Archived Content

Health Canada Santé Canada

Final Audit Report

Information Technology (IT) Security

March 2011

Table of Contents

Executive Summary

The *Policy on Government Security* defines Information Technology (IT) Security as the "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. In 2005, the Treasury Board Secretariat of Canada requested that all departments implement, by December 2006, the Management of Information Technology Security (MITS) standard. This operational security standard represents the baseline IT security standards for all Government of Canada departments to follow.

The objective of the audit was to assess the internal controls in place to support IT security at Health Canada as stated in the Management of Information Technology Security (MITS) standard. Specifically, the audit assessed the: IT Security Organization; Departmental IT Security Policy and Program; IT Security Controls; and Operational and Technical Safeguards.

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*.

Currently, Health Canada is not yet fully compliant with the operational security standard although the Department has put significant resources towards achieving MITS compliancy. Achieving the baseline standard has been a challenge across government and few departments are compliant. Despite challenges, in 2009-10 Health Canada received an *acceptable* rating in its Management Accountability Framework assessment. Historically, the Information Management Services Division has made progress in identifying where IT and information control gaps exist and where stronger and more effective controls are needed. While IT security control "gaps" have been identified, more needs to be done to close those gaps. As a result, there are some areas of vulnerability which should be addressed to further strengthen the Department's IT security posture (See Appendix B – scorecard).

The report includes seven recommendations aimed at further strengthening IT Security at Health Canada. Management has agreed to each of the recommendations with a detailed action plan.

1. Introduction

1.1 Background

The *Policy on Government Security* defines Information Technology (IT) Security as the "safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. Since 2002, the Treasury Board Secretariat of Canada has worked with lead security agencies and some departments to issue several operational and technical security standards that departments must fulfill to ensure the security of information and information technology assets under its control. In 2005, the Treasury Board Secretariat of Canada requested that all departments implement, by December 2006, the *Management of Information Technology Security (MITS)* operational standards as the baseline requirements for their departmental IT security program. Meeting the baseline requirement has been a challenge across government and most departments have received an "acceptable" rating from the Treasury Board of Canada Secretariat's Management Accountability Assessment. Health Canada received an *acceptable* rating in 2009-10, noting it has achieved the 3 priority objectives that form the foundation for Management of Information Technology Security (MITS).

Network security involves all activities that Health Canada undertakes to protect the value and ongoing use of assets as well as the integrity and continuity of operations. An effective IT security strategy requires identifying threats and then choosing the most effective set of tools to combat them. There is a need to ensure that those having access to government information, assets and services are entitled to them. As such, Health Canada must proactively manage security threats, risks and incidents in an ever changing threat environment in order to protect critical assets, information and services while achieving departmental strategic goals.

1.2 Audit Objective

The objective of this audit was to assess the internal controls in place to support IT security at Health Canada as stated in the Management of Information Technology Security (MITS) Standard. Specifically, the audit assessed IT security in relation to:

- IT Security Organization;
- Departmental IT Security Policy;
- IT Security Controls; and
- Operational and Technical Safeguards.

1.3 Audit Scope and Approach

The *Management of Information Technology Security* (MITS) *Standard* (12.11.2) specifies that planning for information technology (IT) security audits is a requirement. Based on risk assessments IT Security was incorporated into the departmental risk-based audit plan. The audit of IT Security was undertaken by the Audit and Accountability Bureau in accordance with the Departmental Risk-Based Audit Plan for 2009-2010 to 2011-2012 which was endorsed by the

Departmental Audit Committee on May 22, 2009 and subsequently approved by the Deputy Minister.

In January 2007, the Treasury Board changed the format of MITS status reporting from 144 elements to approximately 50. The audit was largely based upon this new requirement, however, not all 50 elements were reviewed. A risk assessment was completed that examined key sections of the standard. The results of the assessment were used to focus the audit on those areas of greatest risk to the Department. The audit criteria were derived from both the MITS standard and the Control Objectives for Information and Related Technology (COBIT).

