O L A

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Teachers Retirement Association
Information Technology Security Controls

August 30, 2007 **07-23**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio) please call 651-296-1235. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

All OLA reports are available at our web site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Financial Audit Division Report

Teachers Retirement Association

Information Technology Security Controls

August 30, 2007 **07-23**

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

OLA

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

Representative Rick Hansen, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Members of the Minnesota Teachers Retirement Association Board of Trustees

Ms. Laurie Fiori Hacking, Executive Director
Minnesota Teachers Retirement Association

We have conducted an information technology security audit of the Minnesota Teachers Retirement Association. The audit focused on the adequacy of the association's information security controls that help to protect the integrity and confidentiality of its computer systems and data. The Report Summary highlights our overall conclusion. Our specific audit objective and conclusion are contained in Chapter 2 of this report. The audit report contained eight findings related to internal control weaknesses.

We would like to thank the staff from the Minnesota Teachers Retirement Association for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

End of Fieldwork: May 25, 2007

Report Signed On: August 27, 2007

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Teachers Retirement Association
Information Technology Security Controls

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Cecile Ferkul, CPA, CISA	Deputy Legislative Auditor
Eric Wion, CPA, CISA, CISSP	Audit Manager
Mike Woolley, CISA, CISSP	Auditor-in-Charge
John Kelcher	Auditor
Carolyn Engstrom, CPA	Auditor
Bill Betthauser	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Minnesota Teachers Retirement Association and the Office of Enterprise Technology at the exit conference held on August 14, 2007:

Minnesota Teachers Retirement Association:

Laurie Fiori Hacking	Executive Director
Luther Thompson	Assistant Executive Director, Administration
John Wicklund	Assistant Executive Director, Legal
Karen Williamson	Assistant Executive Director, Operations
Aaron Winterfeldt	Planning Director
Geoff Strub	Systems Manager
Carol Sachs	Systems Administrator
Chad Borsheim	Network Engineer
Roger Moeller	Network Engineer

Office of Enterprise Technology:

Mark Mathison	IT Compliance Manager

Minnesota Teachers Retirement Association
Information Technology Security Controls

Report Summary

Conclusion:

The Minnesota Teachers Retirement Association (TRA) did not have adequate security controls to protect the integrity and confidentiality of its computer systems and data.

This report contains eight findings relating to internal control weaknesses.

Key Findings:

- TRA did not have a comprehensive security management program. (Finding 1, page 6)
- TRA did not adequately filter network traffic to protect its computers and data. (Finding 2, page 7)
- TRA did not enforce strong account and password controls. (Finding 3, page 8)
- TRA did not adequately restrict access to some computer systems and data. (Finding 5, page 10)
- TRA had not developed a continuity of operations plan. (Finding 6, page 11)

Audit Scope:

We assessed the TRA's security controls as of May 2007.

Background:

The Minnesota Teachers Retirement Association administers retirement benefits for Minnesota public school educators. Educators and their employers contribute to TRA during their working years and obtain benefits upon retirement, disability, or termination of employment.

TRA's members include teachers and administrators employed in Minnesota's public elementary and secondary schools, charter schools, the Minnesota State Colleges and Universities system, and all other state educational institutions, with the exception of teachers employed by the cities of Saint Paul and Duluth and the University of Minnesota. As of June 30, 2006, over 550 employers, 79,000 active members, and 44,000 retirees and beneficiaries participated in the retirement plan, which had $17.8 billion in net assets. Fiscal year 2006 retirement contributions and payments to beneficiaries were $356 million and $1.2 billion, respectively.

This page intentionally left blank.

Chapter 1. Introduction

The mission of the Minnesota Teachers Retirement Association (TRA) is to administer retirement benefits for Minnesota public school educators. Educators and their employers contribute to TRA during their working years and obtain TRA benefits upon retirement, disability, or termination of employment. Benefits can take the form of monthly payments to retired members or refunds of employee contributions plus interest to members who leave the teaching profession prior to retirement.

