The Road Beyond Risk

Recommendations to Safeguard the Security of Vermont's Financial and Human Resources Information Systems

Issue Date: April 4, 2003
Elizabeth M. Ready, State Auditor

Mission Statement

The mission of the State Auditor's Office is to be a catalyst for good government by promoting reliable and accurate financial reporting as well as economy, efficiency and effectiveness in State government.

The Road Beyond Risk

Recommendations to Safeguard the Security of Vermont's Financial and Human Resources Information Systems

Table of Contents

Appendices

EXECUTIVE SUMMARY

This high-level review was completed as part of our Office's annual audit of the State's financial systems. It is offered to the new managers in the Douglas Administration as a resource to help them identify and resolve security issues in Vermont's financial and human resource information systems.

In May 2002, this Office easily gained unauthorized access to nearly all units of the State's enterprise-wide accounting system, VISION. This demonstrated that a would-be hacker could have entered, changed and approved payments from virtually every department in government.

Today, the system software still does not prompt or require mandatory password changes on a regular basis. Many key State departments continue to run software without formal or documented security policies and procedures.

These problems point to the need for Vermont to take a serious look at how it designs systems like VISION, and how it secures them once they become operational.

Vermont has rapidly increased its reliance on information technology (I.T.) systems. Taxpayer investments in these assets neared $70 million in Fiscal Year 2002.

With this reliance comes a responsibility to ensure that appropriate security measures are in place to protect these assets from theft, sabotage or natural disaster.

This report is part of our Office's ongoing efforts to improve the overall security of Vermont's I.T. systems. In this report, we focus on Vermont's two major statewide software systems – HRMS and VISION.

HRMS (Human Resources Management System) is managed by the Department of Personnel. The system tracks all payroll information of state employees including the distribution of overtime, benefits and other contract-related items. HRMS cost taxpayers more than $4 million to develop and put in place in the early 1990s.

VISION (Vermont Integrated Solution for Information and Organizational Needs) is managed by the Department of Finance and Management. This PeopleSoft product is the chief accounting software to officially record all financial transactions made by the State's 62 business units. VISION took several years to plan, design and implement at a cost to taxpayers of nearly $20 million before it went live on July 1, 2001.

Our Office, along with KPMG's Risk Advisory Services, identified a number of high-level risks to these systems. We found:

- Neither financial system is designed to mandate password changes on a regular basis. Departments currently only issue memos and send out e-mails informing users that they have to change their passwords; and,

- The departments in charge of these systems use them without written, formal security policies and procedures to protect the integrity of the information.

THREE STEPS TO BETTER IT SECURITY

This report builds on this Office's past assessments of I.T. security. In *Securing the Enterprise*, a special report our Office issued on February 19, 2002, we found:

- There is limited formal written 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. In *Securing the Enterprise* we recommended a three-pronged, interrelated approach:

- The Office of the Chief Information Officer (CIO) should monitor and enforce the implementation of statewide I.T. 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 be provided adequate resources to conduct external audits to assure compliance.

DETAILED OBSERVATIONS - HIGH RISK

Observation

Neither HRMS nor VISION is currently configured to mandate password changes on a regular basis. A further investigation revealed that the applications could not track or monitor when or how often passwords are changed.

In early May 2002, the Office of the State Auditor found it could gain easy access to key VISION user accounts in almost all business units tested – including the Executive Office. A person with basic knowledge of VISION could have entered, changed, approved and budget-checked vouchers for payments. The Office alerted the Department immediately, and it took corrective action. (*See Appendix B*).

When VISION was first implemented, the Department of Finance and Management gave users accounts in which their default password was their state identification number. This information was widely disseminated, and allowed this serious breach to occur.

Management has since reset password defaults and reminds users to change them regularly. Current Finance and Management Commissioner Rob Hofmann told our Office, on March 11, 2003, that a planned upgrade to VISION in Fiscal Year 2004 would mandate password changes.

There is also no written comprehensive I.T. security policy and procedure manual for the Department of Finance and Management and the Department of Personnel with respect to VISION and HRMS. Additionally, the Office of the CIO does not monitor the development of these policies and procedures.

