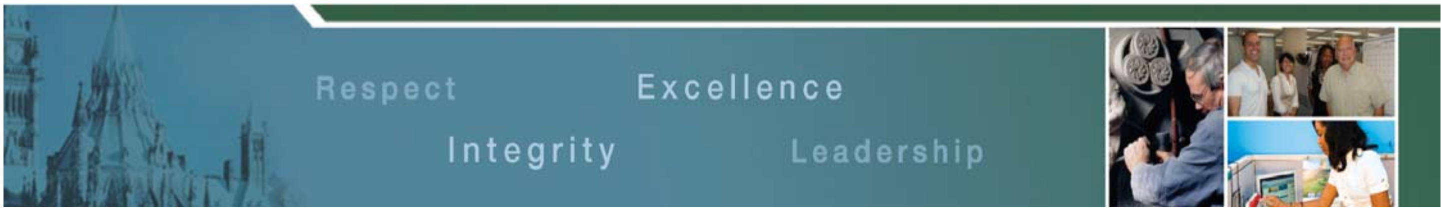

Final Report

2007-723

Audit of Access Management for Selected Information Technology (IT) Systems

Office of Audit and Evaluation

March 19, 2009

Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada
Canada

TABLE OF CONTENTS

MAIN POINTS

What was examined

i. Access management is intended to ensure that only authorized individuals can access information technology (IT) resources and information on a need-to-know[1] basis. These individuals should have the appropriate security level and be authenticated prior to being given access to the IT resources and information.

ii. The audit examined the access management for two IT systems used by the Translation Bureau for the translation of classified information, and the Human Resources Management System (HRMS) used by the Human Resources Branch to manage employee and position information for the department.

Why it is important

iii. Access management is an important element of IT security. Limiting access to IT systems and the information they contain is particularly important when the information is sensitive.

iv. Depending on the level of sensitivity, unauthorized access to classified or protected information stored on PWGSC IT systems could lead to loss of reputation or injury to the department and its clients, the government or even to the Canadian public.

What was found

v. Passwords are one of the key controls used to manage access to IT systems. The PWGSC IT Security Standards include password composition rules, however not all password composition rules are presented as mandatory. Other guidance issued by the department is inconsistent with the PWGSC IT Security Standards. However the IT Security Standards has been under review since September 2008.

vi. There are IT applications, such as the application used by PWGSC employees to log on to their workstations or the application to access the Internet, that do not enforce the password composition rules stated in the PWGSC IT Security Standards.

vii. The Translation Bureau has implemented certain measures to control access to the systems they use for the translation of classified information. However, processes and procedures used to manage access to IT systems were not fully documented.

[1] The need-to-know is defined as the need for someone to access and know information to perform his or her duties.

Certain controls were missing, such as logical access control and a formal management approval for the creation and modification of user accounts. The systems were not certified and accredited as mandated in the *Government Security Policy (GSP)*. However, the Translation Bureau has taken some steps towards certification and accreditation.

viii. The Human Resources Branch has controls in place to limit access to the Human Resources Management System (HRMS). However, two previous recommendations regarding access management were not implemented.

Recommendations and Management Action Plan

Management Response

Information Technology Services Branch considers that the results of the Audit accurately and fairly reflect the guidance on the use of passwords in Public Works Government Services Canada. The Information Technology Services Branch intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

The Chief Executive Officer of Information Technology Services Branch should:

1. Update the Public Works and Government Services Canada Information Technology Security policy instruments and user guidance to ensure consistency amongst policy instruments and user guidance.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

   1.1 ITSB will identify the PWGSC Information Technology Security policy instruments and user guidance that are impacted by this audit. This action will be completed by March 30, 2009.
   1.2 ITSB will validate the information to ensure consistency and update policy instruments and user guidance as required. This action will be completed by June 30, 2009.
   1.3 ITSB will seek departmental approval for policy instruments that need to be updated as required. This action will be completed by Sept 30, 2009.

