Special Review

OFFICE OF THE STATE AUDITOR

Securing the Enterprise

Elizabeth M. Ready
Vermont State Auditor

Issued: February 19, 2002

To obtain additional copies of this report contact:

Elizabeth M. Ready
State Auditor

Office of the State Auditor
132 State Street
Montpelier, VT 05633-5101
(802) 828-2281
1-877-290-1400 (toll-free in Vermont)
auditor@sao.state.vt.us

This report is also available on our website:
www.state.vt.us/sao

Securing the Enterprise

State Auditor's High-Level Assessment of
Vermont's Information Technology Security & Data Recovery Policies

Table of Contents

Page

Executive Summary 3

Objective, Scope & Authority 4

Methodology 4

Findings and Recommendations 6

Implementation Strategy 11

Endnotes 11

Findings & Recommendations

Finding A: The State lacks proper security controls and data recovery policies 8

Finding B: Agencies & Departments lack disaster recovery plans 8

Finding C: Insufficient controls exist regarding user rights 8

Finding D: Insufficient controls exist regarding data back-up and program changes 9

Finding E: System servers are not adequately secure 10

Finding F: Databases used by some Departments do not have adequate security 10

Appendices

Appendix A: Agency of Administration's Response to Draft Review

Appendix B: Department of Motor Vehicles' Response to Draft Review

Executive Summary

Last year when some Vermont taxpayers logged on to the State's electronic tax filing system, they accessed the filings of other taxpayers – including confidential and personal data. This security breach is the old-fashioned kind – the result of human and technological error.

Since September 11, managers within state government have awakened to a new sense of risk. Not only must they prepare for traditional information technology (IT) disasters and glitches, but they must also anticipate perils that are planned and willfully carried out.

The State of Vermont has a number of security improvements on the drawing board, but currently lacks proper oversight and management to protect its IT assets. As a result, the State's investments in IT infrastructure may be at unnecessary risk of sabotage, loss, theft, or natural disaster.

We found:

- There is limited formal guidance or direction regarding the implementation and monitoring of prudent security and data recovery policies;
- Agencies and departments lack effective business continuity plans;
- System servers are not adequately secure; and,
- Critical systems are running on applications that offer inadequate security.

Vermont can best make progress by focusing on the basics. We recommend a three-pronged, interrelated approach:

- The Office of the Chief Information Officer (CIO) should monitor and enforce the implementation of statewide IT policies;
- Agencies and departments should implement these policies to ensure adequate business continuity plans, user name and password protocols, data back-up and server security requirements, and power back-up plans exist; and,
- The Office of the State Auditor should conduct external audits to assure compliance.

A New Mindset

The best private and public sector managers agree on one thing: No risk, no gain. But, understanding today's IT risks and communicating them to employees takes a new mindset and a new set of leadership skills.

Since September 11, many organizations have taken a big picture view of risk management, systematically evaluating enterprise-wide exposures.

For some, this means a Chief Risk Officer (CRO) who is responsible for assessing the system-wide potential for disaster. Instead of managing facilities, infrastructure, and information technology separately, the CRO looks at the entire organization from a holistic perspective. In Vermont, this function could be located within the Agency of Administration.

A High-Level Assessment of Vermont's Information Technology Security & Data Recovery Policies

Office of the State Auditor

Objective, Scope & Authority

The Office of the State Auditor has conducted a limited, high-level assessment to determine if Vermont has adequate policies and procedures in place to protect its information technology (IT) systems.

This assessment was conducted pursuant to the State Auditor's authority contained in 32 V.S.A. §§163 and 167, and was performed as part of the State Auditor's special review of how state and federal funds are spent on information technology across state government.

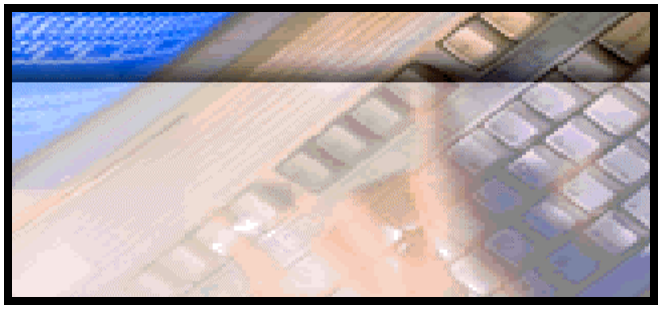
An assessment differs substantially from an audit conducted in accordance with applicable professional standards. The purpose of an audit is to express an opinion. Its purpose is to identify findings and observations and to make recommendations so that the reviewed agency or program can better accomplish its mission and more fully comply with laws, regulations, and grant requirements. An assessment relies upon representations of, and information provided by, a variety of state employees. If an audit had been performed, the findings and recommendations might or might not have differed.