TRA's members include teachers and administrators employed in Minnesota's public elementary and secondary schools, charter schools, the Minnesota State Colleges and Universities system, and all other state educational institutions, with the exception of teachers employed by the cities of Saint Paul and Duluth and the University of Minnesota. Effective June 30, 2006, the Minnesota Legislature merged the Minneapolis Teachers Retirement Fund Association into TRA. As of June 30, 2006, over 550 employers, 79,000 active members, and 44,000 retirees and beneficiaries participated in the retirement plan, which had $17.8 billion in net assets. Fiscal year 2006 retirement contributions and payments to beneficiaries were $356 million and $1.2 billion, respectively.

TRA contracted with a vendor to develop a new computer system to handle virtually all aspects of managing a retirement system, including recording member demographic information, employer and employee retirement contributions, and paying benefits. This computer system went into operation over a period of time that concluded in 2006. As of March 2006, TRA members had access to their account information and future benefit estimates via the Internet.

This information technology audit assessed the adequacy of the department's security controls that help it to protect the integrity and confidentiality of its business data.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We used guidance contained in the *Control Objectives for Information and Related Technology (COBIT)* and *ISO/IEC 17799* as our criteria to evaluate controls.[1] We also used the Teachers Retirement Association's policies and procedures to obtain evaluation criteria. Finally, we used information published by applicable technology vendors to evaluate select controls.

[1] COBIT, published by the IT Governance Institute, is an IT governance framework providing organizations with a set of generally accepted measures, indicators, processes and best practices to assist them in developing appropriate IT governance and control in an organization. ISO/IEC 17799 is an international information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

This page intentionally left blank.

Chapter 2. Security Controls

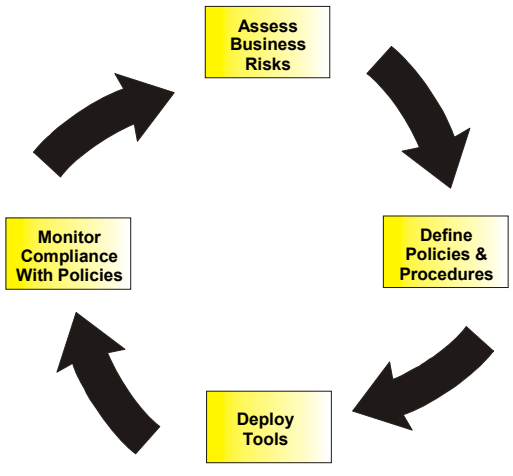
Chapter Conclusion

TRA did not have adequate security controls to protect the integrity and confidentiality of its business data.

Historically, many government organizations treated security as a technology issue. However, given government's reliance on technology for its day-to-day mission critical business processes, security must be a core business requirement that involves adequate risk management, reporting, and accountability. Furthermore, citizens are demanding strong security controls as concerns about identity theft and privacy skyrocket.

Organizations must deploy robust security controls to ensure data integrity, confidentiality, and system availability. Data integrity controls help protect the accuracy and completeness of data. Confidentiality controls help ensure that sensitive data, such as social security numbers and banking information, cannot be seen by unauthorized individuals. Finally, system availability controls help minimize the amount of time when citizens or staff cannot use the system to conduct business.

Figure 2-1
Security Management Lifecycle



Source: Auditor prepared.

Even with strong controls, it is impossible to be completely secure. This fact makes designing and implementing a security program an ongoing exercise in risk management. As illustrated in Figure 2-1, organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies and procedures to reduce their exposures to a level that executive management is willing to accept. Organizations then deploy tools, such as access control software, to enforce the policies and procedures sanctioned by management. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine-tune subsequent risk assessments in the ongoing security management lifecycle.

Our review of controls focused on the adequacy of selected security controls. Specifically, we designed our work to answer the following question:

- Did TRA have adequate security controls to protect the integrity and confidentiality of its business data?