2. Update the Public Works and Government Services Canada Information Technology Security Standards to ensure that password rules reflect inherent risks based on documented criteria and are stated as mandatory requirements.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

2.1 ITSB will review current document IT Security Standards password rules in light of inherent risk, and state password rules as mandatory requirements. The coming into force of the revised password rules will reflect inherent risks. This action will be completed by June 30th, 2009.
2.2 Seek departmental approval for the IT Security Standards password rules. This action will be completed by September 30, 2009.
2.3 Publish Security Standards documentation related to password rules. This action will be completed by November 30th, 2009.

3. Enforce compliance with the Public Works and Government Services Canada Information Technology Security Standards for all Public Works and Government Services Canada Information Technology systems and applications managed by the Information Technology Services Branch.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

3.1 ITSB will conduct a gap analysis to evaluate retrofit work required to implement updated password rules, by August 30th, 2009.
3.2 ITSB will prepare and present a business case to the Chief Financial Officer to obtain departmental approval for the most appropriate and cost-effective approach towards the implementation of the new password rules. This action will be completed by September 30th, 2009.
3.3 Upon approval of the most cost-effective approach towards the implementation of the new password rules, and commensurate with the approved funding, ITSB will implement the new password rules. This action will be completed by December 31st, 2010.
3.4 Service Management & Delivery (SM&D), Application Management and IT Operational Services (AMITOS), and PWGSC Branches will report their compliance on a periodic basis to the Office of the Chief Information Officer (OCIO). The OCIO will report the status of compliance to the Departmental IM/IT Steering Committee on a periodic basis. This action will be completed by November 30th, 2009.

Management Response

Translation Bureau considers that the results of the Audit accurately and fairly reflect the state of the management control framework in place to protect Information Technology Systems used in support of translation of classified information against unauthorized access. The Translation Bureau intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

The Chief Executive Officer for the Translation Bureau should:

1. Document, approve and implement access management processes and supporting procedures for every service point where Public Works and Government Services Canada owned Information Technology systems are used in support of translation of classified information. These processes should be compliant with the Treasury Board of Canada Secretariat Security Policy Instruments and Departmental Policies.

   Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following actions:

   Deliverable: Directive (processes and procedures).
   1.1 Identify missing components in the current Translation Bureau framework and procedures by March 2009.
   1.2 Draft the final version of the deliverable by May 2009.
   1.3 Validate the deliverable by July 2009.
   1.4 Draw up a communications plan by May 2009.
   1.5 Obtain final approval of the Translation Bureau Chief Executive Officer by August 2009.
   1.6 Implement the communications plan by August 2009.

2. Develop a process to govern the disposal of classified information entrusted to the Translation Bureau and processed on Public Works and Government Services Canada owned systems.

   Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following actions:

   Deliverable: Directive (processes and procedures).
   2.1 Identify missing components in the current Translation Bureau framework and procedures by March 2009.
   2.2 Draft the final version of the deliverable by May 2009.
   2.3 Validate the deliverable by July 2009.
   2.4 Draw up a communications plan by May 2009.
   2.5 Obtain final approval of the Translation Bureau Chief Executive Officer by August 2009.
   2.6 Implement the communications plan by August 2009.

3. Certify and accredit Public Works and Government Services Canada owned systems used in support of the translation of classified information by Translation Bureau personnel.

Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following actions:

Deliverable: Certification and accreditation of standard IT solutions used to handle classified information in the Translation Bureau.

3.1 Review actions to be taken as part of the certification process under way with the Information Technology Security Directorate by April 2009.

3.2 Complete all standardized stages in the process of certifying standard IT solutions used to handle classified information in the Translation Bureau:

- 3.2.1 Confirmation of certification and accreditation procedures according to level of effort by April 2009.
- 3.2.2 Confirmation of the certification plan with the Information Technology Security Directorate by May 2009.
- 3.2.3 Statement of acceptable risks by July 2009.
- 3.2.4 Validation of architecture and design with the Information Technology Security Directorate by October 2009.
- 3.2.5 Validation of security requirements with the Information Technology Security Directorate by February 2010.
- 3.2.6 Report on certification process findings by April 2010.
- 3.2.7 Certification letter issued by the Certification Authority for Translation Bureau's Systems and Applications, namely the Director, Information Technology Security Directorate within the Office of the Chief Information Officer Sector within the Information Technology Services Branch, by June 2010.