Methodology

The methodology involved a review of relevant statutes, regulations, policies, contracts, internal memoranda, and correspondence. It included interviews with numerous state employees involved in IT project development and management.

We also reviewed the State's security policies developed by the Information Resource Management Advisory Committee (IRMAC). Throughout this assessment, KPMG's Risk and Advisory Services Practice provided advice and counsel. They also participated in interviews, on-site security tests and fact-finding.

We assessed the State's IT security risk by performing security reviews at the Department of Motor Vehicles, the Department of Prevention, Assistance, Transition and Health Access, and the Office of the State Treasurer.



Introduction

Vermont's IT leaders are aware that Vermont faces system-wide security risks, and they have begun to address the problems. We applaud their efforts and encourage them to forge ahead.

Currently, the State has security policies on data back-up, access and intrusion, but they are one-page documents that provide little more than statements and statutory references. To date, the Chief Information Officer (CIO), the Information Resource Management Advisory Committee (IRMAC), and the Division of Communications Information Technology (CIT) have yet to provide proper guidance or direction regarding the implementation and monitoring of prudent security and data recovery policies.

The State has taken a good first step by setting in place the Vermont Computer Security Incident Response Team (VCSIRT), which was created by IRMAC's Security Intrusion Policy. VCSIRT provides a central coordination center and single point of contact for computer security issues, such as virus and worm incidents or hacker intrusions.

The overall goal of VCSIRT, according to IRMAC's policy statement, is to ensure, provide and create a "safe and secure technical environment for the purpose of conducting government business." This is a laudable goal. The policy continues to say, "VCSIRT will achieve this goal by providing:

- Single point of contact for security issues and guidance
- Acoordinated response among system administrators, investigators and law-enforcement to a reported incident
- Liaison to other CSIRT in both the private and public sectors
- Coordination of services which improve security and minimize the threat of damage from intrusions
- Performing periodic network vulnerability assessments
- Distribution of information to all staff that recognizes that prevention, and not simply detection, is key to thwarting attackers"[1]

Three Steps to Security

Vermont can best make progress by focusing on the basics. We recommend a three-pronged, interrelated approach.

One: Office of the CIO

The Office of the Chief Information Officer should provide statewide direction, policies, guidelines and monitoring to ensure each department has adequate IT security.

Two: Agencies & Departments

Agencies and departments should develop and test disaster recovery plans that are communicated to all personnel and tested periodically. They should also be given the direction and resources to:

- Implement protocols related to passwords, data back-up and program changes;
- Assess server security, power back-up and the risks of not making changes; and,
- Examine the cost/benefit of moving critical applications from MS-Access to more secure server platforms.

Three: The State Auditor

The Office of the State Auditor should be given adequate resources to conduct external security audits to determine whether:

- disaster recovery plans are current and have been tested;
- access controls are adequate;
- processing controls are appropriate; and,
- department policies are adequate and properly implemented.

VCSIRT consists of state employees with other major responsibilities, and has not been provided the resources necessary to meet its goal to provide a "safe and secure technical environment." VCSIRT is comprised of a member from GovNet, the Deputy CIO, the Director of CIT and two departmental representatives.

In recent correspondence with our Office, Bob West, the Deputy CIO, informed our Office that VCSIRT is developing a website to help departments understand the state's security procedures regarding viruses and worms as well as hacker and social and physical incidents related to IT and IT infrastructure. As part of this website endeavor, VCSIRT will make it easier for people to receive security alerts by e-mail. Subscribers will also be notified of other general contact addresses, such as how to: report problems; ask general questions about improving security; and, receive sample policies.

While certainly a step in the right direction, this approach fails to bring a strong, uniform method of securing the State's IT infrastructure. VCSIRT has created is an outline of existing state procedures as a guideline for departments to follow, but offers no strict guidance about how to develop, adopt or test security plans. This effort is further hampered by a failure of the State to either monitor departments'security plans, or adopt an enterprise-wide security policy standard.