Current Findings and Recommendations

1. TRA did not have a comprehensive security management program.

A security management program is a formal way to manage risks effectively throughout the organization and promptly respond to constantly changing threats. Not unlike other important business functions, such as accounting and finance, responsibility and authority for system security should be established at the highest levels of the organization, be well managed, and include appropriate planning and oversight.

TRA has not given a specific person or group the responsibility and authority to develop and enforce a security program. Instead, TRA has relied on a few information technology staff to make ad hoc security decisions and implement controls without providing them appropriate authority, guidance or oversight. Although these staff and others play a vital role in security, complete reliance on them typically does not work well because they are only responsible for portions of the organization's computing environment and internal controls. In addition, they are busy with their day-to-day tasks, that do not include security, and that may be at odds with security. Finally, technology and risks are constantly changing; therefore, it is critical that TRA have staff whose primary job responsibilities are devoted to managing its security program.

TRA has not developed risk assessment methodologies nor conducted a risk assessment. Without an assessment of risks, TRA's management does not know the degree of risk that exists nor can it determine what level of risk is acceptable and what steps it needs to take to reach that level.

Finally, TRA had virtually no written policies, procedures, and standards addressing information technology risks and security. Written policies, procedures and standards are critical because they outline management's security expectations and methods to fulfill those expectations. Staff cannot make consistent security decisions without policies and standards to refer to as guidance. Had it proactively defined and communicated its security expectations, TRA may have averted many of the findings in this report.

Recommendations

- *TRA should develop a comprehensive security management program.*

- *TRA should give a person or group the responsibility and authority to develop and implement its security program.*

- *The person or group in charge of the security program should be provided sufficient resources to:*
  - *lead organization-wide risk assessment efforts;*
  - *coordinate the development and dissemination of policies, procedures, and standards; and*
  - *monitor and enforce compliance with policies, procedures, and standards.*

2. TRA did not adequately filter network traffic to protect its computer systems and data.

TRA did not adequately filter network traffic to limit access to only people, programs, and computers that needed it. Network segmentation is a security strategy that involves placing similar computer resources into individual segments and limiting traffic between them to only what is needed. For example, an organization may place personal computers used by business staff in a different segment than computers running business applications or containing sensitive data. Similarly, an organization should place computers accessible by untrusted internet users in its own segment, separate from any segments containing computers on the internal private network.

A firewall and switch are computer devices used to accomplish segmentation and improve security controls. A firewall separates an organization's internal private network from the public Internet. A switch separates segments in an organization's private network. Serving as gatekeepers, a firewall examines all traffic that attempts to enter or leave an organization's private network, while a switch examines traffic that attempts to enter or leave different segments on the internal private network. Traffic that does not meet certain conditions, defined in security rules, is not allowed to pass.

TRA defined many traffic filtering rules in its firewall. However, TRA did not require rules to go through a formal change management process that included request, review, and approval procedures. Furthermore, it did not document or review rules on a periodic basis. As a result, staff struggled to identify the business justification for some rules, and some rules did not adequately filter traffic; most significantly, firewall rules did not filter traffic between a public web server and an internal server storing critical business data. Our inquiries resulted in TRA removing 14 rules while several more required additional investigation.

With a few exceptions, TRA did not define traffic filtering rules in its switch to limit traffic between different segments on its internal private network. For example, it allowed any traffic between the segment containing business users' personal computers and the segment containing mission critical business applications and data.

Recommendations

- *TRA should filter external and internal network traffic to only what is needed.*

- *TRA should develop change management procedures for critical security devices, such as its firewall and switch.*

- *TRA should document traffic filtering security rules and periodically review them for appropriateness.*

3. TRA did not enforce strong account and password controls.

TRA did not configure some computers to enforce strong password controls. Strong password controls are critical because they help prevent hackers from assuming the identity of legitimate system users. Most computer systems have features that can be customized to enforce strong password controls. For example, features can be enabled that prevent users from selecting easy to guess passwords, like dictionary words, and requiring passwords to periodically change. We examined these and other customizable password features and found several inconsistencies and weaknesses. In some cases, TRA did not implement important security controls. In others, security features were implemented, but some accounts were permitted to circumvent those controls.

