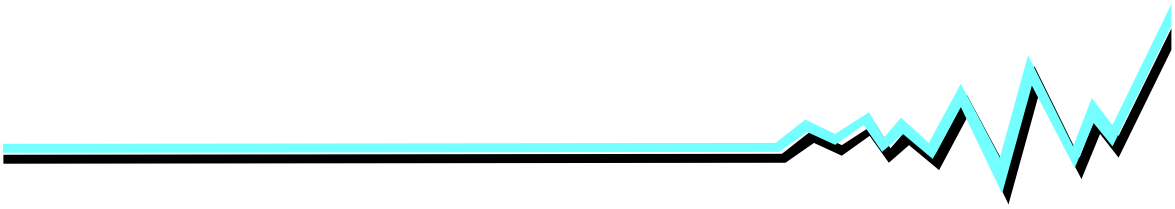
Veterans Affairs Canada | Anciens Combattants Canada

Information Management Risk Assessment

Final - August 2011



Canada

ACKNOWLEDGEMENT

The review team would like to acknowledge all those who assisted us with this review. The team acknowledges in particular, the cooperation and assistance given to us by Veterans Affairs Canada management and staff in the Information Technology and Information Management divisions related to this Risk Assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Information is a vital corporate asset that allows Government to deliver programs and services to the public, make informed decisions, and promote government transparency and accountability. Information Management is about ensuring that the right information gets to the right people, at the right place and time.

Subject to the exceptions listed in subsection 8(2), the *Privacy Act* requires that personal information be used only for the purposes for which it was collected and that it be shared, with the consent of the individual, only on a need-to-know basis. In the fall of 2010, the Office of the Privacy Commissioner investigated a complaint alleging Veterans Affairs Canada's mishandling of an individual's personal information. The Office of the Privacy Commissioner concluded that the Department was not compliant with federal privacy legislation and required improved controls to protect sensitive information from being widely disseminated within the Department. A 10-point Privacy Action Plan was developed in response to the Privacy Commissioner's recommendations. This action plan far exceeds the report's recommendations strengthening the protection of personal information and the ability of staff to provide quality service.

In January 2011, the Audit & Evaluation Division commenced a Risk Assessment of Information Management within the Department. The purpose of this Risk Assessment was to provide Senior Management with a comprehensive analysis of all aspects of information management within the Department to ensure that Veterans Affairs Canada had appropriately responded to all potential risks. A total of 14 entities relating to Information Management were analyzed utilizing risk assessment methodology developed by the Office of the Comptroller General.

The results of the risk analysis of the 14 entities (four high, four medium, and six low) confirmed that significant progress has been made since the fall 2010. However, given the importance of information management and the current sensitivity, even with the progress, four entities (Business Continuity Planning, Access to Information and Privacy Requests, Privacy Impact Assessments, and Access to Information and Privacy) were assessed as high risk and the following items requiring management attention were identified:

- The absence of a fully operational and tested IT Continuity Plan exposes the Department to significant risk and could result in interruptions to Departmental service delivery.

- The absence of an approved Emergency Operations Centre places the Department at risk in the event of a major incident.

- Development of an Electronic Document and Records Management System has been approved in principle; however, funding has not been obtained. The current absence of such a system is problematic for capturing and receiving information.

- VAC is not meeting the 30 day turnaround time for Access to Information and Privacy (ATIP) Requests which is not compliant with the *Access to Information Act.*

- The current Information Management Continuity Plan lacks sufficient detail as to the roles, responsibilities, and associated accountabilities. The process of shipping information to and from Matane, Quebec, increases the risk for lost or misplaced information increasing the importance of a well developed IM Continuity Plan.

- The intent of Transformation is to overhaul service delivery and reduce program complexity, thus requiring additional Privacy Impact Assessments. The resulting impact will be increased workload and a possible shift in responsibilities.

Recommendation

It is recommended that the Assistant Deputy Minister, Corporate Services table the above identified risks to Senior Management Committee to determine the appropriate departmental approach to manage these risks.

