OLA OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

PUBLIC EMPLOYEES RETIREMENT ASSOCIATION

INFORMATION TECHNOLOGY AUDIT

August 14, 2008 **Report 08-18**

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

August 13, 2008

Representative Rick Hansen, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Mary Most Vanek, Executive Director
Public Employees Retirement Association

This report presents the results of our information technology audit of the Public Employees Retirement Association's security controls. The audit focused on controls that protect the integrity, confidentiality, and availability of the association's computer systems and business data. The report contains six findings.

We discussed the results of the audit with association staff on July 31, 2008. Management's response to our findings and recommendations is included in the report.

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

/s/ James R. Nobles	*/s/ Cecile M. Ferkul*
James R. Nobles Legislative Auditor	Cecile M. Ferkul, CPA, CISA Deputy Legislative Auditor

Table of Contents

Page

Report Summary

Conclusions

The Public Employees Retirement Association (PERA) generally had adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data. However, the department had six weaknesses related to internal control over some significant aspects of its operations. We highlight the findings below.

Findings

1. Prior Finding Partially Resolved: PERA did not design and implement an overall security management framework.
2. PERA did not have adequate controls to ensure computer users' access was appropriate on an ongoing basis, and it did not adequately restrict access to some computer systems and data.
3. Prior Finding Partially Resolved: PERA did not develop comprehensive security monitoring procedures.
4. PERA did not follow adequate change management procedures.
5. PERA had not segmented its internal private network to improve security over its computer systems and data.
6. PERA has not fully tested its continuity of operations plan, developed continuity training, or selected adequate facilities to recover computer operations.

Audit Objectives and Scope

Our audit objectives were to answer the following questions:

- Did PERA have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data?
- Did the organization resolve prior audit findings?[1]

We assessed PERA security controls as of April 2008.

Background

PERA administers four public employee retirement plans: the Public Employees Retirement Plan, Police and Fire Plan, Correctional Plan, and the Defined Contribution Plan. Employees and their employers contribute to these plans during their working years and obtain benefits upon retirement, disability, or termination of employment. At June 30, 2007, the retirement association reported that its pension funds had $19.5 billion in net assets. Fiscal year 2007 retirement contributions and payments to beneficiaries were $693.2 million and $1.1 billion, respectively.

[1] Financial Audit Division Report 02-62.

Public Employees Retirement Association

Agency Overview

The Public Employees Retirement Association (PERA) administers four public employee retirement plans: the Public Employees Retirement Plan, Police and Fire Plan, Correctional Plan, and the Defined Contribution Plan. Employees and their employers contribute to these plans during their working years and obtain benefits upon retirement, disability, or termination of employment.

Approximately 2,000 government employers, including counties, cities, townships, school districts, and other local units of government contribute to PERA's four retirement plans. Collectively, these four plans hold retirement assets for 236,000 active and former employees and their beneficiaries. At June 30, 2007, the retirement association reported that its pension funds had $19.5 billion in net assets. Fiscal year 2007 retirement contributions and payments to beneficiaries were $693.2 million and $1.1 billion, respectively.

This information technology audit assessed the adequacy of the retirement association's security controls that help it to protect the integrity, confidentiality, and availability of its computer systems and business data.

Objectives, Scope, and Methodology

Our audit of PERA's security controls focused on the following audit objectives for controls as of April 2008:

- Did PERA have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data?
- Did the organization resolve prior audit findings?[2]

To answer these questions, we interviewed PERA staff and reviewed PERA policies, procedures, and other relevant documentation. We also used a variety of computer-assisted auditing tools to analyze the security infrastructure.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in the *Control Objectives for Information and Related Technology (COBIT*),[3] published by the IT Governance Institute and applicable special publications, primarily *800-53 Recommended Security Controls for Federal Information Systems*, published by the National Institute of Standards and Technology's (NIST) Computer Security Division.[4] We also used PERA's policies and procedures to obtain evaluation criteria. Finally, we used information published by applicable technology vendors to evaluate select controls.