Many accounts had weak, easily guessable passwords. Over 20 accounts, some very powerful, had passwords that matched their account names. In addition, TRA did not change a default password on a purchased software product. Many purchased software products come with default user accounts and passwords. It is important to immediately change default passwords because they provide an easy avenue for hackers to gain unauthorized access. In fact, lists of default accounts and passwords for most purchased software products can be easily found on the Internet.

Finally, some staff shared accounts with extremely powerful security clearances. Sharing passwords is never acceptable because it eliminates individual accountability. Information security relies on two fundamental principles: 1) positively confirming the identity of system users and 2) always having a mechanism to trace critical activities to specific individuals. Choosing not to vigorously enforce these principles exposes the computer systems and their data to unnecessary risks.

Recommendations

- *TRA should implement and rigorously enforce strong account and password management controls.*

- *TRA should immediately change all default passwords after installing software.*

- *TRA should prohibit the sharing of accounts and passwords.*

4. TRA did not have adequate controls to ensure computer users' access was appropriate on an ongoing basis.

TRA did not have adequate controls to ensure computer users' access to critical resources, such as business applications and data, was appropriate on an ongoing basis. More specifically, TRA lacked formal processes to:

- request, review and authorize access for computer users;
- periodically review and recertify computer users access;
- notify security staff when an employee leaves the organization; and
- identify and disable unused or dormant accounts in a timely manner.

In addition, TRA did not have adequate documentation to help managers make informed access decisions for their staff. Such documentation would describe, in nontechnical terms, the access options available and any access combinations that would result in someone having incompatible access. Without adequate information, TRA's managers often requested someone's access be set the same as another employee's access without explicitly defining the specific access needed. This is a risky practice because it can lead to employees obtaining inappropriate access.

Managing security of TRA's primary business application is extremely difficult because of the way security was designed and implemented. It has resulted in TRA customizing security for each employee rather than creating security groups that emulate business functions or processes and assigning security groups to people. Customizing security for each employee can be a very daunting task because there are over 80 employees, and the system has approximately 500 different objects that can be read, modified, or deleted.

Programmers did not consistently program security logic into the application. For example, the system was designed to provide employees different degrees of access, including no access or read access only. However, some people were able to process transactions when assigned security levels of no access or read only. Without going back through and testing the entire application, TRA may have difficulty ensuring the application always makes the proper security decision.

Recommendations

- *TRA should develop the following procedures to ensure a user's access is appropriate on an ongoing basis:*
  - *formally request, review, and authorize a computer user's access to critical resources;*
  - *periodically review and recertify a computer user's access;*
  - *notify security staff when an employee leaves the organization; and*
  - *identify and disable unused or dormant accounts in a timely manner.*

- *TRA should develop nontechnical security documentation to provide guidance to managers making security decisions.*
- *TRA should require that managers request specific access when setting up an employee's access.*
- *TRA should study solutions to avoid customizing security employee by employee.*
- *TRA should test its business application logic to ensure the proper security decision will be made.*

5. TRA did not adequately restrict access to some computer systems and data.

Some employees had inappropriate access to TRA computer systems and data. Of most significance, it did not protect two financial files, and computer programmers had excessive and incompatible access.

All employees had the ability to read files containing nonpublic financial information, including bank routing information. Twenty accounts, belonging to system administrators, computer programmers, contractors, and computer programs, also had the ability to modify the data in these files. In addition, TRA transmits these files electronically to the Office of Enterprise Technology unencrypted. These files should not be accessed by any TRA staff on a regular basis.

Computer programmers had inappropriate access to a critical database and several computers that allowed them to perform system administration tasks and alter or replace important files. Programmers also had physical access to TRA's data center that housed its most critical computers and data. Accordingly, unauthorized or erroneous computer program codes could be introduced to TRA's computing environment.