Recommendation

Forced password change is not currently an option in the PeopleSoft versions of either HRMS or VISION. However, Vermont could try one of the following approaches:

- Create a procedure to take a picture of the PeopleSoft encrypted password table on a prescribed basis and then compare the picture to the same table at a different point in time. A simple analysis of the two data files can reveal if passwords are being changed as mandated. This cost-effective approach can be done using a simple MS Access Database.*

- Force password change at the network server login and/or at the Citrix server login stage. Additional functionality may be required and examined for cost effectiveness.

- Purchase third-party software that works in conjunction with PeopleSoft to force application password change.

** The first option noted above is not only a short-term fix. Many organizations with the same password change limitations have used it as a long-term solution. One software package that is commercially available is PentaSafe's VigilEnt Password Manager for Oracle, which enforces and automates compliance with security policies, including forced password changes.*

DETAILED OBSERVATIONS - HIGH RISK

Observation

On June 1, 2001 the Office of the State Auditor issued a special review of the implementation of the VISION accounting software system. The Office recommended that the Agency of Administration implement security policies and procedures for VISION. On July 17, 2001, Andersen's Technology Risk Consulting issued a PeopleSoft logical security review report reiterating this need.

The State currently has some documents that relate to various security procedures. However, there is no comprehensive, written manual for statewide security policies and procedures. The Office of the CIO is developing a statewide policy to address these issues, according to Department personnel.

Recommendation

A formal statewide information security policy should be finalized as soon as possible and issued to all State agencies/departments.

Furthermore, compliance with the policy should be monitored frequently and a formal audit plan to ensure compliance should be introduced. We also recommend a complete system and integration controls (SIC) review be conducted for VISION, and possibly HRMS.

DETAILED OBSERVATIONS - HIGH RISK

Observation

Despite a newly-installed card access system at a critical building that houses computer operations, there are no written comprehensive policies and procedures to bar unauthorized personnel access to critical computer networking areas and potenially sabotage either HRMS or VISION. Staff indicated that such a written policy is more than halfway completed.

The card access system works as follows, according to the Department of Finance and Management: Upon recommendation from an Appointing Authority and approval of the Director of Communications & Information Technology a badge is issued to authorized personnel to gain access to the computer operations area. There are two access points to the area during the day and three access points during the off hours. This information is on the security system and backed up and stored by Security. All non-badge visitors must sign in, state the purpose of their visit and be escorted while in the facility.

Recommendation

Both departments should immediately complete formal written physical access policies and procedures manuals, and implement procedures to achieve compliance.

DETAILED OBSERVATIONS - HIGH RISK

Observation

The fire suppression system in the HRMS/VISION server storage areas has been removed. The departments rely on the fire department that is "just down the block" in case of a fire emergency. There are no current plans to replace the disabled fire suppression system.

The Department of Labor and Industry and the State Fire Marshall have approved the State's new system, which is similar to one used in the State Capitol building, according to Department personnel.

The *fire extinguishing* system where the main computers are that run these software networks was removed and only replaced with a fire and smoke *detection* system. In the event of the fire, servers, electronic data storage systems, and other critical computer systems could be put at even greater risk of destruction because the only means to extinguishing a fire is by the local fire department.

Recommendation

The National Fire Prevention Association (NFPA) recommends several Halon alternatives for the suppression of fires in computer equipment storage areas. Management should immediately take proactive steps to install a fire prevention system to safeguard all mission critical applications.

The Department should meet the codes and standards set by the National Fire Protection Association (NFPA), which includes the use of "a gaseous agent inside units in sprinklered or non-sprinklered computer areas."

THREE STEPS TO BETTER IT DESIGN

To ensure I.T. Security is a key function in any new I.T. system design, Vermont and its leaders must recognize information technology as a critical asset that is essential to the State's ability to continue serving citizens efficiently and effectively.

In *Wiring Vermont's Future*, a special report our office issued on March 14, 2002, we recommended Vermont take three important steps:

- Establish an independent I.T. Investment Board comprised of private and public sector professionals both with business and I.T. expertise, the CIO, and representatives from the Legislature to provide technical assistance in the oversight and evaluation of I.T. project development, and help select, prioritize and approve I.T. investments;

- Require the preparation of a strategic plan for I.T. investments; and,

- Empower the Office of the CIO with the statutory authority and resources to oversee the enterprise-wide development and effective use of I.T. resources.