Conclusions

Generally, PERA's security controls were adequate to protect the integrity, confidentiality, and availability of its computer systems and business data. However, the association could improve controls over some aspects of its security, as explained in the following findings. PERA resolved five of six prior findings.

[2] Financial Audit Division Report 02-62.

[3] COBIT 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.

[4] NIST is a nonregulatory federal agency within the U.S. Department of Commerce. The Computer Security Division responds to the Federal Information Security Management Act of 2002.

Findings and Recommendations

Finding 1

Prior Finding Partially Resolved: PERA did not design and implement an overall security management framework.

PERA made significant progress in resolving weaknesses discussed in Finding 1 of the prior audit report.[5] For example, it conducted a risk assessment, developed additional security-related polices, added new security-related hardware and software, and hired another person to help manage computers that performed important security functions.

While these are important ingredients of a security program, PERA had not established an overall management framework to ensure the program was well managed, e.g., comprehensive, tasks were coordinated, and program goals and objectives were achieved. Although several employees were responsible for different tasks important to the security program, PERA had not given a specific person or group the overall responsibility, authority, and resources to develop, manage, and enforce the program. PERA also had not articulated the security program's scope, objectives, goals, and responsibilities.

A security 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, identify roles and responsibilities, and include appropriate planning and oversight. A comprehensive security plan includes:

- a complete set of security policies and standards;
- procedures to implement and enforce the policies and standards;
- required financial and staffing resources; and
- security awareness and training.

Recommendations

- *PERA should give a person or group the responsibility, authority, and resources to develop, manage, and enforce the organization's security program.*
- *PERA should define the security program's scope, responsibilities, goals, and objectives.*

[5] Financial Audit Division Report 02-62.

Finding 2

PERA did not have adequate controls to ensure computer users' access was appropriate on an ongoing basis, and it did not adequately restrict access to some computer systems and data.

PERA did not have adequate controls to ensure it provided employees with appropriate access to critical resources, such as business applications and data. More specifically, PERA lacked formal processes to:

- request, review, and authorize access for computer users;
- periodically review and recertify computer users' access; and
- notify security staff when an employee leaves the organization.

PERA 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 in the business application and any access combinations that would result in someone having incompatible access. Without adequate information, PERA'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.

Some employees had inappropriate access to PERA computer systems and data. Of most significance, PERA did not protect some financial files, adequately restrict security administration access, and computer programmers had excessive and incompatible access.

- Twenty-three people, including computer programmers, system administrators, and business staff, had the ability to modify files containing nonpublic financial information, including bank routing information. No PERA staff should access these files on a regular basis.
- PERA transmitted nonpublic files electronically to the Office of Enterprise Technology unencrypted.
- Three technology staff had the ability to modify employees' security clearances in PERA's computer system used to manage member accounts, although their job duties did not require such access.
- Three computer programmers had temporary access that PERA had not subsequently removed. Another programmer had the wrong security template.

Recommendations

- *PERA should develop formal procedures to:*
  - *request, review, and authorize access for computer users;*
  - *periodically review and recertify computer users' access; and*
  - *notify security staff when an employee leaves the organization.*
- *PERA should develop nontechnical security documentation to provide guidance to managers making security decisions.*
- *PERA should restrict access to computer systems and data to only those who have a business need.*
- *PERA should work with the Office of Enterprise Technology to encrypt nonpublic data transmitted between them.*

Finding 3

Prior Finding Partially Resolved: PERA did not develop comprehensive security monitoring procedures.[6]

PERA 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 PERA did log some security events, others were not logged, some were inconsistently logged, and events were often not routinely reviewed.

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 or abuse. 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.

In addition to external attacks, other events require monitoring, such as system misuse by employees, changes to critical computer settings, and exceptions to defined policies and procedures.

Recommendation

- *PERA should assess its monitoring needs to define specific security events to log and regularly review those logs to identify potential security breaches, system misuse by employees, and exceptions to policies and procedures.*

[6] This weakness was reported in Finding 1 of the prior audit report, Financial Audit Division Report 02-62.

Finding 4

PERA did not follow adequate change management procedures.