Recommendations

- *TRA should restrict access to computer systems and data to only those who have a business need.*
- *TRA should not allow programmers incompatible access to production computers and data.*
- *TRA should work with the Office of Enterprise Technology to encrypt nonpublic data transmitted between them.*

6. TRA had not developed a continuity of operations plan.

TRA had not developed a continuity of operations plan. A continuity of operations plan is a series of documented plans used to respond, recover, resume, and restore from a business interruption. Business interruptions can result from many events, including natural disasters, computer failures, and loss of key personnel. The Office of Enterprise Technology

developed a draft policy and standard in 2007 that will require executive branch agencies to have a business continuity of operations plan. Table 2.1 identifies the processes required to develop a business continuity of operation plan and each processes purpose.

Table 2.1
Processes Required to Develop a Business Continuity of Operations Plan

Process	Purpose
Periodic Risk Assessments	To identify potential events that could adversely affect the organization, the damage such events can cause, and the controls needed to prevent or minimize the impact.
Business Impact Analysis	To identify services and processes, the priority for their restoration and the support services that support them to help ensure services of the organization will be restored in the appropriate order based on priority. This analysis should include adequate representation from all business units and be validated and approved by management.
Recovery Strategy	To identify the specific steps needed to recover from a business interruption in a predetermined amount of time. Recovery strategies must be tested periodically.
Plan Documentation	To ensure the agency can respond to an incident, recover, and resume the critical processes and return to normal operations in a structured, orderly, and timely manner.
Periodic Plan Exercises and Maintenance	To verify the plan will work and information is current.
Awareness and Training Program	To ensure that all employees understand their roles and responsibilities in the event of a disruption.

Source: Office of Enterprise Technology Draft Enterprise Security Standard on Continuity of Operations 2007 – 01.

Organizations that fail to adequately plan for disruptions may find themselves unable to conduct business for undesirable and prolonged timeframes. A significant disruption could prevent TRA from collecting and recording retirement contributions or paying and recording benefits in a timely manner. In addition to not being able to conduct business, the organization would likely incur significant costs resulting from staff being unproductive.

Recommendation

- *TRA should develop a continuity of operations plan.*

7. TRA had not updated software running on some computers to remedy known security flaws.

TRA did not promptly install software updates or security-related software patches on some of its computers. TRA uses many commercial software packages. Computer hackers

routinely discover and exploit flaws in commercial software to gain unauthorized access to computer systems. When these exploits occur, vendors develop and publish software patches to correct the deficiencies in their products. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers. Staying up to date with software patches can be a very challenging task for an organization. To meet this challenge, organizations need a formal process to learn about new vulnerabilities and determine whether their systems are at risk. Also, organizations need formal testing and installation procedures that include an exit strategy, should a software patch result in a system failure.

Recommendation

- *TRA should develop procedures to promptly test and install security-related software patches and updates.*

8. TRA did not develop comprehensive security monitoring procedures.

TRA did not develop comprehensive monitoring procedures to detect and promptly respond to security-related events, such as unauthorized attempts to access computer systems and data. Although the best security controls are those that prevent inappropriate events from happening, it is virtually impossible to design flawless preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization also must have predefined incident response procedures. Organizations that do not have effective procedures may fail to discover their computer systems and data are insecure until it is too late, and someone has gained unauthorized access.

TRA can customize many commercial software products to log various types of security events. Many software products can even send alerts to specific individuals when events occur. In some cases, TRA did not assess its risks and define specific events to log. Furthermore, TRA rarely reviewed the security event logs that some software products generated.