3.3 Final approval of the accreditation letter by the Accreditation Authority for Translation Bureau's Systems and Applications, namely the Chief Executive Officer for the Translation Bureau, by June 2010.

Management Response

Human Resources Branch considers that the results of the Audit accurately and fairly reflect the state of the management control framework in place to protect the Human Resources Management System against unauthorized access. The Human Resources Branch intends to act on the recommendation of the audit by implementing a Management Action Plan, detailed as follows.

The Assistant Deputy Minister for the Human Resources Branch should:

1. Address all outstanding recommendations related to access management contained in the Threat and Risk Assessment dated 2007-12-20.

Human Resources Branch's Response. The Human Resources Branch accepts the recommendation and will be taking the following actions:

1.1 In order to address the first Threat and Risk Recommendation (Consider Data transfer encryption to improve security), the Human Resources Branch will enter into a written agreement with the Information Technology Services Branch to ensure that Protected B data transmitted between the Human Resources Management System and other PWGSC Systems is encrypted. This action will be completed by March 31, 2009.

1.2 The Human Resources Branch will track progress against the written agreement until all interfaces between the Human Resources Management System and other PWGSC Systems, and between the two components identified in the Threat and Risk Assessment are modified to ensure that Protected B data transmitted is encrypted. This action will be completed by March 31st, 2010.

1.3 As of Fall 2008, the intention was to migrate to PeopleSoft, including all Human Resources Management System historical data. However, due to lack of funding, the project has been delayed and, the decision to not migrate all historical data has been made based on a more cost efficient approach. Therefore, to address the second Threat and Risk Recommendation related to access management (Consider moving to [the appropriate] Protected hosting environment), the Human Resources Branch will enter into a written agreement with Information Technology Services Branch to ensure that the Human Resources Management System is hosted in an appropriate environment managed by the Information Technology Services Branch. This action will be completed by June 30th, 2009.

1.4 The Human Resources Branch will track progress against the written agreement until the work required to host the Human Resources Management System in an appropriate environment is completed. This action will be completed by March 31, 2011.

INTRODUCTION

1. Access management is intended to ensure that only authorized individuals can access information technology (IT) resources and information on a need-to-know basis. These individuals should have the appropriate security level and be authenticated prior to being given access to the IT resources and information.

2. The objectives of the 2002 *Government Security Policy (GSP)* are to protect employees; to preserve the confidentiality, integrity, availability and value of assets; and to ensure the continued delivery of services. Since the Government of Canada relies extensively on information technology (IT) to provide its services, this policy emphasizes the need for departments to monitor their electronic operations.

3. The Management of Information Technology Security (MITS) standard supports the GSP by defining baseline security requirements that Federal Government departments must fulfill to ensure the security of information and IT assets under their control. MITS provides direction on the organization and management of IT security within departments, including a description of management controls, as well as technical and operational safeguards that support these controls.

4. The main departmental policies and standards that deal with IT access management are:

   - Departmental Policy (DP) 055 - Information Technology (IT) Security Program
   - DP 029 - Employees Leaving PWGSC
   - PWGSC IT Security Standards

5. Public Works and Government Services Canada (PWGSC) manages over 400 business applications and supporting systems. Many of these systems store and process sensitive information. Based on a risk analysis, three systems were chosen for this audit: two systems used by the Translation Bureau in support of the translation of classified documents as well as the Human Resources Management System (HRMS).

6. The Translation Bureau provides services to its customers through some 60-service points located in the National Capital Region and throughout Canada. The audit examined two different systems used by the Translation Bureau in support of the translation of classified documents at two service points. In this report, these systems are referred to as “Secret Document Processing Solutions” or “Solutions” and the two service points examined by the audit are referred to as service point A and service point B. Solutions used in both service points rely on stand alone Personal Computers not connected to the Internet or to the PWGSC Intranet. Conclusions drawn on the systems examined cannot be applied to other systems as different service points use different systems. However, the Translation Bureau intends to deploy the Solution

examined in service point A to other service points where classified information is translated.