DETAILED OBSERVATIONS - MODERATE RISK

Observation

No formal policy exists regarding how new users are granted access and how existing users have their access terminated for either HRMS or VISION. New user accounts are created as a result of a written request from department supervisors. User accounts are terminated via informal documentation.

The Department of Personnel and the Department of Finance and Management maintain that accounts are “terminated automatically when staff leave State employment, either through retirement or death.” However, there has been no formal documentation of how this automation works.

According to information provided to the Office of the State Auditor, business managers are “encouraged to e-mail [the Department] when an employee was terminated.”

Recommendation

A formal I.T. hire/termination process should be written, communicated, monitored and audited.

DETAILED OBSERVATIONS - MODERATE RISK

Observation

The Department of Finance and Management and the Department of Personnel do not have formal written policies and procedures to ensure that only appropriate personnel make program changes to applications and hardware and that these changes are documented as well as audited on a regular basis.

Recommendation

Both departments should create formal, documented program change policies and procedures. Adherence to the policies and procedures should be tested and monitored regularly.

DETAILED OBSERVATIONS - MODERATE RISK

Observation

During a tour of the HRMS/VISION server storage areas, personnel made assertions that the battery/generator backup system was fail-safe. However, on September 4, 2002, a power outage caused “several system problems” with VISION that led to the system being shut down for repairs. Personnel claimed that “the [server] plugs were pulled out of the outlet” during work on some cables in the server storage area. Despite repeated requests by the Office of the State Auditor, the Department of Finance and Management has not fully explained what led to the September 4, 2002 power failure.

The Department said it is currently running an 80KVA UPS connected to a 300KVA Diesel generator with a 10-second delay programmed into the system. The Department asserts that the system was off the power grid five times last year and has “never lost data.”

Recommendation

Management should identify all risks related to power disruptions and mitigate those risks to ensure that business continuity is not affected.

DETAILED OBSERVATIONS - MODERATE RISK

Observation

There are no formal tape backup procedures for either the HRMS or VISION systems to transcribe and store an electronic record of key daily transactions. This means an entire day's activities could be lost as a result. Additionally, tape backups are stored in buildings within close proximity to the server storage locations. Finally, backup tapes are not tested to ensure backups were successful, or conducted per Agency policy. Both departments note that they have informal backup procedures and have assigned I.T. personnel to perform the backups.

The procedures provided to us by the Department of Finance and Management on this issue, while they represent a good initial step, still remain incomplete. These procedures do not define who is responsible for backups, who is the replacement when the staff who performs the backup is out, how backups are audited to ensure they are being performed correctly, if at all.

Recommendation

Both departments should take immediate steps to develop and implement formal tape backup procedures. After implementation, these procedures should be monitored and audited on a regular basis.

Additionally, management should take immediate steps to find a secure off-site location to store all backup tapes.

THE RISK ENVIRONMENT

THE PERCEPTION OF INFORMATION TECHNOLOGY 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 I.T. safeguards.

THERE IS RENEWED EMPHASIS on basic security measures like policies, locks, user names and passwords, firewalls and anti-virus software.

ORGANIZATIONS ARE IDENTIFYING senior managers responsible for assuring and planning for system-wide risk.

DETAILED OBSERVATIONS - LOW RISK

Observation

Detailed job descriptions have not been established for HRMS personnel responsible for information security. Therefore, it cannot be determined if personnel responsible for HRMS information security have the requisite skills to meet the demands called for in their positions.

The staff position to which the security responsibility has been assigned is within the State's System Developer series of job descriptions. These I.T. descriptions are broadly written, however, and do not include the tasks related to information security operations, according to Department personnel.

Recommendation

Formal job descriptions for all I.T. personnel should be clearly defined and documented.

Management should then determine if the staff in current I.T. positions have the necessary skills needed to perform their jobs effectively, especially as it relates to information security.

DETAILED OBSERVATIONS - LOW RISK

Observation

Access into the main entrances of the server storage locations for both HRMS and VISION are secure, but there is no closed-circuit television (CCTV) camera to monitor the entrance.

Data centers of many public and private institutions that house sensitive information, while in compliance with various government entities, utilize CCTV technology to enhance the security of these centers.

Recommendation

Management should consider installing CCTV cameras at all access points to critical server storage areas.