Corrective action to be taken	**Office of Primary Interest**	**Target date**
Initial IM Briefing – Update	ITIM	June 2011
SMC Briefing – IM Risk Assessment	A&E/ADM CS	July 2011
Update IM Strategy and Develop Implementation Plan	ITIM	September 2011
Execute plan to coincide with transformation agenda	ITIM	March 2014

Original signed by *July 27, 2011*

_____ _____

Don Love Date
Chief Audit Executive

The review team consisted of the following members:

Jonathan Adams, Director, Audit and Evaluation Division
Roger Doiron, Audit Manager
Tim Brown, Audit and Evaluation Officer
Sivajan Nagulesapillai, Junior Auditor

1.0 BACKGROUND

Information is a vital corporate asset that allows the Department to deliver programs and services to the public, make informed decisions, and promote government transparency and accountability. Information Management is about ensuring that the right information gets to the right people, at the right place and time.

Canadians require access to a wide range of information about government. There is compelling public interest in openness, to ensure that the government is fully accountable for its goals and that its performance can be measured against these goals. This renders the government more accountable to the electorate and facilitates informed public participation in the formulation of public policy.

In the summer 2010 a complaint was filed to the Privacy Commissioner of Canada regarding Veterans Affairs Canada's (VAC) management of an individual's information. The Privacy Commissioner of Canada is a special ombudsman who has the authority to investigate privacy complaints filed by Canadian citizens against the Canadian government for violation of the *Privacy Act* regarding personal information of individuals. In the fall 2010 the Office of the Privacy Commissioner (OPC) of Canada completed an investigation and identified some instances where VAC contravened the *Privacy Act* with respect to the handling of personal information.

Subject to the exceptions listed in subsection 8(2), the *Privacy Act* requires that personal information be used only for the purposes for which it was collected and that it be shared, with the consent of the individual, only on a need-to-know basis. The Privacy Commissioner concluded that there was a lack of controls to protect personal information from being widely disseminated within the Department and offered the following recommendations:

- Take immediate steps to support an enhanced privacy policy framework with adequate protections and controls to regulate access to personal information within the Department;

- Revise existing information management (IM) practices and policies to ensure that personal information is shared within the Department on a need-to-know basis only; and

- Disseminate its strengthened privacy policy framework to all of its employees and provide training to employees about appropriate personal information handling practices.

A 10-point Privacy Action Plan was developed in response to the Privacy Commissioner's recommendations. This action plan far exceeds the report's recommendations, strengthens the protection of personal information, and brings about significant improvements to VAC's Privacy Management Framework. Every employee of VAC is responsible for the management of information. IM is much broader than the Information Management Services Directorate (IMSD) and the increased focus on IM will foster a major culture change for VAC.

The following is the current status of the Minister's 10-point Privacy Action Plan.

Action Plan Point	Current Status
1. Review system access in detail Detailed review of approximately 2,800 user accounts in the Client Service Delivery Network (CSDN).	Information Technology (IT) Security now monitors activity reports, reviews, and investigates electronic system access of CSDN.
2. Communicate discipline policy A strengthened discipline policy and guidelines with clear sanctions have been developed and communicated to staff.	An email was sent department wide on January 4, 2011 stating the ongoing process of monitoring CSDN and the procedure that will be taken when disciplinary measures are necessary.
3. Introduce a privacy lens for briefing note processes New procedures have been issued on the appropriate use of Veteran information when preparing briefing notes and other documents prepared for use within the Department.	The VAC *Guidelines on Handling Personal Information in the Preparation of Briefing Materials* have been issued Department wide to ensure that Senior Management briefing notes only contain information required.
4. Appoint external systems expert External experts in electronic information systems management will review and recommend changes to departmental systems.	An external systems expert from FINTRAC reviewed VAC's systems and provided a report with recommendations.
5. Appoint external privacy expert A team of experts in government Information Management and Privacy is working with the Department. These experts will review and recommend	A TBS expert in privacy assisted VAC in reviewing the policies and procedures for the new privacy framework from October – December 2010. The new *Privacy Protection Infrastructure* was created in