This website makes evident that IT security is a concern of the state, although a lack of existing funding precludes further progress. The CIO told this Office that a statewide security audit would be her first priority if she had additional resources.[2]

Findings & Recommendations

During our Office's special review of state and federal funds spent on IT, we conducted a limited, high-level security assessment to determine if the State had adequate polices and procedures in place to protect its IT assets.

This assessment does not equate to a full-scale, statewide security audit of the State's IT network, which we do recommend. However, the assessment did uncover several areas of concerns that refer back to our general concerns about Vermont's policies and procedures regarding the planning, management and implementation of IT infrastructure: There is little oversight and no guidance.

While the State has some policies in place, and is working on other ways to protect the State's IT system, the CIO offers no direction to implement these protective policies. Where there is mandatory adoption of policy, there is no post-implementation monitoring. Policies alone are not enough.

This assessment is best used as a companion to other IT reports issued by our Office. Addressing security problems without addressing other recommendations will not solve the State's larger IT problems.

What's Changed

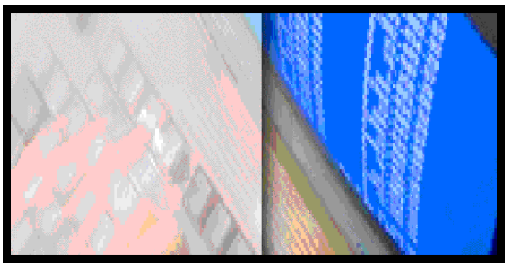
> The perception of IT risk has shifted radically from perils that arise from disasters and glitches to damage that is planned and willful.

> Managers must now take an enterprise-wide, rather than piecemeal, approach to IT safeguards.

> There is renewed emphasis on basic security measures like policies, locks, IDs, firewalls and anti-virus software.

> Organizations are identifying senior managers responsible for assuring and planning for system-wide risk.

How States Are Improving IT Security



The events of September 11, 2001 have provided laser-like focus on the issue of IT security. Many states, however, recognized the need to address cyber security years ago.

The Texas Department of Information Resources released a statewide IT security assessment conducted by Sprint E/Solutions more than a year ago. The report found that "security training and security awareness [was] generally inadequate in many State agencies."[3] Texas' statewide IT planning manager noted, "[W]e had an idea that security probably wasn't as robust in the state as we move services online. What was evident is that either agencies have policies that are not being enforced, are not being followed for the most part, or there were no policies."[4]

The Texas Legislature approved funding for an Office of Information Security within its Department of Information Resources in response to these findings. The role of the office is to apply policies and monitor the state's Internet architecture. The office already has sample templates for a variety of security policies including passwords, portable computing and vendor access. Its web site offers a clearinghouse of information on security and business continuity as well as emergency alerts and training opportunities. In addition to the resources available at the IT office, the Texas State Auditor provides an Automation Controls Self-Assessment Guide on their web site that can help departments assess the status of their computer operations control environment.[5]

Pennsylvania's Governor announced an initiative to strengthen security and privacy policies - PA Secure Online - in October 2001. The plan, which was in development prior to September 11, includes creating a cyber-academy to help educate state employees about detecting threats, hiring an ombudsman to oversee compliance and amending criminal codes to better address cybercrime.[6]

Iowa, California, Utah and Kansas have also established enterprise-wide policies and dedicated personnel to create, oversee and test security policies and measures.

Iowa conducted a study of its security systems three years before Texas' study. The state's Security Officer noted, "[T]he reason why nobody knew about us was because the study itself contained specific vulnerabilities and had issues concerning each one of the agencies, and because of that it needed to be confidential."[7]

System-vulnerability testing is done in many states, but only North Carolina and Rhode Island have enacted legislation classifying the reports generated from security testing. Legislators in Rhode Island faced protests from the American Civil Liberties Union, but the auditor general's office, which was given the authority to do the vulnerability testing, prevailed. Auditor General Ernest Almonte comments, "If we made them public, it would be a roadmap for a hacker to get into systems."[8]

>|<

Finding A
Vermont lacks proper security controls and data recovery policies to protect against unauthorized access, use and dissemination of information.

Our security assessment of three departments found that Vermont offers specific guidelines concerning security policy in regard to viruses or worms, but offers no such specifics regarding access and protection, security intrusion and back-up.

