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

Canada

Respect • Integrity • Excellence • Leadership

Serving GOVERNMENT, Serving CANADIANS.

Final Report

2009-714

Audit of PWGSC's Compliance with Selected Management of Information Technology Security Standard Requirements

September 8, 2011

Office of Audit and Evaluation

www.pwgsc-tpsgc.gc.ca

TABLE OF CONTENTS

MAIN POINTS

What we examined

i. The *February 2002 Government Security Policy (replaced in 2009 by the Policy on Government Security)* sets out the baseline requirements for safeguarding employees and assets and assuring the continued delivery of services. The Treasury Board of Canada Secretariat augmented this Policy by issuing security directives and operational security standards. One of these standards, the 2004 Management of Information Technology Security Standard (MITS) required full Departmental compliance by December 31, 2006.

ii. We examined compliance with those MITS elements deemed by the Office of Audit and Evaluation to be high risk to the Department. More specifically, we examined the compliance of selected portions of six critical information technology (IT) systems located in the National Capital Region that support critical services. The systems selected for this audit were the: Project and Business Management System; SIGMA; Canada Gazette Production System; Living Disaster Recovery Planning System; Enterprise Document and Records Management System; and, Departmental Industrial Security Information System.

iii. Even though the audit focused exclusively on the above-mentioned systems, we anticipate the results of this audit will serve to improve the security of all departmental IT systems. Consequently, we expect that the scope of the actions contained in the Management Action Plan prepared in response to the audit recommendations will include all departmental critical IT systems and not just the six systems examined during the audit.

Why it is important

iv. IT security is an integral part of a continuous program and service delivery. Sound IT security can prevent the loss of service as a result of IT security breaches. The MITS Standard defines baseline security requirements that federal departments must meet to ensure the security of information and information technology assets under their control.

v. In March 2005 the Office of the Auditor General (OAG) expressed concerns about IT security throughout the federal government. The OAG indicated that senior management is not aware of IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government. The OAG also stated that the majority of the departments do not meet minimum IT security standards. In October

2005, the Treasury Board Secretariat stated that the MITS standard is key to the Government of Canada's efforts to improve IT security.

vi. Departments were required to report a self-assessment of their compliance against the MITS Standard to TBS in 2005, and again in 2006. Subsequently, TBS incorporated their assessment of departmental compliance against the MITS Standard as part of the annual Management Accountability Framework (MAF) process.

What we found

vii. We found that vulnerability assessments were conducted regularly on the IT infrastructure of the critical IT systems accessible from outside PWGSC. Vulnerability assessments conducted on the internally accessible components of critical IT systems were performed only if the owner of the critical IT system specifically requests it and were not done on a regular basis. Five of the six critical systems selected for this audit were only accessible from within PWGSC. We also noted that no formal procedures existed to ensure identified vulnerabilities were addressed and to monitor the implementation of such actions.

viii. However, we found that four of the six critical IT systems that were selected had an approved patch management process to ensure security-related patches were applied in a timely-manner.

ix. We noted that five of the six critical IT systems tested had good segregation of duties to prevent unauthorized changes to the systems and/or the databases and servers.

x. Finally, we found that security audit log files were produced and reviewed in four of the six critical IT systems that we examined.

Management Response

The Information Technology Services Branch (ITSB) has reviewed the audit report and accepts the recommendations found therein. ITSB has developed a Management Action Plan to ensure that the audit recommendations are fully addressed.

Management acknowledges the Audit report's conclusions, and would like it noted that ITSB refers to the PWGSC's Business Continuity and Critical IT (BCCIT) Report of 2010 as the definitive record of the department's critical systems.

Management has already addressed many of the findings and recommendations contained in the audit report. The completion of the BCCIT Vulnerability Assessment that identified key dependencies between critical services and their IT systems is one example of the work accomplished by ITSB. Management has also increased the number of Vulnerability Assessments performed on external interfaces and has improved processes to monitor and apply corrective measures to vulnerabilities discovered during the Vulnerability Assessments. Finally, the Departmental Industrial Security Information System (DISIS) has since been migrated to an ITSB managed data center and is now supported with the same rigor as the other critical systems.