The audit was primarily carried out in the National Capital Region however phone interviews were conducted with some Region staff. The examination phase included interviews with officials from the Corporate Services Branch and the Regions and Programs Branch. This phase also included a review of records and an examination of selected documentation, including threat and risk assessments, vulnerability assessments, statements of sensitivity, privacy impact assessments, policies, standards, guidelines, service level agreements, frameworks and plans.

The audit did not examine areas in the operational security standards relating to occupational health and safety, physical security, wireless and Business Continuity Planning. Business Continuity Planning was the subject of an internal audit at Health Canada, tabled in March 2011 and Wireless was the subject of a recent external audit completed by the Privacy Commissioner.

1.4 Statement of Assurance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing.*

2. Findings, Recommendations and Management Responses

2.1 IT Security Organization

2.1.1 Governance Structure

Audit Criteria: *There should be a governing framework to provide oversight for IT Security.*

Health Canada's IM/IT governance structure consists of a few key oversight bodies – the Executive Committee, its subcommittee on Operations, and the Information Management Services Directorate - Executive Committee. The directorate level committee is supported by two working groups: Operation Management Committee and the Operations Oversight Committee. At the time of the audit, the Information Management Accountability Board was in place with senior level representation from the Branches.

IT Security is further supported by an external advisory body. Supporting all government departments and agencies is the Canadian Cyber Incident Response Centre (CCIRC) which is governed by Public Safety Canada. The Canadian Cyber Incident Response Centre monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. Any results relating to Health Canada are communicated to the Departmental Security Officer for action. Health Canada also relies on the Communications Security Establishment Canada (CSEC), Canadian Security Intelligence Services (CSIS), and Royal Canadian Mounted Police (RCMP) for IT Security expertise and intelligence.

2.1.2 Key Roles and Responsibilities

Audit Criteria: *Senior Management positions defined in the operational security standard should be assigned in the Department.*

The Information Management Services Directorate, within the Corporate Services Branch, provides organization-wide IT services and is responsible for major elements of Health Canada's IT infrastructure. Health Canada has an IT Security Coordinator (ITSC) who reports directly to the Chief Information Officer and (functionally) to the Departmental Security Officer both whom provide leadership for the Department's IT security posture. Each of these positions has a direct reporting relationship to the Assistant Deputy Minister, Corporate Services Branch. In addition, Health Canada has six regional offices each with its own IT Security group. These staff report through the Assistant Deputy Minister, Regions and Programs Branch. The roles and responsibilities are listed in the IT Security Order, and were last updated in December 2006.

The Chief Information Officer (CIO) is responsible for the workings of the Information Management Services Division. As expected by the IT security standard, the CIO works closely with the IT Security Coordinator to manage the Department's IT security so that appropriate security measures are applied to all departmental IT assets, activities and processes.

The Deputy Minister has delegated the Director, IT Security to act as the departmental IT Security Coordinator. Primarily, the IT Security Coordinator provides overall program direction for technical security and acts as the departmental point of contact with Government of Canada lead agencies in matters of information technology security. These responsibilities compare with those outlined in the security standard. The IT Security Coordinator is presently supported by 21 staff.

The Deputy Minister has delegated the Executive Director, Safety, Emergency and Security Management as the Departmental Security Officer. The Departmental Security Officer is responsible for the provision of the overall program leadership in regards to security within Health Canada. Compliance with these provisions is mandatory as indicated by the Policy on Government Security and its associated supporting documents as represented by Treasury Board Operational Security Standards.

As mentioned, Health Canada has six regional offices each with its own IT Security group. These staff report through the Assistant Deputy Minister, Regions and Programs Branch. A regional review of IT security was conducted via an examination of regional documentation and interviews with regional information security staff. [redacted].

Recommendation 1

It is recommended that the Assistant Deputy Minister, Corporate Services Branch, as the functional authority for IT Security, work with the Branches to [redacted] meets Health Canada's security requirements.