Departments have been told to develop a security plan, but neither the CIO nor IRMAC has suggested content requirements or provided any measurable oversight. In each department where we conducted an assessment, the risk analysis questions we asked triggered more comprehensive thinking about potential vulnerabilities, including access to networks, internal threats and the adequacy of back-up procedures.

Recommendation A
The CIO, in cooperation with IRMAC and CIT, should develop enterprise-wide protocols and policies related to data recovery, protection from unauthorized access, physical security and the use and dissemination of information.

Finding B
Agencies and departments lack business continuity (or disaster recovery) plans.

Most departments and agencies have business contingency, or disaster recovery, plans for Y2K, but they have not been updated since 1999. Most were Y2K plans, which were incomplete and/or inadequate at the time. As a result, many plans fail to address the needs of current information systems and applications.

These plans assume a disruption that lasts no more than 30 days. Most assume a loss of power and systems, but not a loss of facilities. The events of September 11, 2001 suggest the need for more comprehensive disaster recovery plans that address longer disruption periods, loss of all facilities and the potential loss of key employees.

Recommendation B
The CIO, in cooperation with IRMAC and CIT, should direct agencies to perform a business impact analysis and develop business continuity (or disaster recovery) plans that are well communicated to all personnel and tested periodically. The CIO should provide guidance regarding what should be addressed in these plans.

Finding C
The State has insufficient controls regarding user rights.

Protocols regarding the issuance, changing and revocation of user names and passwords for access to agency networks and critical applications vary widely. In some departments, user protocols do not exist. This places the State at unnecessary risk of cyber-sabotage.

For example, in one department an employee left state government and still had access critical systems for up to 30 days.

The best private and public sector managers agree on one thing: No risk, no gain. Understanding today's IT risks, however, takes a new mindset and a new set of leadership skills.

Security experts repeatedly warn that insiders are the major threat to sensitive data and applications. Stronger password protocols, consistent enforcement and regular audits of user rights protocols are needed. As one of the State's network administrators quotes in his e-mail signature, "Passwords are like underwear. You don't share them, you don't hang them on your monitor, or under your keyboard, you don't email them, or put them on a web site, and you must change them very often."[9]

Recommendation C
The CIO, in cooperation with IRMAC and CIT, should develop enterprise-wide protocols and policies for the issuance, changing and revoking of user rights.

Finding D
The State has insufficient controls regarding data back-up and program changes.

While most departments have data back-up procedures for critical applications, there is limited logging or testing of the performance of these procedures. Back-up data sets are often stored in close proximity to the original data.

Back-up policies relating to user data and documents vary by department, if they exist at all. Some departments require users to save their data to network locations, which are backed up regularly, while others simply trust the back-up habits of the user. Where policies do exist, users are not audited to test conformance.

Program changes in critical applications are also not adequately controlled. Logs of changes are kept, but they are not audited against authorized change requests. There are no controls to detect unauthorized changes.

When data is not adequately, or safely, backed up and stored it puts this information at risk of being tampered with by unauthorized users. Or, in the event of a sudden power loss or catastrophe, this data could be lost.

Recommendation D
The CIO, in cooperation with IRMAC and CIT, should develop enterprise-wide protocols and policies for backing up systems and storing back-up data, as well as a program change policy that includes reviews for unauthorized program changes.

Finding E
Systems servers, which are the computers that departments use to store data and software applications, are not adequately secure.

System servers, which are today's mainframe computers, are often located in unsecured areas, with inadequate (and even dangerous) fire prevention systems, poor temperature controls and insufficient protection from static electricity dangers and floods.

For example, in one agency location, there was a sprinkler system (non-halogen) in a server room that is set to go off in case of a fire in other rooms of the building. In other departments, the server is only as secure as the entire building.

Some agencies lack the necessary precautions to ensure data integrity in the event of a power or server failure. While most servers do have some type of uninterrupted power supply back-up device, many departments do not have the technology needed to recognize a power failure and begin orderly shutdown procedures. While some of these deficiencies are due to informal cost/benefit assessments, there is a need for enterprise-wide protocols and some degree of oversight.

An unscrupulous individual could walk into a building that lacks a secure server and damage hardware and/or data stored on that server. Consequently, applications that run the department's basic programs, including e-mail and word processing, could be compromised. Departments with client or customer records are generally more secure from inadvertent intrusion, but could still be severely impaired in the event of a fire, flood or other catastrophe.