Action Plan Point	Current Status
changes to departmental processes that will ensure information is protected and access is controlled.	February 2011 to introduce the Privacy Steering Committee, the Chief Privacy Officer, and the ATIP Coordinator.
6. Enhance monitoring of electronic systems A team began to proactively monitor, review and investigate who is accessing client information. Where there is inappropriate access, disciplinary measures will be taken.	As of October 2010, IT Security monitors activity reports, reviews, and if necessary, investigates electronic systems access of CSDN. An email was sent department wide on January 4, 2011 stating the ongoing process of monitoring CSDN and the procedure that will be taken when disciplinary measures are necessary.
7. Provide mandatory privacy training A mandatory privacy awareness program for all staff was launched on October 19, 2010. This program covers the "need to know", the need for Veteran consent when sharing information, and the range of disciplinary measures that will be taken if privacy is breached. Ste. Anne's Hospital, as an accredited hospital, has its own programs relating to privacy and confidentiality of Veteran information.	Mandatory “Need-To-Know” awareness sessions for all staff have been implemented (approximately 82% have been trained to date). In addition, the "need to know" messaging has been incorporated into the Demystifying Information Management course syllabus and the Manager Orientation sessions. As well starting in June 2011, “need to know” sessions are being offered to students and new employees of the Department.
8. Provide in-depth training on Government policies and procedures on privacy In-depth training for all staff on the new policies, guidelines and procedures.	During March 2011, in-depth training and discussion took place with the management teams of each and every Division in the Department, including Regional Offices. These sessions provided in-depth explanations of the Privacy Management Framework, policies and guidelines.
9. Conduct independent annual assessment An annual independent assessment of VAC's compliance with the *Privacy Act* and	In July 2011, Audit Services Canada from Public Works and Government Services Canada, completed an independent assessment of the Department’s

Action Plan Point	Current Status
the *Access to Information Act*.	compliance with the *Access to Information Act* and the *Privacy Act*. The focus of this assessment was whether the policies and procedures were designed to deliver services in compliance with the Acts.
10. Prepare for Privacy Commissioner's audit The Department has already started preparations for a comprehensive audit by the Privacy Commissioner which is expected to start immediately.	The Department has many ongoing initiatives, such as the points of this 10-piont action plan, to prepare for the Privacy Commissioner's audit scheduled for the fall of 2011.

Supporting the above action plan are three separate initiatives. The first is a Risk Assessment of Information Management within VAC to ensure that the Department has appropriately responded to all potential risks. The second is an external assessment conducted by Audit Services Canada of VAC's compliance with the *Privacy Act* and the *Access to Information Act* in accordance with the ninth point of the 10-point Privacy Action Plan. This external assessment will be completed in July 2011. The third initiative is OPC's audit of VAC's Access to Information and Privacy which is scheduled to commence in the fall 2011.

2.0 ABOUT THE RISK ASSESSMENT

2.1 OBJECTIVES

Prior to the OPC investigation the Audit and Evaluation Division had identified the need for an audit of information management as part of the 2010 – 2013 Audit Plan. This audit was originally scheduled to commence in the fall 2010; however, given the OPC investigation it was agreed to delay starting the audit so that the findings from the OPC investigation could inform the scoping of the audit. In January 2011, it was agreed that a Risk Assessment of Information Management within the Department would provide more value to senior management than an audit. The purpose of this Risk Assessment was to provide senior management with a comprehensive analysis of all aspects of information management within the Department to ensure that VAC had appropriately responded to all potential risks. The objective of this IM Risk Assessment is to assess key areas associated with IM within VAC.

Risk is defined in the Institute of Internal Auditors' (IIA) *International Professional Practices Framework* (IPPF) as "the possibility of an event occurring that will have an impact on the achievement of objectives" and it "is measured in terms of impact and likelihood."