Management Response

Management agrees with the recommendation.

[redacted]

[redacted]

2.2 IT Security Policy and Program

2.2.1 IT Security Policy

Audit Criteria: *Health Canada should have an IT Security Policy which is supported by an IT Security Program.*

An effective IT Security program has three interrelated and interdependent core components - an IT Security Policy (with clear statements that support the business and security objectives of the Department), skilled and knowledgeable IT Security practitioners (who provide guidance, interpretation and enforcement of these policy objectives), and functional integration into the IT services of the Department. While Health Canada has developed these three entities to varying degrees of maturity – they are not effectively synchronized as an enterprise IT security program should be to protect information and information assets. The Department has developed and documented departmental policies and procedures that would provide a framework for implementing such a program. The Program should consider including: risk assessments; information systems security planning (including existing and planned IT security requirements); routine testing strategies to evaluate the security controls and to determine the effectiveness of IT security policies and procedures; remedial action plans which would identify the resources needed to correct or mitigate known security weaknesses along with complete and accurate systems inventory.

Health Canada's 2006-07 MITS compliance project was used as the vehicle to develop requirements for an IT Security policy. Supporting the IT Security policy are several IT Security Orders and IT Security Tools. However, some of the IT Security Orders on Health Canada's Intranet site are limited to titles without the associated text explaining the actual security order and are listed as being "preliminary" and "under development".

Recently, the IT Security function has merged under a single management unit with a mandate to better integrate security into the IT functions of Information Management Services Directorate (IMSD).

Recommendation 2

It is recommended that the Assistant Deputy Minister, Corporate Services Branch develop and document an IT security program in line with the Health Canada IT Security Policy.

Management Response

Management agrees with the recommendation.

[redacted]

2.3 IT Security Controls

2.3.1 Application Life Cycle Management

Audit Criterion: *The architecture of Health Canada's IT security management controls should encompass all aspects of the system development life cycle as a shared responsibility between IT Security and Business Owners.*

Business owners need to consider the security issues related to a new application at the very early stages of the project life cycle and they should work closely with IT security to leverage the concepts of the "secure software development life cycle approach". Attempting to put security controls in place at the end of the lifecycle leads to time and cost inefficiencies. In using the *Application Software Registry*, the IT security team can manage the security requirements throughout the stages of the applications life cycle.

The *Application Software Registry* is a web application which facilitates the collection of the information for all systems and applications within Health Canada, and also supports the Department's ability to manage information about its applications throughout the system development life cycle. The Application Development and Internet Division (ADID), IT Security Services and the MITS Project teamed up to develop a new approach to achieve better security completion rates for applications being put up on the Department's network. With a simplified

application registration and Statement of Sensitivity processes, business owners should be able to quickly and simply comply with Treasury Board Secretariat, *Management of Information Technology Security Standard* (MITS) requirements. The guidance for business owners has been provided in the *IT Security – Orientation for Application Business Owners*.

However, the number of applications fulfilling the complete security review remains fairly low (see table below). A recurring issue is that the business owners of critical assets have not yet agreed with all the security recommendations and/or have not signed off on the Threat and Risk Assessments. IT security has no clear mandate and authority to have business owners comply. As a result, the IT security processes and controls often do not get carried out as designed. For the period under examination, the following table illustrates the results of the audit testing:

Results of the Audit Testing

Number of Registered Applications	Statements of Sensitivity Completed	Threat and Risk Assessments Completed	Certifications Completed	Accreditations Completed
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

The audit team examined [redacted] new applications in production since April 2009 [redacted].

2.3.2 Security Risk Management

Audit Criterion: *Departments must continuously manage the security risks to information and IT assets throughout the life of the programs and services.*

IT Security also uses the *Application Software Registry* to manage security risks. These activities include specifying the sensitivity of information and IT assets, conducting threat and risk assessments, as well as conducting security certification and accreditation of all IT assets. These controls exist to ensure that new application development and modifications to existing applications do not introduce security risks into the network environment.