APPENDIX A

(Objective & Scope)

SCOPE & OBJECTIVE OF IT SECURITY REVIEW

The Office of the Vermont State Auditor conducted this high-level I.T. security assessment in connection with the annual audit of the general purpose financial statements for the year ended June 30, 2002. The Office received assistance from KPMG's Risk Advisory Services (RAS) in its review of select State agencies and departments.

The objective of this high-level assessment was to establish a standard for future I.T. review, and its scope was to examine logical access security and physical security of the following I.T. systems:

- Human Resources Management System (HRMS) at the Department of Personnel; and,
- Vermont Integrated Solutions for Information and Organizational Needs (VISION) at the Department of Finance and Management.

Along with this high-level assessment, a draft audit plan for conducting future I.T. security (logical and physical) audits was created. This audit plan will be used to test agency/department ability to comply with any previous (and future) recommendations made by the State Auditor.

Additionally, The Office and KPMG performed I.T. security audits of two systems at two departments - HRMS at the Department of Personnel and VISION at the Department of Finance and Management.

In completing our high level security review, we performed the following activities:

Conducted in-person meetings on August 21 and 22, 2002 as well as various follow-up phone and e-mail interviews with the following personnel to gain an understanding of the security and operations practices:

Margaret Ciechanowicz, I.T. Director, Department of Finance and Management;
Cindy LaWare, Deputy Commissioner, Department of Personnel;
Steve Zuanich, Director of Payroll, Department of Personnel;
Pam Perry, System Developer, Department of Finance and Management;
Shannon Spidle, Security Officer, Department of Finance and Management;
Bill Laferriere, Director, Division of Communications and Information Technology, Department of Buildings and General Services;
Jack Storti, I.T. Manager-Technical Support, Division of Communications and Information Technology, Department of Buildings and General Services;

SCOPE & OBJECTIVE OF IT SECURITY REVIEW

Rick Conklin, I.T. Manager-Data Center Operations, Division of Communications and Information Technology, Department of Buildings and General Services;
Laura Morse, Infrastructure Manager, [VISION], Department of Finance and Management;
Brad Ferland, Director of Financial Operations, Department of Finance and Management;
Jeanne Malachowski, Database Administrator, [VISION], Department of Finance and Management;
John Hackney, Security Administrator, [VISION], Department of Finance and Management;
Bob West, Deputy CIO, Office of the Chief Information Officer; and,
Tom White, Office of the Chief Information Officer.

Reviewed the following documentation provided by the Department of Finance and Management and the Department of Personnel:

Andersen's Technology Risk Consulting PeopleSoft Logical Security Review;
State of Vermont VISION Preference Administrator's Guide;
Draft Security Summary for Vermont's PeopleSoft HRMS 7.51;
HRMS User Access Memorandum dated July 15, 2002;
SQR Updating Procedures for HRMS;
Electronic Communications and Internet Use, State of Vermont Personnel Polices and Procedures (Number 11.7) dated July 1, 1999;
Memorandum of Understanding regarding shared I.T. services between the Department of Finance and Management and the Department of Personnel as of December 2001;
Department of Personnel Organizational Chart;
Department of Finance and Management Organizational Chart;
Physical Security Assessment Report prepared by Mantech Security Technologies Corporation dated December 18, 2000;
Andersen's Technology Risk Consulting Application Security Strategy;
Security Procedures Memorandum for VISION; and,
VISION Production Passwords Memorandum dated June 22, 2001.

SCOPE & OBJECTIVE OF IT SECURITY REVIEW

Reviewed the following documentation provided by the Department of Finance and Management and the Department of Personnel:

VISION – Accounts and Passwords Memorandum dated July 1, 2001;
Tape Backup Procedures for VISION Documentation**;**
VISION Fiscal-Year 2002 Year-End Closing Instructions;
State of Vermont Project Vision Security Roles Overview;
Department of Finance and Management Network Diagram;
Draft of the Information Technology Security Manual (currently being developed by CIT); and,
Application Security Strategy Document.

APPENDIX B

(Correspondence from/to the State Auditor)

ELIZABETH M. READY
STATE AUDITOR

STATE OF VERMONT

OFFICE OF THE STATE AUDITOR
132 STATE STREET
MONTPELIER, VERMONT 05633-5101

May 7, 2002

Sean Campbell, Commissioner
Department of Finance and Management
109 State Street
Montpelier, VT 05609-0401

Dear Commissioner Campbell:

I am writing to bring to your immediate attention a serious breakdown in existing controls surrounding access to the VISION system.