In Performance Standard 2120: Risk Management, the IPPF requires the internal audit function to evaluate the effectiveness and contribute to the improvement of risk management processes.

2.2 SCOPE

The scope of the Risk Assessment included VAC's entire IM universe. This Risk Assessment included all policies and practices effective April 1, 2011 and considered the progress since fall 2010 and planned work ahead.

It is important to note that VAC's IM universe is not exclusive to its Information Management Services Directorate (IMSD). The review team also scoped entities from Security and Real Property Services Directorate and the IT Infrastructure and Operations Directorate.

2.3 METHODOLOGY

This Risk Assessment was conducted in accordance with the IIA's *Standards for the Professional Practice of Internal Auditing*, as required by the Treasury Board's *Policy on Internal Audit*.

The Office of the Comptroller General of Canada, Internal Audit Sector's *Practice Guidebook on the Internal Audit Planning for Departments and Agencies* was applied to assess the risk exposure of the scoped auditable entities. This methodology involved ranking the auditable entities based on a series of prioritization criteria. The review team applied the criteria to each of the auditable entities based on information gathered through documentation review, interviews, and consultation with senior management.

A risk exposure analysis was completed by studying the risk considerations, potential risk events, and recent events for each of the five key risk factors – degree and recentness of change, degree of complexity, legislative or other compliance requirements, degree of knowledge, and degree of dependency – for each auditable entity. The risk levels were calculated by ranking the likelihood and impact for each key risk factor. The sum of the risk levels for the key risk factors was multiplied by a significance to determine the weighted risk ranking of each entity.

The review team originally identified 27 auditable entities within VAC's IM universe. These entities were subsequently combined by the review team as many had similar functions and qualities.

Appendix 1: Risk Exposure Analysis – Weighted Score Ranking provides a table of the prioritization of entities ranked by the weighted score. The highest possible risk assessed score is 90 and the lowest risk assessed score is 10. It is important to note that the team applied analytical, judgemental, and evidentiary methodology to determine the weighted score in the Risk Assessment.

3.0 SUMMARY OF RISK ASSESSMENT

The following table identifies the entities assessed by the review team and ranked in terms of high, medium, and low weighted score. Refer to Appendix 1: Risk Exposure Analysis – Weighted Score Ranking.

IMPACT	LOW	MEDIUM	HIGH
HIGH		Privacy Impact Assessments	Business Continuity Plan ATIP Requests Access to Information and Privacy
MEDIUM		IT Security Policies Information Holdings IM Continuity Plan Threat and Risk Assessments	
LOW	Forms Management Advice and Guidance Spam Monitoring and Prevention IM Clauses for SOW and Contracts Editing and Translation Library		

LIKELIHOOD

3.1 High Risk Entities

3.1.1 Business Continuity Planning (including the IT Continuity Plan) (90)

The *Policy on Government Security* and its associated standards describe baseline security requirements, including the establishment of a Business Continuity Planning (BCP) Program. Business continuity planning enables organizations to survive disruptions while continuing to deliver essential programs/services and is the cornerstone of departmental security and emergency preparedness. Business continuity plans also establish a governance structure, lines of authority, accountability and responsibility for activities deemed essential. It must also establish emergency communications strategies, training plans and recovery options, and create provisions for continuous testing, audit, and review of the plan. The absence of a BCP would likely cause a high degree of inconvenience to Canadians and the government if they were disrupted. VAC's Senior Management Committee is the governing body appointed to support the BCP Program.

Business continuity plans in each area will evolve as VAC is currently revising many programs and business operations due to Transformation. The Department also anticipates a high number of staff to retire in the next five years and the resulting loss of corporate knowledge and skill sets will expose the Department to a greater risk. Business continuity planning involves extensive training and certification. In addition, they need to rely on each organization to design an effective and implementable BCP for their respective area. There is also a high degree of co-dependency with other departments and facilities as they would be supplying back-up. All areas within VAC, except for one, have a BCP.