Recommendation 1: The Chief Information Officer, Information Technology Services Branch should implement mechanisms to ensure that all highly sensitive or highly exposed IT systems supported by ITSB are subjected to regularly scheduled vulnerability assessments and identified vulnerabilities are formally monitored and corrected.

> **Management Action Plan 1.1:** Define a vulnerability assessment standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.
>
> **Management Action Plan 1.2:** Identify gaps and, review the process to meet the defined standard for systems identified in 1.1.
>
> **Management Action Plan 1.3:** Implement the process and identify corrective measure requirements to meet the vulnerability assessment standard for systems identified in 1.1.
>
> **Management Action Plan 1.4:** Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 2: The Chief Information Officer, Information Technology Services Branch should examine the patch management process of all critical IT systems supported by ITSB and work with responsible Assistant Deputy Ministers to ensure appropriate system patches are applied.

> **Management Action Plan 2.1:** Define a patch management standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.
>
> **Management Action Plan 2.2:** Identify gaps against the defined standard for systems identified in 2.1.

Management Action Plan 2.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 2.4: Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 3: The Chief Information Officer, Information Technology Services Branch should examine segregation of duties in all critical IT systems supported by ITSB and work with responsible Assistant Deputy Ministers to address concerns with conflicting responsibilities.

Management Action Plan 3.1: Define a segregation of duties standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 3.2: Identify gaps against the defined standard for systems identified in 3.1.

Management Action Plan 3.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 3.4: Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 4: The Chief Information Officer, Information Technology Services Branch should examine the security audit log functions in all critical IT systems supported by ITSB and work with appropriate Assistant Deputy Ministers to address identified deficiencies in the LDRPS and DISIS systems.

Management Action Plan 4.1: Define a standard, including a schedule for ongoing reviews, for monitoring security audit logs in all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 4.2: Identify gaps against the defined standard for systems identified in 4.1.

Management Action Plan 4.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 4.4: Provide compliance reports against the standard to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 5: In line with the requirements of PWGSC Policy on IT Security (DP104), the Chief Information Officer, Information Technology Services Branch should provide functional guidance to Assistant Deputy Ministers to ensure proper IT security of all departmental systems not supported by ITSB, including guidance to ensure requirements related to vulnerability assessments, patch management, segregation of duties and security audit logs are met.

Management Action Plan 5.1: Provide functional guidance to ADMs/RDGs by communicating Branch/Regional responsibilities for MITS to the Departmental Security Committee.

Management Action Plan 5.2: Provide the PWGSC standards (developed in 1.1, 2.1, 3.1, 4.1), to relevant ADMs/RDGs for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems not supported by ITSB and request that they comply with these standards.

Management Action Plan 5.3: Instruct ADMs/RDGs to monitor and confirm compliance against the PWGSC standards (defined in 1.1, 2.1, 3.1, 4.1) by requesting they report to the IT Security Coordinator. Included in the reports, are the activities defined to address gaps on a non-compliance status.

Management Action Plan 5.4: Identified action plans in 5.3 are monitored and reported to the CIO on an ongoing basis commencing in March 2012.

INTRODUCTION

1. The *Policy on Government Security* provides requirements for protecting government assets, including information, and directs federal departments and agencies to which the policy applies to establish an IT security strategy. The *Policy on Information Management* requires that information and records be managed as valuable assets. The *Management of Information Technology Security (MITS)* standard expands upon the requirements of both policies.

2. The MITS standard defines the baseline security requirements that federal departments must meet. These requirements include elements such as the management of vulnerabilities to programs, systems and services; the discovery of threats and the implementation of corresponding solutions; the management of patches, which involves acquiring, testing, and installing software fixes; the segregation of duties; and the maintenance of a security audit log to record activities related to the security, integrity and availability of a system. The MITS standard promotes a risk management philosophy whereby the specific implementation of the baseline requirements and additional safeguards should be determined using a risk-based approach.