Recommendation E
The CIO, in cooperation with IRMAC and CIT, should develop enterprise-wide protocols and policies for securing and protecting all critical system servers.

Finding F
Databases that are critical to providing quality customer service, in some departments, do not have adequate security.

We visited three departments during our security assessment to determine if adequate procedures and policies were in place. One key area is the security of applications that run crucial department functions.

We found that one department ran a number of critical applications as Microsoft Access databases. Although it is a cost-effective platform, Microsoft Access lacks the full suite of user rights tools, data protection, tracking, and auditing of data changes offered in more advanced database platforms. This means that a user could easily change, or delete, crucial data in the department's applications.

We did not review or survey all departments to determine how many are using Microsoft Access to run critical applications.

Recommendation F
Agencies should examine the cost benefits of moving critical applications from MS-Access to a more scalable and secure platform such as SQL or Oracle.

Implementation Strategy

We hope these recommendations will help to protect and preserve the State's IT infrastructure. To fully succeed, the Office of the CIO should adopt an implementation strategy, and the Legislature should fund it. The following details an integrated approach to protect the State's IT assets.

First, the Office of the CIO should provide statewide direction, policies, guidance and monitoring as detailed above.

Second, agencies and departments should be given the direction and resources to:

- Develop and test disaster recovery plans that are communicated to all personnel and tested periodically. Test results should be used to ensure continuous improvement of the plan;
- Implement the protocols related to passwords, data back-up and program changes;
- Conduct periodic assessments regarding server security, power back-up and the risk of not addressing known deficiencies; and,
- Examine the cost/benefit of moving critical applications from MS-Access to a more scalable and secure server platform such as SQL or Oracle.

Finally, the Office of the State Auditor should be given resources to conduct external security audits to determine:

- Whether disaster recovery plans are current and have been tested;
- Whether access controls are adequate;
- Whether processing controls are appropriate; and,
- Whether department policies are adequate and properly implemented.

The Legislature should consider whether information from these security audits are exempt from public records disclosure.

Endnotes

1 "Security Intrusion Policy" adopted by the Information Resource Management Advisory Council. Effective date: March 17, 2000.

2 Interview with Patricia A. Urban, Chief Information Officer, by Nancy Wasserman, Chief, Special Audits and Reviews and Andrew Gottschalk, Senior Manager, KPMG, October 22, 2001.

3 Available online at http://www.dir.state.tx.us/IRAPC/security_assessment/html/DIR.SSA.FinalReport.htm

4 Sarkar, Dibya, "Texas Setting up Security Office," Civic.com, June 5, 2001.

5 http://www.dir.state.tx.us/security/index.html

6 Sarkar, Dibya, "Pa. Strengthens Cybersecurity," *Government E-business*, October 22, 2001.

7 Sarkar, Dibya, "Security in Numbers," Civic.com, August 6, 2001.

8 Perlman, Ellen, "Staying Ahead of Hackers," *Governing*, January 2002.

9 Attributed to Kurth Bemis, used by Bennet Deliduka, Network Administrator at CIT.

Appendix A

RESPONSE TO DRAFT COPY OF AUDITOR OF ACCOUNT'S REPORT
ON
Security & Data Recovery Policies
AS OF JANUARY 29, 2002

Prepared by the Agency of Administration
February 4, 2002

Findings:

- "There is no formal guidance or direction regarding the implementation and monitoring of prudent security and data recovery policies;
- Agencies and departments lack business continuity plans;
- System servers are not adequately secure;
- and, critical systems are running on applications that offer inadequate security."

Response: As you mentioned in your report we have taken an important step by putting in place the Computer Security Incident Response Team (CSIRT), which was created by IRMAC's Security Intrusion Policy. Additional resources are necessary to continue the expansion of effort in this area. Additional information about CSIRT can be found at http://www.bgs.state.vt.us/csirt. Although this effort is very important to our goal of a "safe and secure technical environment" it only provides one piece of the solution when creating an enterprise wide security policy.