7. The Human Resources Management System (HRMS) is used by the Human Resources Branch to manage employee and position information for PWGSC. This information is used to support Human Resources functions such as classification, compensation, performance review, staffing, official languages, workforce adjustments and employment equity. The HRMS runs on the IT Shared Services (ITSS) infrastructure, which is managed by the Information Technology Services Branch (ITSB).

FOCUS OF THE AUDIT

8. The objective of this internal audit was to assess the adequacy of the management control framework designed to protect against unauthorized access to selected IT systems. Specifically, this audit assessed whether appropriate measures were in place to control and limit access to systems and sensitive information to individuals with formal access approval, requisite security clearance, and the need-to-know.

9. The audit examined access management for three systems: two systems used by the Translation Bureau in support of the translation of classified documents in two service points, and the Human Resources Management System (HRMS).

10. The audit did not examine the physical security protecting the systems or the security of the IT shared services infrastructure.

11. More information on the audit objective, scope, approach and criteria can be found in the “About the Audit” section at the end of the report.

OBSERVATIONS

PWGSC IT SECURITY STANDARDS

Guidance on the use of passwords is inconsistent and not enforced

12. Passwords are one of the key controls used to manage access to IT systems. They are intended to ensure that access to applications and supporting systems is granted only to authorized individuals. Password composition rules dictate the number and type of characters required for given passwords. The more complex the password, the less likely that it will be by-passed.

13. The audit team expected that the department would have clear, consistent and mandatory password composition rules that are supported by departmental systems and applications and consistent with the GSP.

14. The audit team found that one of the password composition rules in the PWGSC IT Security Standards is stated as a good practice and not as a mandatory requirement. In addition, there are contradictions in the direction provided on the PWGSC Intranet regarding password requirements. While PWGSC IT Security Standards state that the "minimum length for a password is eight characters" several other PWGSC documents are inconsistent with the PWGSC IT Security Standards. These include the PWGSC IT Security Awareness course and Security Awareness documents, which indicate that the minimum length for a password is six characters.

15. Password composition rules implemented on applications used by PWGSC employees to access Novell (network access), Outlook (e-mail), the Internet and HRMS, do not enforce the PWGSC IT Security Standards.

16. Without password rules that are clear, consistent and enforced by PWGSC systems and applications, there is a risk of unauthorized access to the information that they protect.

CLASSIFIED SYSTEMS USED BY THE TRANSLATION BUREAU

17. The goal of a management control framework is to ensure that the organization meets its objectives. The management control framework to protect against unauthorized access to IT systems is expected to ensure that access is limited to only individuals who have the appropriate security level, have been authenticated and authorized, and have the need to know.

18. In order to meet these objectives, the management control framework should include multiple controls: Access control guidance should be compliant to the GSP, and supporting documentation should had been developed, disseminated and maintained; a knowledgeable and responsible manager should provide formal access approval to individuals requiring access to sensitive information or assets under the "need-to-know"; access should be limited to individuals who have appropriate security clearance; identification and authentication safeguards should be incorporated into applications and supporting systems; Access privileges should be kept up to date; segregation of responsibility should be reflected in access privileges; and processes should be in place to address unauthorized access.

19. We found the controls mentioned above were not consistently implemented by the Translation Bureau at the two service points examined to protect against unauthorized access to systems used in support of translation of classified information. However, many controls were in place, particularly in service point A. For Service Point A,

access privileges were up to date. However, the procedures to revoke logical access were partially documented. Segregation of duties was implemented through segregation of roles, and processes to address unauthorized access have been documented. For Service Point B, no logical access to the IT Systems has been implemented.

Processes and procedures are not fully documented

20. While a process describes what needs to be done (e.g., the creation of a user account), a procedure describes how it should be done. The requirements stated in a process can be achieved by one or more procedures. Controls are any action taken by management and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

21. By documenting processes, management can communicate the process and ensures that all individuals involved have a common understanding of the process and associated controls. It helps ensure that activities are executed and controlled consistently, even when individuals responsible for activities and controls change. Documented processes also help individuals involved in the process understand the context for specific activities and controls, and therefore, provides information for making appropriate decisions.