3. For the purposes of the MITS standard, the term 'IT security' refers to the safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

4. Although program and service delivery managers may delegate responsibility for IT security to technical experts, they remain accountable to the Deputy Head and are responsible for ensuring the security of the programs and services under their authority. In PWGSC, the implementation of IT Security has been delegated to the Director, Information Technology Security Directorate (DITSD) within the Information Technology Services Branch (ITSB). Other sectors of ITSB are also impacted by the MITS standard.

5. The PWGSC *Policy on Information Technology Security (DP104)* published in July 2010 ensures the security of departmental electronic information, IT assets and related services. The policy provides a common understanding on the part of all key departmental stakeholders of their roles, responsibilities and obligations with respect to IT security. The policy was developed in support of the Departmental IT Security Program and should be read in conjunction with the MITS standard. The policy assigns overall responsibility for the Departmental IT Security Program to the Information Technology Services Branch (ITSB) while Branch Heads are responsible for providing

and ensuring adequate funding for regular and frequent review of their systems IT security requirements.

6. ITSB provides Information Management (IM)/Information Technology (IT) support to approximately 80% of the IT systems in PWGSC. ITSB does not own, operate and support all IT systems in the department since some branches choose to develop and operate their own systems without the involvement of ITSB. Two sectors within ITSB are responsible for IT operations and IT services. AM&ITOS provides operational support of applications and infrastructure for PWGSC. The IT infrastructure itself is obtained from and supported by SM&D.

7. The Application Management and IT Operational Services (AM&ITOS) Sector is the operating arm for the internal services for ITSB. AM&ITOS performs functions such as system integration and software application development and maintenance in order to support other PWGSC branches/regions in the delivery of their programs and services." AM&ITOS provides Web application development and application management services to shared systems, and develops niche application services. IT security is an integral part of continuous program and service delivery as performed by AM&ITOS.

8. The Service Management and Delivery (SM&D) sector provides mainframe, mid-range computing, office desktops and Local Area Network (LAN) automation services. SM&D also provides business continuity, disaster recovery, printing and distribution services. These services are also subject to the MITS standard.

9. The increased availability of common and shared services can help PWGSC and its clients meet their security requirements. While this offers the potential for improved efficiency, PWGSC recognizes that the security decisions it makes can impact other organizations.

10. Appendix A provides a glossary of the key terms used in this audit report.

FOCUS OF THE AUDIT

11. The objective of this audit is to determine whether PWGSC complies with selected *Management of Information Technology Security (MITS)* standard requirements for selected portions of critical IT systems that support critical services.

12. The scope of the audit covers four key requirements of the MITS standard. They are:

- *Vulnerability management:* Continuously manage threats to programs, systems and services. This management task includes the discovery of threats and the implementation of corresponding solutions.
- *Patch management:* Acquire, test, and install software fixes on an administered IT system.
- *Segregation of duties:* Separation of responsibilities related to an IT system or business function to avoid situations where a single individual can make a system vulnerable to undetected abuse.
- *Security audit log:* Maintain records of activities related to the security, integrity and availability of a system.

13. These four requirements were selected because they were deemed by the Office of Audit and Evaluation to be of higher risk to the Department.

14. For this audit, portions of six critical IT systems were selected for testing. We have defined critical IT systems as the systems that were in place to support a critical business function or a critical service as defined in the March 9, 2010 PWGSC Business Impact Analysis Summary Report. These six systems are located in the National Capital Region and were selected because they support many Tier 1 critical services, which need to be recovered within 72 hours. The six critical IT systems selected were:

    - Project and Business Management System (PBMS) from Real Property Branch;
    - SIGMA from Finance Branch (PWGSC's financial management and materiel management system);
    - Canada Gazette Production System from Consulting, Information and Shared Services Branch (CISSB);
    - Living Disaster Recovery Planning System (LDRPS) from Corporate Services and Strategic Policy Branch (CSSPB);
    - Enterprise Document and Records Management System (EDRMS) from CSSPB; and,
    - Departmental Industrial Security Information System (DISIS) from CISSB.