A major component of BCP is the IT Continuity Plan. An IT Continuity Plan ensures that those IT services which are deemed essential will be available within a preapproved recovery time. IT Continuity Planning is the development of plans, procedures, and arrangements to ensure minimal or no interruption to the availability of critical IT assets and services. An IT Continuity Plan is a critical component to ensure that information is available to enable continuation of service delivery. Most divisions and directorates within VAC have created BCPs, which include aspects of IT continuity. However the absence of a fully developed and tested IT Continuity Plan for the Department threatens the viability of the various departmental BCPs and also contravenes the *Policy on Government Security*. Failure to have a robustly designed and tested IT Continuity Plan will have a detrimental overall effect on the execution of the BCP.

The Department would be highly reliant on an IT Continuity Plan in the event of a major incident as it would outline the roles, responsibilities, and accountabilities of staff, as well, the location of back-up or replacement equipment. The plan would also align the management of technological assets and services between Head Office, the Regions,

and the area offices across the country. The complexities of aligning staff and the dependency on equipment and staff availability nationwide in the event of a major disaster cannot be stressed enough. An Emergency Operations Centre (EOC) is vital to the execution of the Business Continuity Plan. With the increased occurrence of epidemics, disasters, IT threats, etc., there is a continuing risk of a massive disruption in operations. Whether it involves information technology or human resources, there will be unforeseen issues. If unprepared, employee anxiety, confusion, and fear would need to be managed. A draft Terms of Reference dated April 01, 2011 has been developed outlining a fully resourced EOC with assigned responsibilities which allows the Department to respond efficiently and effectively in the event of a crisis. The EOC has not been approved nor integrated into the BCP.

The absence of an IT Continuity Plan also increases the risks of a potential failure to implement the Transformation Agenda, health and financial harm to Veterans, and the potential loss of Veteran information and the accompanying unfavourable media attention. The most important risk would be a possible catastrophic failure of all departmental operations due to the lack of a plan for the continuation of services. In addition, recent cyber attacks in 2010/11 on federal government departments such as the Department of Finance increase the need for a fully-funded and tested IT Continuity Plan.

In February 2009, VAC developed and approved in principle an IT Continuity Plan; however, the plan was not implemented due to a lack of resources. Since 2009, both VAC operations and the IT environment have significantly changed in response to new technology and threats, therefore, potentially making that plan obsolete. For one key system, the Federal Health Claims Processing System (FHCPS), a fully-tested IT Continuity Plan exists. This IT Continuity Plan was developed and managed by the external Contractor and it was a key requirement of the contract. However, for VAC's remaining systems, such as the Client Service Delivery Network (CSDN) and FreeBalance, which contain the majority of Departmental and corporate information, no such IT Continuity Plan exists which contravenes the *Policy on Government Security*.

Prior to this assessment the AED had planned an audit of VAC's IT Continuity Plan for 2011/12. Given the absence of a plan and broader concerns about the Information Management area, this risk assessment was performed instead of the audit.

3.1.2 Access to Information and Privacy (ATIP) Requests (78)

The ATIP Unit of IMSD deals directly with employees and the public to respond to formal and informal requests for records accessible under the *Access to Information Act* and the *Privacy Act*. The unit serves as a centre of expertise for all ATIP-related issues. Each Head Office division and region has an ATIP Liaison Officer to coordinate inquiries.

The *Access to Information Act* grants the public the right of access, with exceptions, to the vast majority of the records that support the administration and the operation of federal government programs and activities. The *Privacy Act* protects the privacy of individuals through the protection of their personal information, allows individuals to request access to their own personal information, and grants to individuals the right to request the correction of their own personal information. When access is requested under these Acts, VAC must give written notice to the requestor as to whether or not access to the record will be provided within thirty days of the request. In 2010 – 2011 there were 488 formal requests which was an increase of 57% from the previous year, mostly attributable to the increase in requests under the *Privacy Act*. These requests range from small requests for specific information to broad requests requiring interdepartmental consultation. Regardless of the size or complexity of the formal request, there is a legislated 30 day turnaround time for Departments to respond. For approximately 30% of the formal requests VAC is not meeting the legislated 30 day turnaround time[1].