As you know, the Governor created a Vermont Terrorism Task Force on 10/19/2001 with executive order #01-10. Although the task force's main charter is the coordinated response to the threat of terrorism, the critical need for Information Technology and the threat of that technology under terrorist attack could deter our response efforts and result in loss of revenue. The Department of Public Safety, Emergency Management Division in Waterbury is currently working on disaster contingency plans statewide. The Director of EMD, Ed Von Turkovich, sent a memo dated November 8, 2001 that asks all state agencies to update their disaster planning and provide that information upon completion. The memo also provides support documents to assist in the planning process. This too is another piece of the solution when planning for enterprise-wide security.

The Agency of Administration, Department of Buildings and General Services has recently hired a security staff focusing entirely on managing the physical security of all state buildings. The CIT division is working closely with the Office of the CIO to locate or build a facility to be used as a hot site for disaster recovery for any and all critical applications. The goal of this initiative would be to have a facility that any department could use in a disaster for continued operation as well as a facility to provide for the testing of business continuity or disaster recovery plans.

A third piece of the solution is the collaborative effort of the Office of the CIO, in cooperation with IRMAC, in working together to enhance and adopt, new policy that fosters our goal of a "safe and secure technical environment".

Because of the events of September 11, 2001, the importance of security, long neglected as a priority for enterprises, has now risen to the top of the priority queue. That event has been the wakeup call for government and industries that operate the interconnected networks and systems that comprise the global information infrastructure. It is important to recognize that the security solution is not an isolated activity for each individual enterprise. We are all interconnected by computers and networks in the global infrastructure and we are only as secure as the weakest link. We all face new security challenges in the information technology community, and need to work together to identify technology solutions, as well as the resources necessary to meet these challenges.

The success of any enterprise wide security policy is the collaborative effort of all agencies and the coordination and communications to support all levels of government. We hope to work with your office as we continue to work with all agencies to create and enhance guidelines for the future.

Recommendation 1: "The Office of the Chief Information Officer should improve guidance and policy development by providing statewide direction on key security issues including business continuity plans, user names and passwords, data backup requirements, security server requirements, and power back-up plans".

Response: We have adopted policies in this area. The following policies have been created by IRMAC specifically addressing data backup, user names and passwords:

POLICY TITLE: ***Access and Protection***

POLICY STATEMENT:

Each agency and office shall utilize risk management analysis and standardized password management techniques to control access to and provide protection for state records, information and facilities.

PURPOSE/STATEMENT:

The intention of this policy is to ensure that public records, information and facilities are protected while allowing controlled access. The use of risk management analysis identifies the appropriate amount of time, money, and effort that is to be spent with each category of record, information and facility. The secondary intention of this policy is to facilitate management efficiencies by ensuring that minimum resources (time, money, personnel) necessary are expended to secure and control access to public records, information and facilities.

POLICY TITLE: ***Security Backup***

POLICY STATEMENT:

Each agency and office shall utilize risk management analysis to identify the backup frequency and type of media necessary to provide adequate protection for state records and information. Security backups, along with system and application documentation, shall be stored in a secured and environmentally stable offsite. Backups, as appropriate, shall be monitored to assure data integrity, media stability, and systems and application compatibility.

PURPOSE/COMMENT:

The intention of this policy is to ensure that public records and information are protected from natural, accidental and intentional hazards. The use of risk management analysis identifies the appropriate backup frequency and type of media (i.e., the amount of time, money and effort) that is to be spent with each record and information category. The secondary intention of this policy is to facilitate management efficiencies by ensuring that minimum resources (time, money, personnel) necessary to protect the operational, legal and evidential value of the records and information and also provide for disaster recovery are expended.

In addition, the Office of the CIO is working closely with CIT to find a facility that would be suitable for a

disaster recovery site for any and all critical systems. The addition of this facility would help us to further define department business continuity plans and provide adequate testing of these plans. We will continue to work with IRMAC to enhance or adopt new policies that further define security & data recovery policies.

Recommendation 2: "Agencies and departments should implement these policies throughout State government".

Response: *Adoption of these policies is mandatory for all agencies and departments within the executive branch*.

Finding A: "Vermont lacks proper security controls and data recovery policies to protect against unauthorized access, use and dissemination of information".