22. We expected to find documented processes and procedures to support management of access to the Secret Document Processing Solutions used at Translation Bureau Service Points. To control access to these Solutions, we expected that the responsible managers would approve the creation and modification of user accounts for individuals with the appropriate security clearance using the “need-to-know” principle.

23. We found that the Secret Document Processing Solutions used in the two service points examined were very different. Further, access to these solutions was also managed differently. Although systems were kept in a secured room at service point B, logical access control such as user id and password, had not been implemented. MITS requires that identification and authentication safeguards be incorporated to all systems. In addition, it was found out of a sample of 107 users who had access to the secured room, 10 users did not have the appropriate security clearance

24. At service point A, while logical access control had been implemented, users had the appropriate security clearance and the Solution was supported by a number of documented procedures, the overall processes to create, modify and revoke accounts were not fully documented. As well, the procedures to support regular account reviews, and to ensure the proper identification of individuals to whom a unique identifier is issued, were not documented.

25. A number of controls related to access management are either missing or inconsistently applied in service point A. For instance, the process does not require that a knowledgeable manager approves the creation or modification of user accounts. Certain passwords do not expire within the schedule prescribed by the PWGSC IT Security Standards. In two cases, a privileged account (user name and password) was shared between two people. These accounts allow individuals to perform sensitive activities such as password changes. When accounts are shared, actions may not be attributable to a single person. The PWGSC IT Security Standards requires that each authorized user be uniquely identified.

26. Because of these weaknesses, activities and controls, which support access management, are not being performed consistently in a manner that complies with the GSP.

Lack of processes for the disposal of classified information

27. Information is the cornerstone of a democratic, effective, and accountable government. Information must be well managed throughout its life cycle, including its disposal. We expected that the Translation Bureau had implemented appropriate processes and associated procedures for the retention and disposal of classified information.

28. The Secret Document Processing Operational Procedure used at service point A describes how to use the Secret Document Processing Solution to process classified information. It guides users through the different phases; reception, translation, revision and correction, delivery and storage. This procedure directs users to save a copy of their final document in a special repository folder. However, the procedure does not specify when classified documents should be disposed of, who is responsible for disposal, and how these activities are controlled. Instead, information in the document repository is kept for an undetermined period of time.

29. Because there is no process in place for disposal of classified information, information remains in the repository and is not disposed of in a manner that complies with policies. Because significant amount of classified information could accumulate in one location over time, it increases the risk that PWGSC becomes a target for unauthorized access as well as the potential impact that an unauthorized access could have.

Secret document processing solutions have not been certified and accredited

30. The Government Security Policy states that departments must certify and accredit their IT systems prior to operation. The purpose of certification is to verify that the security requirements identified for a particular system or service are met and that controls and safeguards work as intended. The purpose of accreditation is to signify

that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service. Accreditation is based on the certification process as well as other management considerations.

31. We expected that the Secret Document Processing Solutions at the two service points would have been certified and accredited. This is especially important because classified information up to Secret is being processed on those IT Systems. Furthermore, Translation Bureau has indicated that their goal is to replicate the solution implemented in Service point A to other service points where classified information will be translated. We found that the IT Systems were not certified and accredited. However, the Translation Bureau has taken some steps towards certification and accreditation.

32. Without certification and accreditation, the Translation Bureau in unable to demonstrate that the security controls and safeguards of the systems are sufficient to address the risks of unauthorized access to classified information.

HUMAN RESOURCES MANAGEMENT SYSTEM (HRMS)

33. We found that the management control framework was generally in place and adequate to protect against unauthorized access to the HRMS. During the course of our audit we identified two areas for improvement, one of which has already been addressed. The significance and impact of these observations, along with a recommendation, are described in more detail in the following sections of this audit report.

Two previous recommendations regarding access management have not been implemented

34. Departments must comply with the baseline requirements of the GSP, and must conduct their own Threat and Risk Assessments (TRA) to determine the necessity to incorporate additional requirements above those stated in the GSP.