15. Even though the audit focused exclusively on the above-mentioned systems, we anticipate the results of this audit will serve to improve the security of all departmental IT systems. Consequently, we expect that the scope of the actions contained in the Management Action Plan prepared in response to the audit recommendations will include all departmental critical IT systems and not just the six systems examined during the audit.

16. The audit did not examine MITS standard requirements related to the protection of classified information, as these are examined in PWGSC's Audit of Classified Information Processed Electronically. In addition, we did not examine the integrity of the data contained within the systems as no access to system or application code was requested.

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

STATEMENT OF ASSURANCE

18. This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

19. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the findings and conclusions in this report and to provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

OBSERVATIONS

VULNERABILITY ASSESSMENTS

Vulnerability assessments not always conducted on a regular basis

20. A vulnerability assessment is a process that is used to identify potential threats in existing IT systems. Vulnerabilities are weaknesses, which may allow an individual to successfully attack an IT system. The MITS standard requires that departments conduct vulnerability assessments regularly on highly sensitive or highly exposed systems, and on a discretionary basis on other systems.

21. Vulnerability assessments are important because they are used to identify, quantify and prioritize the threats to an IT system. Based upon the information contained within vulnerability assessments, departments are able to identify solutions to the identified threats.

22. We expected that PWGSC would have conducted regular vulnerability assessments on highly sensitive or highly exposed IT systems accessible from within and from outside PWGSC as required by the MITS standard. According to the Treasury Board Secretariat, the term "regular" refers to a set schedule (for example; weekly, monthly, quarterly, etc.) based on a risk assessment conducted on the system.

23. We also expected to find that if a vulnerability assessment could not be performed at the application level, then one would be conducted at an IT infrastructure level (at the IP address level). This would require knowing all the IP addresses for each application in the department.

24. We found that vulnerability assessments were conducted regularly on the IT infrastructure of the critical IT systems accessible from outside PWGSC. Vulnerability assessments conducted on the internally accessible components of critical IT systems were performed only if the owner of the critical IT system specifically requests it and were not done on a regular basis. Five of the six critical systems selected for this audit were only accessible from within PWGSC.

25. According to the Information Systems Audit and Control Association (ISACA), upwards of 80% of all malicious activities originate from current or former employees. The Office of Audit and Evaluation did not test for malicious activities and found no evidence of malicious activities from current or former PWGSC employees. However the risk that vulnerabilities may be undetected increases when internal components of critical IT systems are not assessed on a regular basis. This weakness could lead to unauthorized access to critical IT systems via internal PWGSC networks.

26. We also found that vulnerability assessments were done at the IT infrastructure level (at the IP address level). However, at the time of the audit ITSB was only able to provide the IP addresses for four of the six critical systems examined. Therefore we were unable to determine whether vulnerability assessments were conducted on the two remaining critical systems. The IP addresses of all six critical systems examined was provided subsequent to the audit examination period and vulnerability assessments had not been conducted on the two remaining systems.

27. Conducting vulnerability assessments at the IT infrastructure level (at the IP address level) provides some assurance that vulnerabilities exposed to the public are discovered and corrected. However these assessments do not provide assurance for the system as a whole given that a system can reside on several different servers with each server having

a different IP address. Therefore if only one IP address is tested and the remaining IP addresses are not tested then the system, as a whole, was not properly assessed.

28. Regular and comprehensive vulnerability assessments help ensure threats are identified in a timely manner.

Management actions resulting from vulnerability assessments not formally monitored

29. Upon completion of the vulnerability assessments, management action plans are developed to address identified risks and threats. Monitoring of management actions to ensure their implementation includes reporting on mitigation strategies used to reduce exposure to potential weaknesses or accept the risks and threats identified in vulnerability assessments.