- **Statements of Sensitivity (SoS)** are an important first step in the risk assessment process. These statements identify and categorize information and related assets according to their sensitivity. (Public, Protected, Secret etc.)
- **Threat and Risk Assessments (TRA)** answer certain questions such as: What needs to be protected? Who/what are the threats and vulnerabilities? What are the implications if they were damaged or lost and what is the value to the Department? They also include recommendations to mitigate risks of confidentiality, integrity and availability.
- **Security Certification (C&A)** is a comprehensive assessment of whether the technical and non-technical security features within a system or application meet a specific set of security requirements. The process also includes the identification and acceptance of residual risks by the business owner. Security accreditation is the official authorisation by management for the operation of an IT system, and acceptance of the associated residual risk.

As mentioned, the registry automatically triggers a requirement for a validation of both the Statement of Sensitivity and the Threat and Risk Assessment by the IT security section. Where warranted, a certification and an accreditation report will be completed for the application. This is currently the process in place; however IMSD must continue to improve its overall effectiveness.

Due to the overwhelming number of applications being registered, IT security has used a "fast-track" process to get applications [redacted] with minimal review. Despite this measure, and as mentioned previously, the completion rate remains low and some software remains on the network beyond the expiration date given by the "interim authority to operate".

Recommendation 3

It is recommended that the Assistant Deputy Minister, Corporate Services Branch work with all other Assistant Deputy Ministers to comply with system development lifecycle controls designed to remove and/or mitigate IT security risk exposure.

Management Response

Management agrees with the recommendation.

[redacted]