Now that Vermont is operating from the platform of a new software system my Office is testing system wide to assure that fraud and theft can be deterred and detected, and that proper internal controls are in place.

I wrote to you on February 6, 2002 regarding my Office's plans to assess the State's new financial management information system, VISION, in preparation for the audit for the year ending June 30, 2002. In that letter, which is attached, I outlined that my Office's audit work would focus on two areas: 1) system implementation follow-up, and 2) internal control documentation and testing in preparation for the FY 2002 audit.

In the course of testing this week, auditors were able to gain easy access to the VISION system in all units tested - <u>except</u> the State Treasurer's Office. This access was attained from a number of computers in state government. While auditors didn't actually process any transactions, it appears they, or others with a basic familiarity with VISION, could have entered, changed, approved, and budget checked vouchers for payment for various business units in the following departments and agencies:

- Executive Office
- Secretary of Administration's Office
- Office of the Chief Information Officer
- Department of Finance and Management,
- Department of Buildings and General Services
- Department of and Aging and Disabilities
- Department of Public Safety
- Legislative Council
- Agency of Transportation
- Court Administrator's Office

The Department of Finance and Management's current ***VISION System Confidentiality Agreement*** requires that state employees agree to change their VISION passwords upon initial use and every 90 days thereafter. Auditors' ability to access the VISION system *as users* in a variety of departments indicates that existing password protocols are inadequate. These inadequate internal controls place the State at significant risk that unauthorized persons may access the system to commit fraud or to otherwise do harm to the State and its assets.

The test work described above, as well as the recent allegations regarding fraudulent checks being cashed against a State account, highlight the need for stronger internal controls to protect the State's assets. Earlier this year my Office released two reports, which are attached, relating to security and data recovery policies and oversight of the State's information technology investments. In these reports we recommended that the Office of the Chief Information Officer implement statewide direction, policies, guidelines and monitoring related to passwords, data back-up and program changes. In addition, we recommended that agencies and departments conduct periodic assessments regarding server security, power back-up and the risk of not addressing known deficiencies.

We now, in addition, recommend that the Department of Finance and Management and each department take immediate steps to remedy these internal control weaknesses surrounding VISION password protocols and procedures. At a minimum these steps should include:

1. Removing easy access to state employee identification numbers from the State's Internet web page.

2. Developing and implementing VISION password protocols and procedures that would require all VISION users to change their passwords upon initial use and every 90 days thereafter. Such protocols and procedures might include a message prompt that requires users to change their passwords or be denied access.

Please let me know by May 17, 2002, what steps your Department plans to take to improve the internal control environment surrounding access to the VISION system. Please let me know if you have any questions.

Sincerely,

Elizabeth M. Ready
State Auditor

cc Office of the State Treasurer

From: Campbell, Sean
Sent: Thursday, May 09, 2002 11:16 AM
To: Cabinet Members
Cc: Clermont, Nancy; Hartrich, Toni; Joshua Slen (E-mail); Kirkland, Nancy; OConnell, Kevin; Otto Trautz (E-mail); Paul Perry (E-mail); Rice, Howard; Stuart Savage (E-mail)
Subject: Important Security Issue

In going live with the VISION system each user was assigned a temporary passcode to initially get into the system. The requirements were that the passcode be changed immediately-it was designed to be temporary. The logic used in creating the temporary passcode has been uncovered and the security of the VISION system breached by the Auditors Office. Nearly every Department and Agency was accessed at some level under one of your employees temporary passcodes. This means the passcodes have not been changed as required and agreed to by the users.

Passcodes must be changed today!

This is a serious matter. If someone can falsely access your books, depending on the level of security assigned to the user, state resources, your budget, and your reports could be seriously compromised. This requires immediate attention. Please share the importance of this matter with the users in your Department or Agency, and make sure they immediately come into compliance with the passcode rules.

The Department of Finance and Management does not know, the passcode of any user that has been changed but we do, of course, know the original and temporary passcodes. Any user still accessing the system with a temporary passcode on Monday will be shutout of the system.

For your information, I have attached the notice sent to your employees who are VISION users.