Response: *Although IT security is a moving target, agencies and departments have made significant improvements in the overall security of their systems in the last year. Firewalls are being installed at the department level to supplement the perimeter security which exists at the enterprise level. This allows the department to control access to its own information and protects that information from non-approved access by other agencies and departments statewide. Firewalls now exist in the Treasurer's Office, Legislative branch, Department of Mental Health Services and Public Safety. We are currently working with the Department of Taxes, Attorney General's Office and the Judicial branch to install department level firewalls. This is a trend that will continue and has our overwhelming support. We will continue to work closely with departments to enhance security.*

In addition, the LDAP / Meta-Directory Task Force was formed by Office of the CIO in October 2000. The Task Force initially explored the possibility of creating a single enterprise directory or repository of data. The LDAP repository would have required everyone to use the same schema (data elements and attributes) or directory structure. We quickly realized this might not be a practical approach due to the many disparate systems in state government. The Task Force, after considerable study, and presentations, recommends that the State of Vermont establish a Meta-Directory infrastructure. Three of the main business issues that are driving the requirement for directory services at the core of the enterprise infrastructure are:
• User Administration: The management of people-based information inside a company as well as across the enterprise, forming the foundation for administering roles, relationships and deploying self-service systems.
• Application Security Management: The need for a common security infrastructure for Web-based (and potentially other) applications provided to the entire enterprise.
• Systems Security Management: The central provisioning of the user authorizations across all existing IT systems such as access to local area networks, mainframe hosts, applications and email systems.

We are currently working with a vendor to provide us with a Meta-Directory and Single Sign-on requirements assessment report for the Criminal Justice Integration System (CJIS) stakeholders. The recommended design from this engagement will provide the foundation to implement a directory solution across the enterprise. Some common goals for an enterprise solution are:
° A single, enterprise wide security and authentication model for all file, application, and print services regardless of user, service and/or device location.
° A single, enterprise wide repository for representing users, technology, and the rules that govern their interaction.

We will continue to work with IRMAC to enhance or adopt new policies that further define security & data recovery policies.

Recommendation A: "The CIO, in cooperation with IRMAC and CIT, should develop a enterprise-wide protocols and policies related to data recovery, protection from unauthorized access, physical security and the use and dissemination of information".

Response: *As already stated, we have policies in place that address your concerns with the exception of physical security, which is being addressed by the Department of Buildings and General Services. BGS is in the process of hiring security personnel to manage the security infrastructure for all state buildings.*

Finding B: "Agencies and departments lack business continuity (or disaster recovery) plans".

Response: *Agencies and departments created 246 business continuity or disaster recovery plans as a result of the Y2K effort. Although these plans addressed a variety of conditions that were envisioned "worst case scenarios" if systems failed because of Y2Kproblems, they provided the basic responses to ensure business continuity and disaster recovery. These plans should be updated, and as a member of the Terrorism Task Force I will suggest updating these plans.*

Recommendation B: "The CIO, in cooperation with IRMAC and CIT, should direct agencies to perform a business impact analysis and develop business continuity (or disaster recovery) plans that are well communicated to all personnel and tested periodically. The CIO should provide guidance regarding what should be addressed in these plans".

Response: *The CIO has provided guidance to departments and assisted in the development of business continuity planning, as a result of the Y2K project. As already stated, we are working with CIT to find a facility that would be suitable for a disaster recovery site for any and all critical systems. The addition of this facility would help us to further define department business continuity plans and provide adequate testing of these plans.*

The Agency of Administration has also partnered with Department of Public Safety, Emergency Management Division in Waterbury to work on disaster contingency plans statewide. The EMD staff has requested that every department update their disaster planning and provide that information upon completion.

Finding C: "The State has insufficient controls regarding user rights".

Response: *Our goal is to implement an enterprise-wide directory service to enhance our security and improve efficiency of user management. As stated above, we are currently working with a vendor to provide us with a Meta-Directory and Single Sign-on requirements assessment report for the Criminal Justice Integration System (CJIS) stakeholders. The recommended design from this engagement will provide the foundation to implement a directory solution across the enterprise. Some common goals for an enterprise solution are:*

° *A single, enterprise wide security and authentication model for all file, application, and print services*

regardless of user, service and/or device location.
° A single, enterprise wide repository for representing users, technology, and the rules that govern their interaction.

Recommendation C: "The CIO, in cooperation with IRMAC and CIT, should develop a enterprise-wide protocols and policies for the issuance, changing and revoking of user rights".

Response: *These policies will be developed or modified with the implementation of the enterprise directory.*

Finding D: "The State has insufficient controls regarding data backup and program changes".