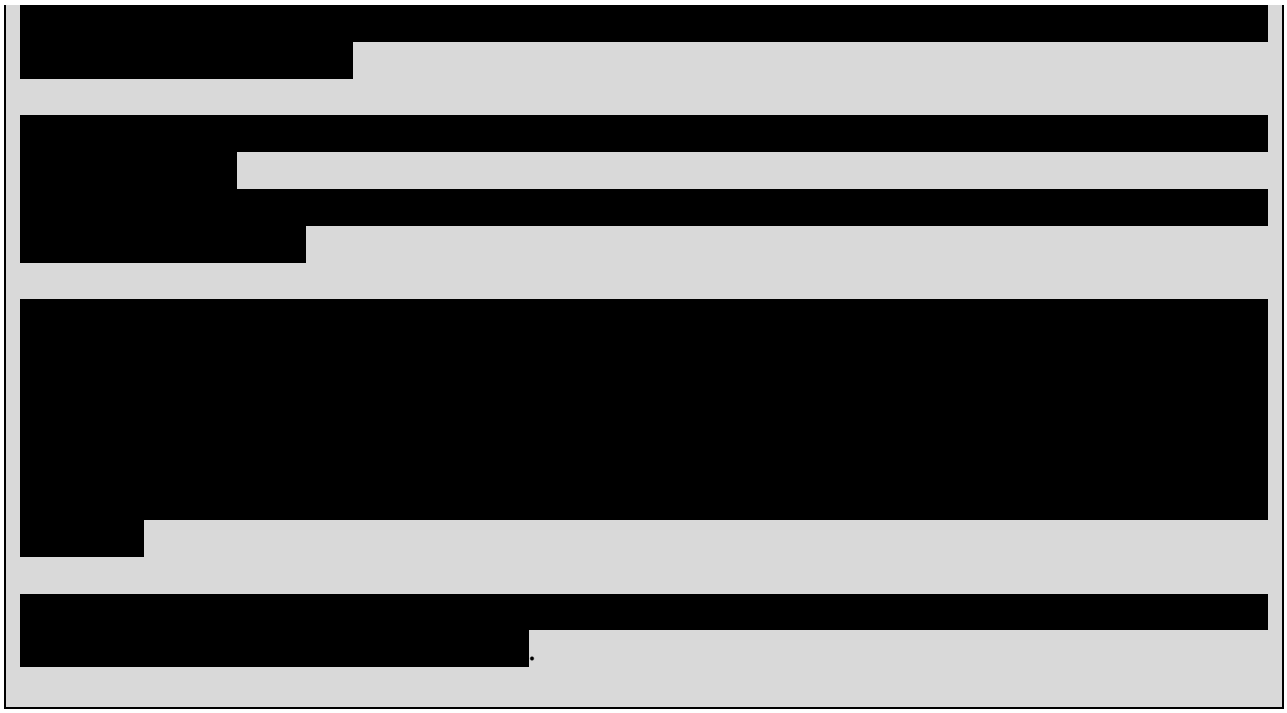
Recommendation 4

It is recommended that the Assistant Deputy Minister, Corporate Services Branch work with all other Assistant Deputy Ministers to develop compensating controls aimed at enforcing the conditional nature and acceptance granted by an interim authority to operate for new or enhanced application development.

Management Response

Management agrees with the recommendation.

[redacted]



2.3.3 Inventory Management

Audit Criterion: *Inventory management for information and IT assets should be identified and categorized using attributes that underscore sensitivity, criticality and any other qualities reflective of value to the organization.*

The Department also uses the *Application Software Registry* to manage applications hosted on the Health Canada network and to identify mission critical departmental applications. IT Security used a bottom-up process to identify critical assets with the intention to design a single methodology that would be repeatable and traceable, risk-based, and successful in audit challenges.

The *"Critical IT Asset Overview"* document highlights the process used to identify, process, rank, and approve critical IT Assets. The process uses attributes that underscore the sensitivity, criticality and priority/severity of the applications. In 2008, the process identified the top 54 critical assets out of an inventory of over 2000 applications. From this list, a Level I list of 12 priority critical applications, those requiring continuous or 24 hour or less availability, were submitted to the Information Management Accountability Board. These 12 assets were approved by the Information Management Accountability Board as the official list.

Currently, when Programs enter applications in the *Application Software Registry,* they make a determination on whether the application is critical by simply checking a box on the screen. This check is now the definitive identifier for a departmental critical asset, yet there is no assurance that this is done based on the attributes identified in the *"Critical IT Asset Overview"* document.

IT Security recognizes this challenge and is in the midst of clarifying a process to determine who should make the final decision around criticality.

Recommendation 5

It is recommended that the Assistant Deputy Minister, Corporate Services Branch review and revise the IT critical asset identification and categorization to meet security standards.

Management Response

Management agrees with the recommendation.

Health Canada has made a significant effort to identify the Department's 12 priority Critical Assets based on Treasury Board of Canada Secretariat and Public Safety Canada criteria. This was necessary to meet MITS compliance requirements in 2008. Due to new mandates (e.g. H1N1), changes to existing applications and technologies, and the changing departmental IT infrastructure, it is necessary to review existing and potential new Critical IT Assets, identify common components, and ensure these assets can meet the confidentiality, integrity and availability requirements.

To better ensure departmental consistency and inclusion, the creation of this list will require the participation of all. The new list, presently in draft form, will require the approval of all Assistant Deputy Ministers for verification of participation.

2.3.4 Vulnerability Management

Audit Criterion: *Vulnerabilities affecting Health Canada's IT infrastructure that impact the programs, systems and services delivered by the Department should be continually assessed.*

The security standard expects that departments will continuously manage vulnerabilities for its programs, systems and services. Also, internal network assessments should include a review of server configuration, security policies and the utilization of network appliances to determine network vulnerabilities on a regular basis.

The Department has a vulnerability assessment tool that has the ability to perform regular vulnerability assessments on network servers, [redacted].

[redacted]

[redacted]

2.3.5 Network Segregation

Audit Criterion: *The IT security program should consider segregation in its control architecture and strategy.*

A segregation strategy for IT security encompasses objects such as roles, systems, processes, and network architecture. The Department's perimeter security is a combined management effort of both the Connectivity and Telecommunications sections of the Data Center Services Division and the Office Automation Division.