30. Monitoring is important because without it PWGSC does not know whether identified risks and threats are being addressed to reduce the exposure to potential weaknesses.

31. The MITS standard requires that departments document vulnerability assessments, subsequent decisions and remedial actions.

32. We expected that the risks and threats identified in vulnerability assessments would be addressed and the implementation of resulting actions would be formally monitored to ensure their full implementation to reduce system exposure.

33. We found that there was no formal procedure for system administrators to respond to follow-up on vulnerability assessment findings. For example, we reviewed six vulnerability assessment reports with a combined total of 26 high-risk vulnerabilities. We found evidence of mitigating activities against nine of the 26 high- risk vulnerabilities identified in the six reports. The nine high-risk vulnerabilities for which mitigation activities had been undertaken were contained in two of the six vulnerability assessment reports. The mitigating activities for the nine high-risk vulnerabilities were found mostly in emails between the system administrator and ITSB security operations. Only some of those mitigating activities were formally documented. We found no evidence of a formal follow-up process with system administrators to ensure all identified high-risk vulnerabilities were resolved. Similarly, the vulnerability assessment on SIGMA, dated March 2008, identified three high-risk and three medium–risk vulnerabilities. Although the Certification Report for SIGMA referenced the vulnerability assessment report, we found no evidence that the identified vulnerabilities were addressed.

34. A follow-up process is important to help ensure identified threats are addressed. Failure to address identified threats could leave critical systems vulnerable.

PATCH MANAGEMENT

Documented patch management process generally followed by PWGSC

35. Patch management is a component of the change management process, involving the acquiring, testing, and installing of software fixes on an IT system. A patch is a piece of software designed to fix security problems, bugs and improve the usability or performance of a computer program, operating system or its supporting data.

36. The main objective of patch management is to create a consistently configured environment that is secure against known threats in operating system and application software, and to ensure that security-related patches are applied in a timely manner. Failure to promptly apply security-related patches that correct new vulnerabilities can lead to serious IT security incidents.

37. We expected that PWGSC would follow the MITS standard by establishing a systematic, documented patch management process and ensure that all critical IT systems have had the latest security-related patches applied to them. We also expected to find that the IT Security Coordinator ensures that this process is effective and is being followed.

38. We found that four of the six critical IT systems that were selected had an approved patch management process to ensure security-related patches were applied in a timely-manner. These applications followed the established SM&D patch management process, which identifies the steps/tasks to be undertaken to implement a patch.

39. The fifth critical IT system that was selected, the Departmental Industrial Security Information System (DISIS), followed a patch management process, however, this process had not been formally approved. An approved patch management process helps ensure that patches are effectively managed and implemented and security vulnerabilities are resolved.

40. For the sixth critical IT system, the Living Disaster Recovery Planning System (LDRPS), we could not assess the patch management process because patches were not available for the heavily customized version of the system used by PWGSC. This customization has resulted in the PWGSC version of LDRPS differing significantly from the version sold commercially. While patches are available for the commercial version of LDRPS,

PWGSC has not been able to install any patches from the vendor due to the Department's customization. Furthermore, the PWGSC version of LDRPS is old and is no longer supported by the vendor.

41. Given that no patches have been applied to the LDRPS system, the department may be exposed to the risk of having the system fail or/and facing a security violation.

SEGREGATION OF DUTIES

Segregation of duties respected in most cases

42. Segregation of duties occurs when more than one person is required to complete a task. It involves separating certain areas of responsibility and duties in an effort to reduce fraud and unintentional mistakes.

43. Segregation of duties is a basic internal control employed when conflicting responsibilities related to an IT system or business function assigned to one individual can render a system vulnerable to undetected abuse or a single point of failure. For example, an ITSB application developer should not be able to approve his/her final testing results since he/she could hide unauthorized changes within the application. Having an independent verification of final testing results provides reasonable assurance that only authorized changes have been made to an application.