From: Domingue, Michelle
Sent: Thursday, May 09, 2002 9:46 AM
To: Campbell, Sean
Subject: Security

I have drafted something below. Let me know if you would like me to rework it or if there is anything else I can do to help.

It has been brought to our attention that users have not been changing their passwords after initial set up or every 90 days. This is a serious security issue. All original passwords were assigned with the same logic.
Uncovering the logic would allow anyone to easily login as you and impact all things in VISION you have access to. This could have serious repercussions.

You must, today, change your passcode if you have not yet changed from the original passcode assigned to you. All users that are still using the initial passcode will lose their security and ability to access the system Monday May 13.

Upon receiving your VISION login you signed the following agreement:

"Employee Acceptance of Confidentiality Agreement

I understand that my UserID is my personal identification and provides permissions to valuable data and automated resources. My UserID is not to be shared with any other person. As the owner of a UserID, it is my responsibility to protect the resources I have been permitted by protecting the confidentiality of my password. I understand that any use of my unique UserID is monitored and that I am accountable for how it is used.

I agree to change my password upon initial use and every 90 days thereafter. I will use a password that preferably contains both letters and numbers and is at least 6 characters in length, and I will keep that password secure."

We ask that you adhere to this agreement and immediately change your password.

Your password is changed on the VISION login screen, first fill in your User Id and current password, then click on "set password" to set and confirm your new password, once clicking okay on that sub-panel VISION will open as normal. If you have any questions about doing this, please call the VISION Help Desk.

APPENDIX C

(Department of Finance & Management’s Response to Draft Report)*

*The Commissioner of the Department of Finance & Management at the time of the review was Sean Campbell

Departments' Response to Draft Report

Recommendation (found on page 3)

Forced password change is not currently an option in the PeopleSoft versions of both HRMS or VISION. However, Vermont could try one of the following approaches:

Create a procedure to take a picture of the PeopleSoft encrypted password table on a prescribed basis and then compare the picture to the same table at a different point in time. A simple analysis of the two data files can reveal if passwords are being changed as mandated. This cost-effective approach can be done using a simple MS Access Database.*

Force password change at the network server login and/or at the Citrix server login stage. Additional functionality may be required and examined for cost effectiveness.

Purchase third-party software that works in conjunction with PeopleSoft to force application password change.

* *The first option noted above is not only a short-term fix. Many organizations with the same password change limitations have used it as a long-term solution.*

DEPARTMENTS' RESPONSE: The Office of the Auditor was able to gain access to the original accounts issued because they were users themselves. Having accounts allowed them to determine the algorithm used for the original issue of account information. All users were to change these accounts. Today, either the accounts have been eliminated or users have reset passwords.

Both departments mandate password change every 90 days. The PeopleSoft software does not provide the capability to force the password change. By procedure all users are notified every 90 days to change passwords. Follow-up procedures are being put in place that will identify those who have not changed their passwords and the department will contact them directly. In addition, when accounts are assigned, users sign a formal document agreeing to change their password regularly and to protect their password from unauthorized use.

The Department is investigating these tools and PeopleSoft is also installing additional configuration options in future releases of its software. Until then the departments are reviewing logs and tables regularly that store date stamped information about users, to identify those who have not changed their passwords. The staff and business managers are contacted to ensure passwords are changed. In addition, users of VISION/HRMS do not login directly to these applications. All staff members must first pass some authentication to gain access to the network. Only after they are authenticated as valid users to the

State systems can they access VISION. In many instances these passwords are under a 'forced change' and/or are considered strong passwords.

AUDIT TEAM'S REPLY: The instructions for obtaining a user's initial password were posted on the VT Intranet, which was accessible to all State employees, including the State Auditor's office. Though the departments might issue memos or send out e-mail reminders telling users they have to change their passwords, the systems do not force any password changes and the process is not monitored. During interviews with the Department of Finance and Management personnel, they said they had no way to force password changes; now they say "they are looking into it." What they did do was once they realized that anyone could find out what a user's password was, they looked at the PeopleSoft table to see what passwords were not changed for the original one given and locked those users out. We are pleased to hear from the current Commissioner of Finance and Management, Robert Hofmann, that plans are in the works to install a software upgrade in the second half of Fiscal Year 2004 that will mandate user password changes.