Recommendation

- *TRA should define specific security events to log and regularly review those logs to identify potential security breaches or system misuse by employees.*

Teachers Retirement Association
60 Empire Drive • Suite 400 • St Paul MN 55103-4000

August 24, 2007

Mr. James R. Nobles
Legislative Auditor's Office
Room 140, Centennial Office Building
658 Cedar Street
Saint Paul, MN 55155-1603

Dear Mr. Nobles:

Thank you for the opportunity to review and respond to your office's security audit of the Teachers Retirement Association (TRA). We take our responsibility to secure data and computer applications seriously. We would like to emphasize that some of the areas cited in your audit are already being addressed in our day-to-day work. However, we agree that TRA lacks formally written policies and procedures and the centralized focus for the security management program that you recommend. We have already implemented several of your recommendations to improve controls. Upon establishment of the security management program, formal written policies and procedures will be developed. Our response to your audit findings and recommendations are:

1. ***Finding: TRA did not have a comprehensive security management program.***

Recommendation 1: TRA should develop a comprehensive security management program.

TRA Response: We agree with your recommendation and believe a centralized focus on security will strengthen security and internal controls on an agency-wide basis, including data and computer systems. TRA management is establishing a cross-divisional team (Security Management Team) charged with the responsibility for researching options and making recommendations regarding the structure and resources needed for a successful security program. We will begin implementing this program with the TRA Board of Trustees approval of the fiscal year 2009 administrative budget.

Person Responsible: Executive Management Team / Management Team

Resolution Date: July 1, 2008

Recommendation 2: TRA should give a person or group the responsibility and authority to develop and implement its security program.

TRA Response: The Security Management Team will explore the staffing and budgetary resources needed to implement a comprehensive security management program and make recommendations for implementation during the fiscal year 2009 budget period. The results will be presented to the TRA Board of Trustees for approval.

651.296.2409 • 800.657.3669 • 651.297.5999 FAX • 800.627.3529 TTY •
www.tra.state.mn.us

Person Responsible: Security Management Team

Resolution Date: July 1, 2008

Recommendation 3: The person or group in charge of the security program should be provided sufficient resources to:

- Lead organization-wide risk assessment efforts;
- Coordinate the development and dissemination of policies, procedures, and standards; and
- Monitor and enforce compliance with policies, procedures and standards.

TRA Response: The Security Management Team will make recommendations to implement a security management program that meet the objectives outlined by the OLA.

Group Responsible: TRA Management Team

Resolution Date: July 1, 2008.

2. Finding: TRA did not adequately filter network traffic to protect its computer system and data.

Recommendation 1: TRA should filter external and internal network traffic to only what is needed.

TRA Response: The external traffic issue was resolved during the audit and we are correcting the internal network traffic issue.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: March 1, 2008.

Recommendation 2: TRA should develop change management procedures for critical security devices, such as its firewall and switch.

TRA Response: The security management person(s) or group will incorporate these procedures into the overall security management program for TRA.

Person Responsible: Security Management person(s) or group

Resolution Date: Starting July 1, 2008.

Recommendation 3: TRA should document traffic filtering security rules and periodically review them for appropriateness.

TRA Response: This will be based on procedures and policies developed by Security Management person(s) or group.

Person Responsible: Security Management person(s) or group

Resolution Date: Starting July 1, 2008.

3. Finding: TRA did not enforce strong account and password controls.

Recommendation 1: TRA should implement and rigorously enforce strong account and password management controls.

TRA Response: TRA had prepared a revised password policy prior to your audit but delayed implementation until seeing the results of your analysis. Now that the audit is complete, the password policy will be implemented.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: October 1, 2007

Recommendation 2: TRA should immediately change all the default passwords after installing software.

TRA Response: We agree with the recommendation.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: Already implemented.

Recommendation 3: TRA should prohibit the sharing of accounts and passwords.

TRA Response: We agree with the recommendation and the isolated instances in which the practice was used has been discontinued.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: Already implemented

4. Finding: TRA did not have adequate controls to ensure computer users' access was appropriate on an ongoing basis.

Recommendation 1: TRA should develop the following procedures to ensure a user's access is appropriate on an ongoing basis:

- Formally request, review and authorize a computer user's access to critical resources;
- Periodically review and recertify a computer user's access;
- Notify security staff when an employee leaves the organization; and
- Identify and disable unused or dormant accounts in a timely manner.