44. We expected that PWGSC segregated IT responsibilities to ensure that no single person has full control of an entire IT system or a major operational function. Individuals who are authorized to conduct sensitive operations must not be responsible for verifying these operations.

45. We found that five of the six IT critical systems tested had proper segregation of duties to prevent unauthorized changes to the systems, databases, and/or the servers.

46. However, we found four individuals within AM&ITOS that had "System Manager" capabilities (access rights) to DISIS. These individuals had complete access to all the DISIS system commands and to restricted functions within the DISIS system.

47. With complete access to DISIS production servers, these individuals could modify the program code within the DISIS system, modify the DISIS database(s) and also grant and remove access to any user or system administrator. Since there were no audit log capabilities identifying who logged onto the DISIS system (see security audit logs section

below) unauthorized and undetected modification could be made to the data contained within DISIS, including the DISIS system code.

SECURITY AUDIT LOGS

Security audit logs monitored for most critical systems

48. An audit log is a record of transactions in an IT system that provides verification of the activity of the system. A security audit log is a subset of an audit log that focuses on activities related to the security, integrity and availability of the system.

49. A security audit log maintains a record of security-related activities including the identification and recording of unauthorized access and unauthorized transactions in a critical system. Such a log is required as part of the MITS standard.

50. We expected all critical IT systems in PWGSC to include a security audit log function that captured events that might indicate attempted and potential security breaches as well as any problems related to the integrity and availability of the system.

51. We found that security audit logs were generated and reviewed in four of the six IT critical systems we examined. For LDRPS, we found that a security audit log was in use but it was not reviewed. We could not determine who was responsible for reviewing the security audit log files for LDRPS. Security audit logs should be reviewed on a regular basis.

52. Although security audit logging is available in DISIS, we found that it was not enabled because of application performance problems. However, if a particular problem were to occur, security audit logging could be enabled for a short period of time.

53. Enabling and reviewing security audit logs would help ensure security breaches for LDRPS and DISIS get detected.

CONCLUSION

54. Overall, we found that PWGSC complied with most of the selected MITS Standard requirements for the majority of the six critical IT systems selected. However, we noted some areas for improvements. We found that PWGSC did not always conduct vulnerability assessments regularly nor were corrective actions formally monitored on the systems selected for this audit.

55. We also found that PWGSC had established a systematic, documented patch management process to ensure that security-related patches are applied in a timely manner. We also noted that overall mechanisms over segregation of duties were adequate in five of the six systems selected for this audit.

56. Finally, we noted that security audit logs were enabled and were reviewed for potential breaches in four of the six systems selected for this audit.

MANAGEMENT RESPONSE

The Information Technology Services Branch (ITSB) has reviewed the audit report and accepts the recommendations found therein. ITSB has developed a Management Action Plan to ensure that the audit recommendations are fully addressed.

Management acknowledges the Audit report's conclusions, and would like it noted that ITSB refers to the PWGSC's Business Continuity and Critical IT (BCCIT) Report of 2010 as the definitive record of the department's critical systems.

Management has already addressed many of the findings and recommendations contained in the audit report. The completion of the BCCIT Vulnerability Assessment that identified key dependencies between critical services and their IT systems is one example of the work accomplished by ITSB. Management has also increased the number of Vulnerability Assessments performed on external interfaces and has improved processes to monitor and apply corrective measures to vulnerabilities discovered during the Vulnerability Assessments. Finally, the Departmental Industrial Security Information System (DISIS) has since been migrated to an ITSB managed data center and is now supported with the same rigor as the other critical systems.

RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

Recommendation 1: The Chief Information Officer, Information Technology Services Branch should implement mechanisms to ensure that all highly sensitive or highly exposed IT systems supported by ITSB are subjected to regularly scheduled vulnerability assessments and identified vulnerabilities are formally monitored and corrected.