Recommendation (found on page 4)

A formal statewide information security policy should be finalized as soon as possible and issued to all State agencies/departments. Furthermore, compliance with the policy should be monitored frequently and a formal audit plan to ensure compliance should be introduced. We also recommend a complete system and integration controls (SIC) review be conducted for VISION, and possibly HRMS.

DEPARTMENTS' RESPONSE: The Office of the CIO, in a combined effort with IRMAC members, has adopted I.T. policies which are monitored and enforced, including those related to security.   All of these policies can be found on the CIO web site.

The following policies have been created by IRMAC specifically to address data backup, and the creation of user names and passwords:

POLICY TITLE: Access and Protection; 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. 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; 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. 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.

AUDIT TEAM'S REPLY: Though Appendix A includes some documents that relate to various security procedures, there is no comprehensive written manual for statewide security policies and procedures. The fact that the above comment says that they are "working on a security policy" refutes any claim that formal written policies and procedures exist. There is no written comprehensive I.T. security policy and procedure manual for the Department of Finance and Management and the Department of Personnel with respect to VISION and HRMS. Additionally, the development of these policies and procedures is not monitored by the Office of the CIO.

Recommendation (found on page 5)

Both departments should immediately complete formal written physical access policies and procedures manuals, and implement procedures to achieve compliance.

DEPARTMENTS' RESPONSE: The State has installed in the 133 State Street building, a card access system. Upon recommendation from an Appointing Authority and approval of the Director of CIT a badge is issued to authorized personnel to gain access to the computer operations area. Two access points during the day and three access points during the off hours. This information is on the security system and backed up and stored by Security. In addition, all non-badge visitors must sign in; state the purpose of their visit and be escorted while in the facility. No un-escorted individuals are allowed in the room. These procedures and the visitor log are maintained by the operations manager and are on file.

AUDIT TEAM'S REPLY: In our tour of the computing facility on August 21, 2002 with Bill LaFerriere we were told that they did not have any written documentation relating to policies and procedures for securing the facility.

Recommendation (found on page 6)

The National Fire Prevention Association (NFPA) recommends several Halon alternatives for the suppression of fires in computer equipment storage areas. Management should immediately take proactive steps to install a fire prevention system to safeguard all mission critical applications.

DEPARTMENTS' RESPONSE: This statement is incorrect. The Halon system was removed 3 years ago. At that time it was replaced with a VESDA particle detection system and was installed with a new fire alarm system in the computer room. This solution was approved by "Labor and Industry" and the "Fire Marshall" as an acceptable solution. The new detection system is similar to that used in the State Capital Building and is industry-proven Technology.

AUDIT TEAM'S REPLY: It is correct, that they have a detection system, but that is not what our observation was. Though they say they are in compliance with the fire marshal and Labor and Industry, they should refer to the National Fire Protection Association (NFPA) and their codes and standards: NFPA 75: The Protection of Electronic Computer/Data Processing Equipment. Chapter 6-4, "where there is a critical need to protect data in process, reduce equipment damage, and facilitate return to service, consideration shall be given to the use of a gaseous agent inside units in sprinklered or non sprinklered computer areas."

Recommendation (found on page 8)

A formal IT hire/termination process should be written, communicated, monitored and audited.

DEPARTMENTS' RESPONSE: The Department of Personnel and the Department of Finance and Management have a strict procedure for granting access to the financial and human resource systems, respectively. Documents were provided to the audit team that describe the process and forms that need to be completed and the specific authorizations required to have an account established for a State staff member. Accounts are terminated automatically when staff leave State employment, either through termination, retirement or death. Individual requests are also processed by Business Managers of departments who are the authorizing agents for access to these systems. These procedures are further specified in Bulletin 3.3.

AUDIT TEAM'S REPLY: The purpose of Bulletin 3.3 is for procedures relating to the delegation of authority for signing documents and talks about how the request for VISION access must be signed by authorized personnel. As far as the statement "Accounts are terminated automatically when staff leave State employment" is concerned, in our meeting with HRMS and VISION personnel (Margaret Ciechanowicz was at both meetings) on August 21 and August 22, 2002, we were told that "managers were encouraged to e-mail them when an employee was terminated" and that there was no formal written policy in place. An explanation of how this process is "automated" would be helpful.

Recommendation (found on page 9)

Both departments should create formal, documented program change policies and procedures. Adherence to the policies and procedures should be tested and monitored regularly.