TRA Response: TRA will take immediate steps to resolve these issues. Additionally, the Security Management person(s) or group will develop formal policies and procedures to address these issues as part of the overall security management program for TRA.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: March 1, 2008.

Recommendation 2: TRA should develop non technical security documentation to provide guidance to managers making security decisions.

TRA Response: TRA will develop a non technical security document to guide managers in making accurate decisions regarding the assignment of security levels for staff.

Person Responsible: Geoff Strub, Systems Manager and the Security Management Team

Resolution Date: March 1, 2008.

Recommendation 3: TRA should require that managers request specific access when setting up an employee's access.

TRA Response: TRA will modify its existing form which managers will be required to submit to give specific access to an employee.

Person Responsible: Geoff Strub, Systems Manager and Security Management Team

Resolution Date: March 1, 2008.

Recommendation 4: TRA should study solutions to avoid managing security employee by employee.

TRA Response: Due to the specialized responsibilities of TRA staff and cross-training used to manage Association work, the group security paradigm was not used to design the existing FROST security. TRA has initiated a project to reevaluate the security package in the FROST system.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: March 1, 2008.

Recommendation 5: TRA should test its business application logic to ensure the proper security decision will be made.

TRA Response: Security code will be reviewed, modified where necessary, and retested.

Person Responsible: Geoff Strub, Systems Manager and user staff.

Resolution Date: March 1, 2008

5. Finding: TRA did not adequately restrict access to some computer systems and data.

Recommendation 1: TRA should restrict access to computer systems and data to only those who have a business need.

TRA Response: TRA will re-evaluate current physical access and further restrict as needed. The data issue is being evaluated.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: January 1, 2008.

Recommendation 2: TRA should not allow programmers incompatible access to production computers and data.

TRA Response: TRA will re-evaluate current access and further restrict as needed.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: January 1, 2008.

Recommendation 3: TRA should work with the Office of Enterprise Technology to encrypt nonpublic data transmitted between them.

TRA Response: We are presently working with OET to resolve this issue.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: November 1, 2007.

6. Finding: TRA has not developed a continuity of operations plan.

Recommendation: TRA should develop a continuity of operations plan.

TRA Response: The development of a business continuity plan is already a management initiative for fiscal year 2008. The TRA Board of Trustees has committed budgetary support for our preliminary analysis and we expect to provide them with a comprehensive strategy beginning with fiscal year 2009.

Person Responsible: Aaron Winterfeldt, Planning Director

Resolution Date: July 1, 2008

7. Finding: TRA has not updated software running on some computers to remedy known security flaws.

Recommendation: TRA should develop procedures to promptly test and install security-related patches and updates.

TRA Response: Software patches and updates have been and will continue to be evaluated on a regular basis and are installed when deemed necessary. We will develop policies assessing the frequency of updates by software product to insure the appropriate patches are applied.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: Ongoing.

8. Finding: TRA did not develop comprehensive security monitoring procedures.

Recommendation: TRA should define specific security events to log and regularly review these logs to identify potential security breaches or system misuse by employees.

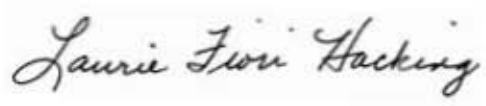
TRA Response: We agree with your recommendation. TRA currently monitors security on a daily basis and will develop formal policies, procedures and standards to maximize utilization of monitoring tools and purchase any additional tools required to fully monitor security in our environment.

Person Responsible: Geoff Strub, Systems Manager

Resolution Date: Starting July 1, 2008.

Thank you for the valuable recommendations you have suggested to improve our operations and for the constructive discussion we have had with you and your staff about the issues reported.

Sincerely,



Laurie Fiori Hacking
Executive Director