There are many potential risks and issues associated with ATIP Requests. A recent request from a Veteran resulted in increased media exposure and a review from the Privacy Commissioner when it was deemed that some staff inappropriately accessed a file. This negative media exposure resulted in a significant increase in ATIP requests with other Veterans concerned with access to their information. This increased workload without a corresponding increase in resources was reported to have put a strain on the well-being of employees and increased the risk of potential errors being created in an attempt to meet the 30 days legislated turn-around time.

To properly process these ATIP Requests, the Department is highly dependent on all staff to catalogue information properly. However, many staff have not been sufficiently trained in the art of managing information, so locating information can be complex resulting in longer turnaround times and increasing the potential for missed information. In addition, ATIP staff have difficulty verifying if the information received regarding the ATIP request is complete. Recently, a “Demystifying Information Management” training

[1] More detailed information on the number of requests and their turnaround times are presented in the annual *Report on the Administration of the Access to Information Act* and the *Report on the Administration of the Privacy Act*.

course was provided to some employees to help educate them on their role with information management. This course is expected to continue to be offered in the future.

Additionally, to improve accountability for the collection of information a new process was implemented effective April 1, 2011. It requires the respective Director General within a division to sign-off as to the completeness of the information assembled and identify potentially sensitive information before sending it to the ATIP unit. The new *Policy and Procedures for the Processing of Requests for Access to Records and Personal Information* under the *Access to Information Act* and the *Privacy Act* will also assist in the accurate and efficient delivery of ATIP services.

3.1.3 Privacy Impact Assessments (72)

There are many potential privacy risks and issues associated with the personal information which VAC has under its control. To address these potential risks and issues, the federal government's Privacy Impact Assessment (PIA) Policy requires that PIAs be conducted for new or redesigned programs. A PIA is a systematic process to determine whether new or existing information systems, administrative programs or services, or policies and practices meet basic privacy requirements. In addition, a PIA helps to ensure compliance with privacy legislation.

The *Directive on Privacy Impact Assessment* requires the conducting of a PIA before federal government institutions undertake any new initiative that could potentially have an adverse affect upon the privacy of individuals. The development of a PIA during the planning or early developmental stages of an initiative allows for privacy to be built into the design and implementation, identify possible compliance issues, and develop strategies to manage risk. Once completed, the PIA could also result in major re-working of Departmental plans depending on the outcome of the assessment.

With the Department's focus on their Transformation Agenda, the number of PIAs required will increase in the coming years. As there needs to be a concentrated effort performed in the development of PIAs, the effort from staff will remain high. A potential new directive may transfer the responsibility of creating PIAs to the business units while IM will continue to provide advice and guidance on this complex process. It should be noted that the complexity of the creation of PIAs has an extensive learning curve of approximately two years.

The recent privacy complaint has made VAC aware that improvements need to be made regarding VAC's management of the privacy of individuals. Although, privacy is not an exact science, anything regarding privacy has become very sensitive and has a

higher impact given the recent media attention to privacy issues. In addition, the task of creating PIA's is made more difficult by the fact that Treasury Board's *Privacy Impact Assessment Guidelines* are extremely complex and VAC's *Privacy Impact Assessment Policy and Procedures* are quite extensive. Adhering to these, as well as the *Directive on Privacy Impact Assessment* and the *Generally Accepted Privacy Principles* is a complex process.

3.1.4 Access to Information and Privacy (ATIP) (69)

Canadians require access to a wide range of information about government. There is compelling public interest in openness, to ensure that the government is fully accountable for its goals and that its performance can be measured against these goals. This renders the government more accountable to the electorate and facilitates informed public participation in the formulation of public policy.

In its day-to-day operations, federal government departments and agencies collect personal information from almost all Canadians. The *Privacy Act* gives Canadian citizens and people present in Canada the right to have access to information about them that is held by the federal government. It also protects against unauthorized disclosure of that personal information. In addition, it strictly controls how the government will collect, use, store, disclose, and dispose of any personal information.