Perimeter security strategy and polices must provide adequate separation of duties; while at the same time preclude the ability of one individual from having control of key systems within the departmental network which could create a single point of failure. Despite the absence of guidelines and formal roles and responsibilities, the perimeter security staff employs "role based" privileges that provide the necessary access to perform their duties. In addition, network firewalls provide fail proof measures of redundancy that mitigate risks. [redacted]

One of the architectural components of a network segregation strategy is the segmentation of the network. Health Canada's network architecture is appropriately designed to separate the departmental internal network from services accessed externally. Segregation of roles and responsibilities for all positions responsible for the operational management of network security are appropriate and include the required backup resources to prevent a single point of failure.

[redacted]

Recommendation 6

It is recommended that the Assistant Deputy Minister, Corporate Services Branch complete risk assessments [redacted]

Management Response

Management agrees with this recommendation.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

2.4 Operational and Technical Safeguards

2.4.1 Active Defence Strategy

Audit Criteria: *Health Canada should adopt an active defence strategy that includes prevention, detection response and recovery.*

An active defence strategy involves several interrelated business functions and integrated activities for the purpose of providing external/perimeter security as well as internal safeguards. Health Canada's active defence strategy includes a firewall management program, intrusion detection and prevention program, patch management, user authentication and remote access capabilities to safeguard the Department's network perimeter.

Firewall Management involves the configuration, coordination and change management of network appliances (servers and routers) whose purpose is to allow authorized network traffic in and to block unauthorized traffic. Firewalls must be configured to provide maximum security to sensitive data and explicit firewall rules should be established to identify the appropriate traffic to pass through. For approximately the past five years the Department has contracted with Public Works and Government Services Canada (PWGSC) to provide managed firewall services

and anti-spam filtering. However, the [redacted] IMSD reports that this was the result of poor communication processes and protocols between Health Canada and PWGSC. As a result, the Department has had to employ additional safeguards to mitigate these risks from re-occurring.

Intrusion Detection and Prevention Services form part of the active defence strategy. The main responsibilities of the Security Technologies Section, within of the Office Automation Division, is to conduct IT forensic investigations, provide anti-virus protection, complete vulnerability assessments, and deliver intrusion detection and prevention services. This team uses commercial off-the-shelf software and network appliances to provide an extra layer of protection from adversarial attacks that may be undetected by the firewall.

Responsibility of "network level" intrusion detection and prevention has been recently shifted to the Communications and Interconnectivity Section. Examination of Network Level (Servers) Intrusion Prevention logs, demonstrated that these preventative controls [redacted]. However, the level of complexity and sophistication of adversarial agents continues to increase.

[redacted].

Patch Management: The Security Technologies Section uses the same software product to remove vulnerabilities from the network servers on a continual basis. Examples of vulnerabilities mitigated using patch management include responding to denial of service attacks where an attacker overloads the system with network traffic in an attempt to bring down the system or elevation of privilege attack where an attacker misleads the system into granting higher than authorized privileges. During the examination phase of the audit, [redacted] as the project moves to full operational production status – this is due by end of March 2011. Patch management of regional servers and workstations that are connected directly to the servers is performed by the National Security Technologies Section. The capacity to do patch management is also enhanced by the Desktop Support Division using a software tool which protects end-user workstations by blocking questionable internet traffic and continually monitoring vulnerabilities to the desktop to prevent viruses from propagating on the desktop and spreading to the network. Health Canada utilizes strong encryption and a single authentication standard for its user authentication and

credential management processes. Access to system services and tools is restricted to appropriate IT administrative staff.

There is also the need to perform regular patch management on departmental end-user workstations [redacted].