DEPARTMENTS' RESPONSE: The application security procedures and detailed documentation of roles and access privileges delineate the accessibility for all users to the panels, processes and reports. This includes access to various modules based on position and job duties within an organization as well as consideration for separation of duties to ensure proper internal controls. These roles and privileges apply to staff within the Department of Personnel and Finance and Management as well as to users. Formal documents and procedures exist for any changes made to reports, interfaces, modifications to the application code and migration and testing of fixes and patches provided by the software/hardware companies. Functional and technical sign-off at the Director level is required.

Recommendation (found on page 10)

Management should identify all risks related to power disruptions and mitigate those risks to ensure that business continuity is not affected.

DEPARTMENTS' RESPONSE: This statement is incorrect. We are currently running an 80KVA UPS connected to a 300KVA Diesel generator with a 10-second delay programmed into the system. Our ability to sustain power and keep the data center running un-interrupted is state of the art. We have been off the power grid 5 times over the last 12 months and have "never lost data" as a result of our front-end power solution.

AUDIT TEAM'S REPLY: On September 4, 2002 the VISION Help Desk sent out the following message to all VISION end users: "A power outage yesterday afternoon created several system problems. We hope to correct these tonight and will be shutting down VISION at 4:30 p.m. today (Thursday, September 5, 2002). This is both Production and Reporting. The problems interfered with normal processing last night so that the Reporting database still has Tuesday data and several overnight jobs had to finish this morning causing additional performance problems." When asked why there was a power failure given the "state of the art" system, Margaret Ciechanowicz said in an e-mail to Susan Watson on September 6, 2002 that, "Well - its like the back-hoe. Apparently some work was being done with the cables and caused the plug to be pulled out of the outlet. When you unplug it, no contingency plan can help you!" We attempted to get further clarification of what exactly led to the power failure but were never given an answer.

Recommendation (found on page 11)

Both departments should take immediate steps to develop and implement formal tape backup procedures. After implementation, these procedures should be monitored and audited on a regular basis. Additionally, management should take immediate steps to find a secure off-site location to store all backup tapes.

DEPARTMENTS' RESPONSE: Formal backup procedures exist for both HRMS and VISION. The schedule is a fixed schedule with primary and secondary responsibility assigned to ensure backups occur according to schedule. Any divergence from this is considered a production down situation and the problem is escalated to the IT Director for resolution. The suggestion of storing a separate electronic record of transactions is moot. The VISION system is mirrored throughout the day (i.e. two copies always exist of the data) and the production system is programmed to fail-over to a duplicate computer. Each night a business copy of the production system is made. Additionally a full tape backup is scheduled every night. Using this model, storing transactions offers no additional recovery capacity.

AUDIT TEAM'S REPLY: The documents provided to us on December 20, 2002 regarding backup procedures were never provided to us during our interviews in September. The only document we received was a simple MS-Excel spreadsheet used to describe the tape retention schedule for VISION. It was by no means a formal written backup procedure. The recent documents provided are better documentation of some of the backup procedures in place, but they are still incomplete. It does not talk about who is responsible for backups, who is the replacement when the staff who performs the backup is out, how backups are audited to ensure they are being performed correctly, or at all.

Recommendation (found on page 13)

Formal job descriptions for all IT personnel should be clearly defined. Management should then determine if the staff in current IT positions have the necessary skills needed to perform their jobs effectively.

DEPARTMENTS' RESPONSE: The staff position to which the security responsibility is assigned is within the State's System Developer series of job descriptions. These I.T. job descriptions are broadly written, but do include the tasks related to information security operations. Skill review is part of the ongoing review of staff and the annual performance review process.

AUDIT TEAM'S REPLY: If these job descriptions are written, we never received copies of them.

Recommendation (found on page 14)

Management should consider installing CCTV cameras at all access points to critical server storage areas.

DEPARTMENT'S RESPONSE: Our operation is run 365 days a year and staffed to support that. We have 2 card access monitoring points to get into the computer room and during off hours, that is increased to 3. We have been audited by the IRS, AHS, Tax Department tand numerous other agencies and have never seen the recommendation to utilize CCTV.

AUDIT TEAM'S REPLY: Though the center may be in compliance with various government agencies, many other data centers (both private and public) with sensitive information utilize CCTV technology to enhance the security of their data centers.

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