PERA did not follow adequate change management procedures. Change management is a process of managing and controlling all changes to the technology infrastructure. Its purpose is to implement only appropriate and authorized changes, causing minimal disruption. Changes often are frequent and can take many forms, including changes to processes, computer programs, and computer settings.

PERA developed and continued to modify several computer programs that are essential to its ongoing business operations. While PERA obtained tools to assist in managing software changes, they had not adopted and enforced rigorous change management procedures. A review of 25 changes found the majority of changes did not include documentation describing the business requirements for the change, testing procedures and results, nor final approval.

Other changes to PERA's technology infrastructure did not typically follow any standard change management procedures. Examples of these changes include software patches or updates and computer configuration changes, including security-related changes. Failure to follow stringent change management procedures may result in unauthorized changes, computer disruption, or security vulnerabilities.

Recommendation

- *PERA should ensure that computer-related changes follow stringent change management procedures.*

Finding 5

PERA had not segmented its internal private network to improve security over its computer systems and data.

PERA had not segmented their internal private network to filter computer traffic and improve security. Someone who accessed PERA's internal computer network, including an employee working remotely, could move throughout the network and attempt to access any computer and computer program on it. For example, anyone connected to the network could attempt to access powerful programs that only administrators need to access. Network segmentation improves control by only allowing authorized traffic in or out of each segment. These devices examine traffic that attempts to enter or leave different segments on the internal, private network. Traffic that does not meet the criteria defined in security rules is not allowed to pass. Segmentation also helps prevent the spread of malicious software, such as viruses, worms, and trojans.

Recommendation

- *PERA should segment its internal network and only allow authorized traffic between each segment.*

Finding 6

PERA had not fully tested its continuity of operations plan, developed continuity training, or selected adequate facilities to recover computer operations.

PERA had not performed a comprehensive simulation exercise to ensure its continuity of operations plan was adequate to meet its recovery time objectives. In addition, PERA has not developed a training program to educate all employees of their roles and responsibilities in the event of a disruption.

A continuity of operations plan is a documented plan used by an organization to respond, recover, resume, and restore people, business processes, and technology from a disruption caused by events such as a tornado, flood, fire, computer virus, computer failure, or terrorism. Without adequate and routine testing, PERA did not have assurance the plan would work if a real event occurred and caused a significant disruption.

PERA's plan included storing computer equipment and backup tapes at locations that lack adequate physical and environmental controls to protect equipment and data. In addition, these locations may not have the telecommunications capacity to handle the computer processing requirements over an extended period.

Recommendations

- *PERA should perform an annual continuity of operations exercise.*
- *PERA should develop a department-wide training program to educate all employees of their roles and responsibilities as they pertain to PERA's continuity of operations plan.*
- *PERA should find adequate off-site facilities to store backup tapes and serve as an alternate computer processing location.*

Public Employees Retirement Association of Minnesota
60 Empire Drive, Suite 200
Saint Paul, Minnesota 55103-2088
Member Information Services: 651-296-7460 or 1-800-652-9026
Employer Response Lines: 651-296-3636 or 1-888-892-73
PERA Fax Number: 651-297-2547 ◆ PERA Website: www.mnpera.org

August 7, 2008

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Room 140, Centennial Office Building
658 Cedar Street
St. Paul, MN 55155-1603

Dear Mr. Nobles:

Thank you for the opportunity to review and respond to the information technology audit you conducted at the Public Employees Retirement Association (PERA). PERA continues to be committed to providing a secure environment for the data we receive and retain in our databases, and appreciate your help in that endeavor. We had been working on all six of your findings prior to your audit, and agree that we need to continue developing formal documentation and a high level security management framework. Our responses to your findings and recommendations are given below.

1. ***Finding: PERA did not design and implement an overall security management framework.***

   Recommendation 1: PERA should give a person or group the responsibility, authority, and resources to develop, manage, and enforce the organization's security program.

   Recommendation 2: PERA should define the security program's scope, responsibilities, goals, and objectives.

   Response: We agree with your recommendation. Our IT management team has been designing and implementing various parts of our security program for the last few years, but we have not yet developed a documented security management framework with formal statements of scope, responsibilities, goals and objectives. We will work on such a program during fiscal year 2009 and determine which group has responsibility to maintain that program.