Account Management and Remote Access Services: Accessibility to IT assets should be established using secure connections that maintain the confidentiality, integrity and authenticity of the traffic communicated between the client and the departmental network. The Office Automation Division's File Print and Remote Management section are responsible for "Web-Office" services. The service uses [redacted] as the means to provide a secure virtual private network for clients to access the departmental network using their web browser. Users can access the departmental network through both dial-up and high speed internet access. The Interconnectivity and Communications Section within the Data Center Services manages this process.

Both the Remote Management and Interconnectivity sections have demonstrated that they employ effective security controls/safeguards in the implementation of their remote access services. Examples include the use of strong encryption, adoption of a single authentication standard, segregated services (access privileges) for administrative and end-user staff. Both sections have also demonstrated an adequate level of redundancy in their assignment of backup resources and in their implementation of high-availability (failover) design in their technical architecture to mitigate risks of a single point of failure.

The Remote Management Section is also responsible for user account management to [redacted].

2.4.2 IT Security and the Management of Change

Audit Criterion: *IT business functions and processes with a security component/impact such as change and configuration management, problem reporting and capacity planning should be managed in accordance with the security risk profile of the Department.*

The MITS standard notes the need to seek the advice or approval from IT security within the Change Management process where changes could potentially expose risks to the system or compromise security. As an integral part of the Change Management Process and practices, the Change Advisory Board has been delegated by the Chief Information Officer to routinely review, validate, and subsequently approve/reject any change request where IT security is an important factor.

The MITS Standard requires that departments monitor system and network capacity in order to plan and implement timely capacity changes. An examination of ten security change requests showed that each of the change requests have addressed the security threats. They were reviewed and approved by IT security and implemented according to the change management process. However, while changes were made, only 30 percent of the change requests examined have been formally tested to see if they work.

The audit team looked at 42 change requests that were rejected by IT security as they were deemed to cause a security risk to the system. The review demonstrated that IT security had exercised its due diligence to reject the requests.

Recommendation 7

It is recommended that the Assistant Deputy Minister, Corporate Services Branch strengthen the operational and technical safeguards around workstation intrusion detection, account management, remote access, and change management requests.

Management Response

Management accepts this recommendation.

[redacted]

[redacted].

2.4.3 Incident Management

Audit Criterion: *The Department should implement measures to identify and classify incidents and sanction accordingly.*

The Department should have the process in place to clearly identify different types of IT security incidents and classify them based on concrete and clear guideline and the best practice evaluation process. It then has to have a clear action plan on how to deal with such incidents as well as to establish effective incident response and IT continuity mechanisms.

In addition, the *Departmental Security Policy* requires departments to establish mechanisms to respond effectively to IT incidents and exchange incident related information with designated lead departments in a timely fashion.

Most of the IT security events are received via the National Help Desk where they are transferred to the IT [redacted]. Each request to the Help Desk is tracked. [redacted].

[redacted].

Currently, the Department is putting together a project plan to move toward an incident management process that will respond to the MITS Standards.

5 stages for handling incidents

1. Identification - determine the type, severity and cause of the incident(s)
2. Response - determine the best approach and take action to contain the damage
3. Reporting - communicate the incident specifics, including the impact and the response, to PSEPC (Public Safety and Emergency Preparedness Canada) and departmental management,
4. Recovery - identify an approach to restore and recover systems and implement approved changes to security devices (e.g. firewall and incident detection rules), and
5. Post-Analysis - Assess the incident and recommend changes in processes and procedures, if required.

IT Incident Response

The Department should have a process in place to deal with the IT security misconduct or negligence. This would include actions to identify, evaluate and report on incidents of misconduct or negligence. It would also include the identification of subsequent actions necessary to reduce or minimize the security risk in the future. In addition, the Department must

have a documented policy for the application of sanctions in case of IT incidents due to misconduct or negligence.

IT security has both anti-virus and forensics functions that triage suspected IT incidents in the workplace. As the result of the investigations, the reports are sent to the requesting parties for further action. In 2009, the IT security forensics team was involved in 147 investigations and to date have been involved in 103 cases. Typically, the Departmental Security Officer initiated the IT related investigations and requested assistance based on the allegations raised. Guidance is being developed to provide functional support to management with respect to conducting an administrative investigation when an allegation of misconduct is directed at an employee or a group of employees.

