be phased in over time. The implementation of this recommendation may be impacted by advice from the Attorney General or Department of Personnel, and by fiscal constraints.

Department of Business & Industry – Response to Audit Recommendations

The Department will establish a policy that new hires will be subject to background checks if they are hired into positions that are considered “sensitive” as described in the State Information Security Standard 4.04, Personnel Security, sections 6A and 6B

The Department is currently assessing the feasibility of performing background investigations on existing IT staff that are in positions that are considered “sensitive”. Those individuals have been working for the state in those positions prior to the effective date of the State Information Security Standard 4.04, Personnel Security (10/03/2006).

The Department already requires background checks when hiring new division administrators and commissioners.

Recommendation #8: Implement a program to provide IT security awareness training at least annually for all employees

The Department accepts this recommendation. The Department is addressing ongoing security awareness for our 600+ employees using the following:

- Quarterly Security Awareness Bulletin – This bulletin, authored by the Directors office, contains relevant IT security information. It is emailed to all Department staff. The first issue was published in the spring of 2010.
- Department Intranet Site – The Director’s Office is adding security awareness content to the Department’s Intranet site to which all employees will have access.
- Security Alerts – Security alerts will be sent to employees on an as-needed basis.

Recommendation #9: Develop a plan to properly secure all servers in accordance with state security standards.

The Department accepts this recommendation. The Department will develop a plan to assess the security of all servers and implement appropriate physical security measures. The Department may encounter fiscal issues with securing servers for a couple of the agencies if there is a need to purchase additional equipment such as locking server cabinets.

Recommendation #10: Coordinate with DoIT to ensure the wireless network grants access only to the Internet by isolating it on DoIT’s Guest Net.

The Department accepts this recommendation. The Department will establish formal procedures to ensure that all future wireless networks within the Department are setup on DoIT’s Guest Net so they are isolated from Silvernet.

Recommendation #11: Disable unneeded services on web servers.

The Department accepts this recommendation. The Department will assess all the web servers that are exposed to the Internet and identify services that should be disabled to mitigate potential threats. The Department will implement the changes as appropriate.

Department of Business & Industry – Response to Audit Recommendations

**Department of Business and Industry
Response to Audit Recommendations**

Recommendation Number	Recommendation	Accepted	Rejected
1	Discontinue collection of SSNs where not authorized by law	X	
2	Remove or mask the five leading digits of all existing SSNs in agency databases where possible	X	
3	Develop a plan to encrypt sensitive data as hardware and software upgrades make this capability available	X	
4	Develop procedures to identify computers without current virus protection	X	
5	Develop a procedure to periodically check software update installations to detect failed or missing update installations	X	
6	Follow state security standards by conducting quarterly reviews of user lists	X	
7	Conduct background investigations on employees with the greatest access to sensitive information or systems	X	
8	Implement a program to provide IT security awareness training at least annually for all employees	X	
9	Develop a plan to properly secure all servers in accordance with state security standards	X	
10	Coordinate with DoIT to ensure the wireless network grants access only to the Internet by isolating it on DoIT's Guest Net	X	
11	Disable unneeded services on web servers	X	
TOTALS		11	0

Department of Business and Industry Response to Audit Recommendations

<u>Recommendation Number</u>		<u>Accepted</u>	<u>Rejected</u>
1	Discontinue collection of SSNs where not authorized by law	<u> X </u>	<u> </u>
2	Remove or mask the five leading digits of all existing SSNs in agency databases where possible	<u> X </u>	<u> </u>
3	Develop a plan to encrypt sensitive data as hardware and software upgrades make this capability available	<u> X </u>	<u> </u>
4	Develop procedures to identify computers without current virus protection.....	<u> X </u>	<u> </u>
5	Develop a procedure to periodically check software update installations to detect failed or missing update installations.....	<u> X </u>	<u> </u>
6	Follow state security standards by conducting quarterly reviews of user lists.....	<u> X </u>	<u> </u>
7	Conduct background investigations on employees with the greatest access to sensitive information or systems	<u> X </u>	<u> </u>
8	Implement a program to provide IT security awareness training at least annually for all employees	<u> X </u>	<u> </u>
9	Develop a plan to properly secure all servers in accordance with state security standards	<u> X </u>	<u> </u>
10	Coordinate with DoIT to ensure the wireless network grants access only to the Internet by isolating it on DoIT's Guest Net.....	<u> X </u>	<u> </u>
11	Disable unneeded services on web servers	<u> X </u>	<u> </u>
	TOTALS	<u> 11 </u>	<u> 0 </u>