> **Management Action Plan 1.1:** Define a vulnerability assessment standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 1.2: Identify gaps and, review the process to meet the defined standard for systems identified in 1.1.

Management Action Plan 1.3: Implement the process and identify corrective measure requirements to meet the vulnerability assessment standard for systems identified in 1.1.

Management Action Plan 1.4: Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 2: The Chief Information Officer, Information Technology Services Branch should examine the patch management process of all critical IT systems supported by ITSB and work with responsible Assistant Deputy Ministers to ensure appropriate system patches are applied.

Management Action Plan 2.1: Define a patch management standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 2.2: Identify gaps against the defined standard for systems identified in 2.1.

Management Action Plan 2.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 2.4: Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 3: The Chief Information Officer, Information Technology Services Branch should examine segregation of duties in all critical IT systems supported by ITSB and work with responsible Assistant Deputy Ministers to address concerns with conflicting responsibilities.

Management Action Plan 3.1: Define a segregation of duties standard, including a schedule for ongoing reviews, for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 3.2: Identify gaps against the defined standard for systems identified in 3.1.

Management Action Plan 3.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 3.4: Provide compliance reports to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 4: The Chief Information Officer, Information Technology Services Branch should examine the security audit log functions in all critical IT systems supported by ITSB and work with appropriate Assistant Deputy Ministers to address identified deficiencies in the LDRPS and DISIS systems.

Management Action Plan 4.1: Define a standard, including a schedule for ongoing reviews, for monitoring security audit logs in all PWGSC Tier 1 or highly exposed or highly sensitive IT systems supported by ITSB.

Management Action Plan 4.2: Identify gaps against the defined standard for systems identified in 4.1.

Management Action Plan 4.3: Identify corrective measure requirements to meet the standard.

Management Action Plan 4.4: Provide compliance reports against the standard to the IT Security Coordinator on an ongoing basis, commencing in March 2012. The reports will include the activities defined to address gaps on a non-compliance status.

Recommendation 5: In line with the requirements of PWGSC Policy on IT Security (DP104), the Chief Information Officer, Information Technology Services Branch should provide functional guidance to Assistant Deputy Ministers to ensure proper IT security of all departmental systems not supported by ITSB, including guidance to ensure requirements related to vulnerability assessments, patch management, segregation of duties and security audit logs are met.

Management Action Plan 5.1: Provide functional guidance to ADMs/RDGs by communicating Branch/Regional responsibilities for MITS to the Departmental Security Committee.

Management Action Plan 5.2: Provide the PWGSC standards (developed in 1.1, 2.1, 3.1, 4.1), to relevant ADMs/RDGs for all PWGSC Tier 1 or highly exposed or highly sensitive IT systems not supported by ITSB and request that they comply with these standards.

Management Action Plan 5.3: Instruct ADMs/RDGs to monitor and confirm compliance against the PWGSC standards (defined in 1.1, 2.1, 3.1, 4.1) by requesting they report to the IT Security Coordinator. Included in the reports, are the activities defined to address gaps on a non-compliance status.

Management Action Plan 5.4: Identified action plans in 5.3 are monitored and reported to the CIO on an ongoing basis commencing in March 2012.

ABOUT THE AUDIT

Authority

This audit was approved by the Audit and Evaluation Committee of Public Works and Government Services Canada as part of the 2009-2014 Risk-Based Multi-Year Audit and Evaluation Plan.

Objective

The objective of this audit was to determine whether PWGSC complied with selected Management of Information Technology Security Standard requirements for selected critical IT systems that support critical services.

Scope and Approach

The scope of the audit covered four key requirements of the MITS standard. They are:

- *Vulnerability management:* Continuously manage threats to programs, systems and services. This management task includes the discovery of threats and the implementation of corresponding solutions.
- *Patch management:* Acquire, test, and install software fixes on an administered IT system.
- *Segregation of duties:* Separation of responsibilities related to an IT system or business function to avoid situations where a single individual can make a system vulnerable to undetected abuse.
- *A Security audit log:* Maintain records of activities related to the security, integrity and availability of a system.

