Chapter 8
Public Employees Benefits Agency
Security Audit Follow Up

1.0 Main Points

Public Employees Benefits Agency (PEBA) has implemented four out of five recommendations that we made in our 2010 audit of its processes to secure its information systems and data. With the implementation of these recommendations, PEBA has strengthened the security over the pension data it manages. PEBA has plans to implement the remaining recommendation in 2012-13 by testing the effectiveness of its IT security.

2.0 Introduction

PEBA administers government pension and benefit plans. This includes the Public Employees Pension Plan (PEPP) and Public Service Superannuation Plan (PSSP). PEBA serves about 81,000 active and inactive (deferred) members, pensioners, surviving spouses and dependents of these plans. Combined assets of all plans administered by PEBA are about $6.2 billion.

To carry out its responsibilities, PEBA must manage a wide range of pension and benefit information. PEBA uses information technology (IT) systems to manage this information and to provide pension and benefit information to its members. Securing pension and benefit information (ensuring its confidentiality, integrity, and availability) is vital to fulfilling PEBA's objectives including delivering its services and protecting the interests of its members.

Inadequate IT security could result in loss, inappropriate modification, and unauthorized disclosure of pension and benefit information. Unauthorized changes to the systems and data could compromise the integrity of the pension and benefit plans. Unauthorized disclosure of members' personal information (e.g., name, date of birth, social insurance number) could lead to the theft of their identity for fraudulent purposes.

In 2010, we assessed PEBA's processes to secure its information systems and data. Our 2010 Report – Volume 2, Chapter 8 (pp. 102-109) concluded that PEBA had adequate controls to secure (i.e., protect the confidentiality, integrity, and availability of) its information systems and data for the period October 1, 2009 to March 31, 2010 except it needed to:

- Periodically review and test the effectiveness of its IT security policies
- Comply with its security policy of monitoring software developers' access to its information systems and data
- Implement its disaster recovery plan

- Implement its approved policies and procedures for making changes to its information technology infrastructure

We made five recommendations to address these weaknesses.

On May 18, 2011 the Standing Committee on Public Accounts agreed with our recommendations.

3.0 Status of Recommendations

This section sets out each of the five recommendations and PEBA's actions up to March 31, 2012. We found that PEBA has implemented four recommendations and has work to do on the remaining one.

3.1 Reviewing Adequacy of Security Policies

We recommended that the Public Employees Benefits Agency periodically review the completeness of its information technology policies. (2010 Report – Volume 2)

Status – Implemented.

In our 2010 audit, we found that PEBA did not periodically review the effectiveness of its security policies. An annual review of security policies or a review when there are major changes to IT infrastructure or changes in technology helps keep security policies current and complete. PEBA has now established an annual review process.

3.2 Testing the Effectiveness of Security

We recommended that the Public Employees Benefits Agency periodically test the effectiveness of its information technology security. (2010 Report – Volume 2)

Status – We continue to make this recommendation.

In our 2010 audit, we found that PEBA did not periodically test the effectiveness of its IT security. The periodic testing of security using external experts helps management to monitor the adequacy of security and to strengthen security.

PEBA told us it is planning to test the effectiveness of its IT security in its 2012-2013 fiscal year.

3.3 Monitoring Software Developers

We recommended that the Public Employees Benefits Agency comply with its security policy of monitoring software developers' access to its information systems and data. (2010 Report – Volume 2)

Status – Implemented.

In our 2010 audit, we found that PEBA's security policies adequately governed the access of external software developers (vendors) to its systems and data. However, one vendor had remote access to a pension plan application and its data and this access was not monitored by PEBA. Consequently, PEBA's confidential data was at increased risk of unauthorized disclosure.

PEBA has removed the vendor's access and is complying with its policy governing vendor access.

3.4 Implementing and Testing Disaster Recovery Plans

We recommended that the Public Employees Benefits Agency implement and test its disaster recovery plan. (2010 Report – Volume 2)

Status – Implemented.

In our 2010 audit, we found that PEBA had developed a disaster recovery plan but it was not implemented and tested. The lack of an implemented and tested disaster recovery plan increased the risk that PEBA could not restore systems and data in the event of a disaster.

PEBA has now implemented its disaster recovery plan and has completed the initial testing of its plan. To maintain an effective disaster recovery plan, PEBA needs to test it annually.

3.5 Infrastructure Change Management Processes

We recommended that the Public Employees Benefits Agency implement its approved policies and procedures for making changes to its information technology infrastructure. (2010 Report – Volume 2)

Status – Implemented.

In our 2010 audit, we found that PEBA did not follow its approved policy for making changes to IT infrastructure. As a result, PEBA faced increased risk of unintended consequences such as the loss of system availability arising from changes to its infrastructure.

PEBA has now implemented its approved policies and procedures for making changes to its information technology infrastructure.