Response: *Departments are responsible for the backup and offsite storage of critical applications . The Office of the CIO will continue, via published standards for security and disaster recovery, to work with agencies in this area and to follow up on implementation progress.*

Recommendation D: "The CIO, in cooperation with IRMAC and CIT, should develop a enterprise-wide protocols and policies for backing up systems and storing backup data, as well as a program change policy that includes reviews for unauthorized program changes".

Response: *The CIO, in cooperation with IRMAC, has created policy for the backup and offsite storage of critical data. We will work with all parties concerned to enhance our existing policy. The Office of the CIO can monitor implementation schedules but review of "unauthorized program changes" for all agencies and departments would require additional resources in the form of software and positions. In a decentralized I.T. environment, this recommendation can only be fully implemented on an individual agency basis. Developing a program change policy that includes reviews of any unauthorized program changes would depend on the systems and application support software being used. An enterprise-wide policy would not include enough information to adequately address all the change requests that could occur at an application level, due to the complexity and disparity of the development environments in state government. Change control needs to be documented at the department level.*

Finding E: "Systems servers, which are the computers that departments use to store data and software applications, are not adequately secure".

Response: *Many of the state's critical systems are stored in a secure climate controlled environment. In some cases, small departmental servers are housed next to the departmental staff for convenience and cost reduction. Physical security of state buildings will be the responsibility of BGS and is being addressed as stated earlier.*

Recommendation E: "The CIO, in cooperation with IRMAC and CIT, should develop a enterprise-wide protocols and policies for securing and protecting all critical system servers".

Response: *We concur that addition policy is needed to provide adequate protection of physical security. BGS has already started working on improvements in this area by hiring security personnel to create*

policy and administer building security. The policies that are developed by BGS will be in cooperation with the CIO, and IRMAC.

Finding F: "Databases that are critical to providing quality customer service, in some departments, do not have adequate security".

Response: *We concur and have always recommended Oracle as the platform for critical databases. Oracle is the state standard for many reasons, some of which are based on security requirements and our ability to provide cross-agency support in the event of a failure.*

Recommendation F: "Agencies should examine the cost benefits of moving critical applications from MS-Access to a more scalable and secure platform such as SQL or Oracle".

Response: *We fully concur with this recommendation. Oracle is the state standard as indicated in the response to Finding "F". Standards have been adopted that address the platform of choice when considering a database solution. I believe, had your survey been somewhat broader, you would have found that Oracle and SQL are the platforms being used for nearly all critical applications. Below is a copy of the State's database standard.*

POLICY TITLE: ***Relational Database Standard***

POLICY STATEMENT:

1) The acquisition and migration to the Oracle relational data base is encouraged when departments are seeking to acquire, replace and/or upgrade database platforms with the purpose or potential of supporting mission critical applications on which government is dependent for its business operations or for service delivery to citizens.

2) Agencies which implement statewide applications, such as the Human Resources Management System and the Financial Management Information System, will take the standard relational database platform into consideration when making decisions on application systems.

PURPOSE/COMMENT:

The intention of this policy is to provide a standardized platform for state government applications such that: (1) state business and service applications can be implemented in an environment which maximizes potential for system interfaces and interoperability; (2) agencies can make cost-effective investments in software applications with the knowledge and assurance that other applications will utilize the same platform.

Appendix B

STATE OF VERMONT
AGENCY OF TRANSPORTATION
DEPARTMENT OF MOTOR VEHICLES
120 State Street, Montpelier, Vermont 05603-0001

4 February 2002

Elizabeth M. Ready
State Auditor
132 State Street
Montpelier VT 05633-5101

FEB 6 2002

Dear Ms. Ready:

Thank you for the opportunity to review the draft of the State Auditor's special review of the State's policies and procedures relating to the security of its information technology systems. Department personnel reviewed the findings and overall do not dispute them. We agree that statewide policies and guidance would be extremely helpful in furthering the security of our systems. We do have confidence in the security of our access databases but will be glad to make a further analysis if it should be required.

The one concern that we have is that there will be a substantial amount of work on the department level if all of the recommendations are followed through. It would be helpful to have the Implementation Strategy expanded to include the allocation of resources to the departments as well as to the Office of the State Auditor to assist in implementation of the new policies and protocols.

Very truly yours,

Bonnie L. Rutledge
Commissioner

BLR/eb