35. We expected that the Human Resources Branch had taken appropriate steps to ensure that HRMS meets the requirements of GSP. While the branch did complete a TRA, it did not ensure that the two recommendations related to access management, which rely on ITSB for implementation, were addressed. While HRB owns both risks associated with the two recommendations in the TRA, the first risk is shared with other Branches of PWGSC, since all PWGSC Branches use the IT Shared Services Infrastructure. This risk is being mitigated by ITSB as part of achieving MITS compliance for the IT Shared Services Infrastructure. While the second TRA recommendation will ultimately require ITSB to implement a solution to mitigate the risk, this risk is specific to HRB. The risk of unauthorized access to HRMS information remains since the TRA recommendations were not addressed.

Generic user identifications were used for operational reasons

36. A generic user identification (ID) is a user name and password which is shared amongst two or more people. Generic user ID's may be used for operational efficiency when two or more users require a particular functionality. Generic multi-user ID's limit the ability to attribute actions to a particular individual, and make access control to the system more difficult to enforce. The use of generic user ID does not comply with the PWGSC Departmental Policy 055 on Information Technology Security, which indicates that before access to IT systems and information is granted, each user will be assigned a unique user identifier. This is important because it allows the actions to be attributable to an individual, and it facilitates access management.

37. We expected that each HRMS user would have a unique user ID. The audit team found that 4 generic user ID's out of approximately 600 accounts were used for operational reasons. HRMS has stopped using all generic user ID's as of June 2008. This was validated by the audit team, and for this reason, no recommendation has been raised for this observation.

CONCLUSIONS

38. The management control framework in place to protect against unauthorized access to Information Technology (IT) systems, used and owned by the Translation Bureau, in support of translation of classified information is not adequate. While some measures were in place to control access to IT Systems, these measures were insufficient to limit access to systems and classified information to individuals with the requisite security clearance, formal access approval and the need to know.

39. We found that the management control framework was generally in place and adequate to protect against unauthorized access to the Human Resources Management System (HRMS). However, there are two Threat and Risk Assessment (TRA) recommendations related to access management, which need to be addressed.

RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

Management Response

40. Information Technology Services Branch considers that the results of the Audit accurately and fairly reflect the guidance on the use of passwords in Public Works Government Services Canada. The Information Technology Services Branch intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

41. The Chief Executive Officer of Information Technology Services Branch should:

1. Update the Public Works and Government Services Canada Information Technology Security policy instruments and user guidance to ensure consistency amongst policy instruments and user guidance.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

   1.1 ITSB will identify the PWGSC Information Technology Security policy instruments and user guidance that are impacted by this audit. This action will be completed by March 30, 2009.
   1.2 ITSB will validate the information to ensure consistency and update policy instruments and user guidance as required. This action will be completed by June 30, 2009.
   1.3 ITSB will seek departmental approval for policy instruments that need to be updated as required. This action will be completed by Sept 30, 2009.

2. Update the Public Works and Government Services Canada Information Technology Security Standards to ensure that password rules reflect inherent risks based on documented criteria and are stated as mandatory requirements.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

   2.1 ITSB will review current document IT Security Standards password rules in light of inherent risk, and state password rules as mandatory requirements. The coming into force of the revised password rules will reflect inherent risks. This action will be completed by June 30th, 2009.
   2.2 Seek departmental approval for the IT Security Standards password rules. This action will be completed by September 30, 2009.
   2.3 Publish Security Standards documentation related to password rules. This action will be completed by November 30th, 2009.