The role of the Departmental Security Officer is to remain at arms length in all investigations and report on the findings of an investigation to management. It is the role of Labour Relations to recommend discipline actions or sanctions that are imposed by the manager.

An IT Security Program would be an ideal vehicle to strengthen the incident management process and provide for direction on the application of sanctions. (See Recommendation 2)

3. Conclusion

Since 2006, Health Canada has strived to be on the leading edge of Information Management and Technology. Major initiatives such as the "Way Forward" (2007-2008) focused on moving the Department towards better economies of scale and standardization in service delivery with the implementation of an enterprise approach to IT. During that time, the Department initiated the "MITS Compliance Project". The single most important outcome was the development of a departmental IT Security Policy. Following this key outcome, Health Canada started a number of project initiatives. Objectives included an assessment of the Department's ability to secure information assets by conducting Threat and Risk Assessments on twelve of the Department's most critical application assets. During this period, a comprehensive Threat and Risk Assessment on Network Interconnectivity was also completed focusing on IT network infrastructure vulnerabilities. An important deliverable resulting from this project was a Safeguard Implementation Plan (SIP) or in essence a gap analysis documenting where the Department was and where they needed to be in regards to network security.

While much has been done to document the IT security risks more needs to be done to mitigate those security risks identified. An integrated IT Security Program to support the IT Security Policy requirements will serve to address security risks and put the Department that much closer to being compliant with the operational security standard. The completion of this IT Security Audit, in itself, fulfills one of the operational security standards. The standard states that "Federal government departments and agencies should assess and audit IT security and remedy deficiencies where necessary".

Health Canada continues to make positive progress in identifying where control gaps exist and stronger and more effective controls are needed. The audit has noted that an organization is in place and appropriate responsibilities have been delegated to manage IT network security operations and risks. However, in the areas of IT Security Controls and Technical Safeguards, while many controls are in place, there are some instances where controls and safeguards are not entirely effective.

As recently as November 2010, the Computing and Network Services Center proposed an "operating plan" for the next fiscal year. The plan contains projects such as the; [redacted]; Desktop Transformation; and Information Protection Center. While the plan has not yet been approved, these projects have the capability to address some of the control deficiencies identified in the audit and to also move the Department closer to compliance with the operational security standard.

Appendix A – Audit Lines of Enquiry and Criteria

Criteria
Organization
Governance Structure: There should be a governing framework to provide oversight for IT Security. Senior Management positions defined in the operational security standard should be assigned in the Department.
Policy and Program
IT Security Policy: There should be an IT Security Policy supported by an IT Security Program.
IT Security Controls
Application Life Cycle Management: The architecture of Health Canada's IT security management controls should encompass all aspects of the system development life cycle.
Security Risk Management: Departments must continuously manage the security risks to information and IT assets throughout the life of the programs and services.
Inventory Management: Inventory management for information and IT assets should be identified and categorized using attributes that underscore sensitivity, criticality and any other qualities reflective of value to the organization.
Vulnerability Management: Vulnerabilities affecting Health Canada's IT infrastructure that impact the programs, systems and services delivered by the Department should be continually assessed.
Network Segregation: The IT security program should consider segregation in its control architecture and strategy. The strategy should include segregation of roles, responsibilities, duties, objects, processes, appliances and functions to mitigate risks to the IT infrastructure and systems.
Operational and Technical Safeguards
Active Defence Strategy: Health Canada should adopt an active defence strategy that includes prevention, detection response and recovery.
IT Security and the Management of Change: IT business functions and processes with a security component/impact such as change and configuration management; problem reporting; and capacity planning should be managed in accordance with the security risk profile of the Department.
Incident Management: The Department should implement measures to identify and classify incidents and sanction accordingly.

Page 20 exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b) of the Access to Information Act