   Resolution Date: June 30, 2009

   Person Responsible: Dave DeJonge

2. ***Finding: PERA did not have adequate controls to ensure computer users' access was appropriate on an ongoing basis, and it did not adequately restrict access to some computer systems and data.***

Recommendation 1: PERA should develop formal procedures to request, review, and authorize access for computer users; periodically review and recertify computer users' access; and notify security staff when an employee leaves the organization.

Response: We agree with your recommendation. We will review our existing method of authorizing access to users and make the changes recommended.

Resolution Date: January 1, 2009

Person Responsible: Dave DeJonge

Recommendation 2: PERA should develop nontechnical security documentation to provide guidance to managers making security decisions.

Response: We agree with your recommendation. We will develop documentation that managers can use when making security decisions.

Resolution Date: January 1, 2009

Person Responsible: Dave DeJonge

Recommendation 3: PERA should restrict access to computer systems and data to only those who have a business need.

Response: We agree with your recommendation. We reviewed existing access and made the changes you recommended during the audit. We have restricted user access to secured files and directories to those users who have a business need.

Resolution Date: Already implemented

Person Responsible: Robert Janas

Recommendation 4: PERA should work with the Office of Enterprise Technology to encrypt nonpublic data transmitted between them.

Response: We contacted OET several times over the past year in an attempt to transmit data securely, and were told they did not have the capability yet. During the audit it was brought to our attention that they now have the capability to accept encrypted files. We will be working with them to encrypt future files containing nonpublic data.

Resolution Date: November 1, 2008

Person Responsible: Dick Rademaker

3. *Finding: PERA did not develop comprehensive security monitoring procedures.*

Recommendation 1: PERA should assess its monitoring needs to define specific security events to log and regularly review those logs to identify potential security breaches, system misuse by employees, and exceptions to policies and procedures.

Response: Although our systems are configured to email any potential security events to our network administrators on a real-time basis, we agree that we could do a better job of logging events and monitoring those logs.

Resolution Date: January 1, 2009

Person Responsible: Dick Rademaker

4. *Finding: PERA did not follow adequate change management procedures.*

Recommendation 1: PERA should ensure that computer-related changes follow stringent change management procedures.

Response: Because we are a small agency, our change management procedures have often been informal but effective. We will formalize those procedures and do a better job of utilizing the tools we already own to manage technological changes.

Resolution Date: January 1, 2009

Person Responsible: Dean Millam

5. *Finding: PERA had not segmented its internal private network to improve security over its computer systems and data.*

Recommendation 1: PERA should segment its internal network and only allow authorized traffic between each segment.

Response: We were in the process of designing the segmentation of our internal network before the audit, and implemented part of it during the audit. We will continue to make the changes recommended during this fiscal year.

Resolution Date: June 30, 2009

Person Responsible: Dick Rademaker

6. *Finding: PERA had not fully tested its continuity of operations plan, developed continuity training, or selected adequate facilities to recover computer operations.*

Recommendation 1: PERA should perform an annual continuity of operations exercise.

Response: PERA made extensive changes to our disaster recovery plan and the method we will use when getting systems back up and running. Those changes required us to make technological changes as well, which we were in the process of doing when the audit began. We had planned to test our plan in September, and are still on track to do so, with adjustments being made after the test results are anlyzed.

Resolution Date: January 1, 2009

Person Responsible: Dave DeJonge

Recommendation 2: PERA should develop a department-wide training program to educate all employees of their roles and responsibilities as they pertain to PERA's continuity of operations plan.

Response: We had planned that for September along with the continuity of operations exercise.

Resolution Date: October 1, 2008

Person Responsible: Dave DeJonge

Recommendation 3: PERA should find adequate off-site facilities to store backup tapes and serve as an alternate computer processing location.

Response: We will test our existing alternate computer processing location in September and make decisions about whether or not we need to find an alternative location. We will also review the facilities we use to store backup tapes.

Resolution Date: January 1, 2009

Person Responsible: Dave DeJonge

Sincerely,

Mary Most Vanek

Mary Most Vanek
Executive Director