3. Enforce compliance with the Public Works and Government Services Canada Information Technology Security Standards for all Public Works and Government Services Canada Information Technology systems and applications managed by the Information Technology Services Branch.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

3.1 ITSB will conduct a gap analysis to evaluate retrofit work required to implement updated password rules, by August 30th, 2009.
3.2 ITSB will prepare and present a business case to the Chief Financial Officer to obtain departmental approval for the most appropriate and cost-effective approach towards the implementation of the new password rules. This action will be completed by September 30th, 2009.
3.3 Upon approval of the most cost-effective approach towards the implementation of the new password rules, and commensurate with the approved funding, ITSB will implement the new password rules. This action will be completed by December 31st, 2010.
3.4 Service Management & Delivery (SM&D), Application Management and IT Operational Services (AMITOS), and PWGSC Branches will report their compliance on a periodic basis to the Office of the Chief Information Officer (OCIO). The OCIO will report the status of compliance to the Departmental IM/IT Steering Committee on a periodic basis. This action will be completed by November 30th, 2009

Management Response

42. Translation Bureau considers that the results of the Audit accurately and fairly reflect the state of the management control framework in place to protect Information Technology Systems used in support of translation of classified information against unauthorized access. The Translation Bureau intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

43. The Chief Executive Officer for the Translation Bureau should:

1. Document, approve and implement access management processes and supporting procedures for every service point where Public Works and Government Services Canada owned Information Technology systems are used in support of translation of classified information. These processes should be compliant with the Treasury Board of Canada Secretariat Security Policy Instruments and Departmental Policies.

   Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following action:

   Deliverable: Directive (processes and procedures).
   1.1 Identify missing components in the current Translation Bureau framework and procedures by March 2009.
   1.2 Draft the final version of the deliverable by May 2009.
   1.3 Validate the deliverable by July 2009.
   1.4 Draw up a communications plan by May 2009.
   1.5 Obtain final approval of the Translation Bureau Chief Executive Officer by August 2009.

1.6 Implement the communications plan by August 2009.

2. Develop a process to govern the disposal of classified information entrusted to the Translation Bureau and processed on Public Works and Government Services Canada owned systems.

   Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following actions:

   Deliverable: Directive (processes and procedures).
   2.1 Identify missing components in the current Translation Bureau framework and procedures by March 2009.
   2.2 Draft the final version of the deliverable by May 2009.
   2.3 Validate the deliverable by July 2009.
   2.4 Draw up a communications plan by May 2009.
   2.5 Obtain final approval of the Translation Bureau Chief Executive Officer by August 2009.
   2.6 Implement the communications plan by August 2009.

3. Certify and accredit Public Works and Government Services Canada owned systems used in support of the translation of classified information by Translation Bureau personnel.

   Translation Bureau's response. The Translation Bureau accepts the recommendation and will be taking the following actions:

   Deliverable: Certification and accreditation of standard IT solutions used to handle classified information in the Translation Bureau.
   3.1 Review actions to be taken as part of the certification process under way with the Information Technology Security Directorate by April 2009.
   3.2 Complete all standardized stages in the process of certifying standard IT solutions used to handle classified information in the Translation Bureau:
   3.2.1 Confirmation of certification and accreditation procedures according to level of effort by April 2009.
   3.2.2 Confirmation of the certification plan with the Information Technology Security Directorate by May 2009.
   3.2.3 Statement of acceptable risks by July 2009.
   3.2.4 Validation of architecture and design with the Information Technology Security Directorate by October 2009.
   3.2.5 Validation of security requirements with the Information Technology Security Directorate by February 2010.
   3.2.6 Report on certification process findings by April 2010.
   3.2.7 Certification letter issued by the Certification Authority for Translation Bureau's Systems and Applications, namely the Director, Information Technology Security Directorate within

the Office of the Chief Information Officer Sector within the Information Technology Services Branch, by June 2010.

3.3 Final approval of the accreditation letter by the Accreditation Authority for Translation Bureau's Systems and Applications, namely the Chief Executive Officer for the Translation Bureau, by June 2010.

Management Response

44. Human Resources Branch considers that the results of the Audit accurately and fairly reflect the state of the management control framework in place to protect the Human Resources Management System against unauthorized access. The Human Resources Branch intends to act on the recommendation of the audit by implementing a Management Action Plan, detailed as follows.

45. The Assistant Deputy Minister for the Human Resources Branch should:

1. Address all outstanding recommendations related to access management contained in the Threat and Risk Assessment dated 2007-12-20.