These four requirements were selected because they were deemed by the Office of Audit and Evaluation to be of higher risk to the Department. Three of the four selected MITS requirements (Vulnerability management, patch management and segregation of duties) are included in part II of the MITS standard, Departmental IT Security Organization and Management. This part of the standard provides direction and guidance on how to organize and manage a departmental IT security program. It covers roles and responsibilities, policy, resources and management controls. The fourth selected MITS standard, Security audit logs, is included in part III of the MITS standard, Detection. These are controls used to detect incidents.

For this audit, portions of six critical IT systems were selected for testing. These six systems are located in the National Capital Area and were selected because they support many Tier 1 critical services, which need to be recovered within 72 hours as defined in the March 9, 2010 PWGSC Business Impact Analysis Summary Report. The six critical IT systems selected are:

- Project and Business Management System (PBMS) from Real Property Branch ;
- SIGMA from Finance Branch (PWGSC's financial management and materiel management system);
- Canada Gazette Production System from Consulting, Information and Shared Services Branch (CISSB);
- Living Disaster Recovery Planning System (LDRPS) from Corporate Services and Strategic Policy Branch (CSSPB);
- Enterprise Document and Records Management System (EDRMS) from CSSPB; and,
- Departmental Industrial Security Information System (DISIS) from CISSB.

The audit did not examine the MITS standard requirements related to the protection of classified information, as these are examined in PWGSC's Audit of Classified Information Processed Electronically. In addition, we did not examine the integrity of the data contained within the systems as no access to system or application code was requested.

This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

During the survey phase, policy instruments were analyzed and members of the Information Technology Services Branch and other selected branches were interviewed. A risk assessment was conducted which identified risks associated with elements of the MITS standard. This risk assessment took into account all the MITS standard sections, PWGSC's MITS standard self-assessment response to MAF Round VII, and TBS's initial assessment of PWGSC's compliance against the MITS standard.

During the examination phase, in-depth interviews were conducted with key branch personnel. Relevant processes and documentation were examined and tested. Based on the analysis of the information and evidence collected, the audit team formulated audit observations that were validated with the appropriate managers.

Criteria

The following criteria were used to assess PWGSC's compliance against selected MITS standard requirements for selected portions of critical IT systems located in the National Capital Area that support critical services:

- PWGSC conducts regular vulnerability assessments on selected critical IT systems and on IT systems accessible from outside Public Works.
- PWGSC establishes a systematic, documented patch management process to ensure that security-related patches are applied in a timely manner, for selected critical IT systems.
- IT systems have good segregation of duties to prevent unauthorized changes to the systems and/or the databases and servers.
- Security audit log functions are included and enabled in selected critical IT systems.

Audit Work Completed

Audit fieldwork for this audit was substantially completed on August 1, 2010.

Audit Team

The audit was conducted by members of the Office of Audit and Evaluation and an audit consultant. It was overseen by the Director Internal Audit, and under the overall direction of the Chief Audit and Evaluation Executive.

The audit was reviewed by the quality assessment function of the Office of Audit and Evaluation.

Appendix A

Glossary

Critical IT Systems	Systems that are in place to support a critical business function or a critical service. ITSB considers critical to a client branch if they have a funded Disaster Recovery plan in place.
Critical Services	A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada and is to be recovered within the first 72 hrs (categorized as Tier-1) in the *PWGSC Business Impact Assessment Summary Report*.
IP Address	A numeric code that identifies all devices that are connected to a network and/or to the internet
Regularly	A set schedule (for example; weekly, monthly, quarterly, etc.) based on a risk assessment conducted on the system A periodic, planned activity that is in line with the department's risk tolerances.
Patch Management	1) Is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system 2) The process of using a strategy and plan of what patches should be applied to which systems at what time
IT System	IT Systems are comprised of not only infrastructure, but also software. IT System are a set of computer equipment and programs used together for a particular purpose