   Human Resources Branch's Response. The Human Resources Branch accepts the recommendation and will be taking the following actions:

   1.1 In order to address the first Threat and Risk Recommendation (Consider Data transfer encryption to improve security), the Human Resources Branch will enter into a written agreement with the Information Technology Services Branch to ensure that Protected B data transmitted between the Human Resources Management System and other PWGSC Systems is encrypted. This action will be completed by March 31, 2009.

   1.2 The Human Resources Branch will track progress against the written agreement until all interfaces between the Human Resources Management System and other PWGSC Systems, and between the two components identified in the Threat and Risk Assessment are modified to ensure that Protected B data transmitted is encrypted. This action will be completed by March 31st, 2010.

   1.3 As of Fall 2008, the intention was to migrate to PeopleSoft, including all Human Resources Management System historical data. However, due to lack of funding, the project has been delayed and, the decision to not migrate all historical data has been made based on a more cost efficient approach. Therefore, to address the second Threat and Risk Recommendation related to access management (Consider moving to [the appropriate] Protected hosting environment), the Human Resources Branch will enter into a written agreement with Information Technology Services Branch to ensure that the Human Resources Management System is hosted in an appropriate environment managed by the Information Technology Services Branch. This action will be completed by June 30th, 2009.

1.4 The Human Resources Branch will track progress against the written agreement until the work required to host the Human Resources Management System in an appropriate environment is completed. This action will be completed by March 31, 2011.

ABOUT THE AUDIT

Authority

The audit was approved by the department’s Audit and Evaluation Committee as part of the 2008-2009 Internal Audit plan.

Objectives

The objective of this internal audit was to assess the adequacy of the management control framework designed to protect against unauthorized access to selected IT systems.

Specifically, this audit assessed whether appropriate measures were in place to control and limit access to systems and sensitive information to individuals with formal access approval, requisite security clearance, and the need to know

Scope and Approach

This audit was conducted from February 2008 to July 2008.

The audit scope included the access management of the systems used in two service points in support of the translation of classified documents by the Translation Bureau; and the Human Resources Management System (HRMS).

The audit did not examine the physical security protecting the systems or the security of the IT shared services infrastructure.

Interviews were conducted with key personnel. Relevant processes and documentation were reviewed. Based on analysis of the information and evidence collected, the audit team prepared audit findings and conclusions, which were validated with the appropriate managers prior to tabling the Draft Final Report at the PWGSC Audit and Evaluation Committee.

The audit was conducted in accordance with the TB *Policy on Internal Audit* and the Internal Auditing Standards for the Government of Canada

Criteria

The criteria for the performance of this audit were developed based on the *Government Security Policy (GSP)* and on the *Management of Information Technology Security (MITS)* standard.

The following audit criteria were used for this audit:

a) Access control guidance is compliant with the Government Security Policy and supporting documentation (standards, directives, guidelines and procedures) has been developed, disseminated and maintained.

b) Access to applications and supporting systems is granted only to individuals who have appropriate security clearance.

c) A knowledgeable and responsible manager has given formal access approval to the individual requiring access to sensitive information or assets under the "least privilege principle".

d) Access identification and authentication safeguards have been incorporated into applications and supporting systems according to the level of risk for the application or the supporting systems.

e) Access privileges are regularly updated to accurately reflect the current responsibilities of the individual; they are revised when individuals move to jobs that do not require the same level of access, and are withdrawn from individuals who leave the organization.

f) Segregation of responsibilities is reflected in access privileges; no one individual can independently control all aspects of a process or a system; individuals who are authorized to conduct sensitive operations must not be allowed to audit these operations.

g) Processes are in place to ensure that unauthorized accesses are detected, investigated, actions are taken to minimize impact, and appropriate administrative, corrective or disciplinary action is taken.

Audit Work Completed

The fieldwork for this audit was substantially completed on July 8, 2008.

Audit Team

The audit was conducted by one member of the Office of Audit and Evaluation and one consultant overseen by the Director, IT Audit and under the overall direction of the Chief Audit Executive, Office of Audit and Evaluation. An additional consultant under the supervision of the Director, IT Audit assisted in the drafting of the audit report.

The engagement was reviewed by the Quality Assessment function of the Office of Audit and Evaluation.