The ATIP Office is consulted on issues relating to a range of matters, from polls, surveys, information management issues, privacy impact assessments, security of information, privacy caveats, and review of draft policies.

Staff require extensive knowledge on the handling of sensitive information and on whether information is protected and/or classified. A mishandling of information could lead to the loss or dissemination of sensitive documents. Compliance is also time consuming and removes focus from service delivery to individuals and recipients.

Since the recent privacy complaint, most activities involving privacy have been assessed as higher risk areas. To combat these risks, access controls over current information systems have increased. In addition, data capture controls have been modified based on the "need-to-know" principle. This includes new monitoring and control policies for the CSDN. Significant progress in this area has been made since the fall 2010.

VAC Guideline on Disclosure of Personal Information to the Minister was published in November 2010 as a result of the privacy complaint to prevent embarrassment to the

Minister and the department. Mandatory “Need-To-Know” training sessions for all staff were implemented (approximately 82% have been trained to date).

Increased scrutiny from other governmental departments such as the OPC has resulted in an upcoming audit by the Privacy Commissioner (fall 2011) and an annual external assessment (presently being conducted by Audit Services Canada) on VAC’s compliance of the *Access to Information Act* and the *Privacy Act* as required in the Minister’s 10-Point Privacy Action Plan. The scrutiny also resulted in a new *Privacy Protection Infrastructure* which was created in February 2011 to introduce the Privacy Steering Committee, the Chief Privacy Officer, and the ATIP Coordinator.

3.2 Medium Risk Entities

3.2.1 IT Security Policies (60)

IT security policy addresses constraints on functions and flow among them, as well as constraints on access by external systems and people. IT security is an integral part of continuous program and service delivery. Departments must view IT security as a business imperative as breaches may result in loss of service and/or trust.

The *Policy on Government Security* outlines the requirements for protecting government assets, including information, and directs the federal departments and agencies to which it applies, to have an IT security policy. The required policy can be a separate document or it can be policy statements within the departmental security policy. As a minimum, a departmental IT security policy must define the roles and responsibilities of IT staff. Additionally, it must make connections with other departmental policies, standards, and other regulatory requirements that relate to IT security.

The *Policy on Government Security* is derived from Section 7 of the *Financial Administration Act* which increases the policy’s importance when considering the new privacy landscape within government. Contravention or inappropriate access to VAC’s computer systems could result in a disruption of operations or even a complete breakdown of the IT infrastructure. Some employees may also be circumventing proper IT security procedures (and not receiving the essential security updates) by not shutting down their computers at the end of the workday, which is required by IT Security.

The introduction of new technology creates potential risk resulting in the requirement to create and update IT security policies. Some VAC IT policies are not being updated consistently resulting in incomplete processes and procedures. The *Policy on Government Security* (2009) replaced the 2002 *Government Security Policy* and the 2004 *Policy for Public Key Infrastructure Management in the Government of Canada.*

However, VAC is in the process of updating its policies to align them with the *Policy on Government Security*. The writing and interpretation of IT security policies require a high degree of knowledge. This knowledge would also be important when deciphering dependencies in regards to the integration of third party systems and applications with external contractors and other government departments.

3.2.2 Information Holdings (46)

Information Holdings is the umbrella entity for Information Holdings Specialist Service, Departmental Subject Records, Departmental Subject Records Repository Service, Regional Records Services, Client Records Operations Services, Ownership of Information, Retention Periods and Documentation Requirements.

Information Holdings provides VAC employees with advice and guidance on organizing information (electronic and paper), and obligations around retention and disposition of information.

The scanning pilot project of all of VAC's incoming mail in Matane, QC will bring about considerable changes to VAC's information holding procedures. VAC's incoming documents will be scanned and stored in Matane by Public Works and Government Services Canada (PWGSC) and electronic copies are to be sent to the respective departments' offices. This creates issues involving the sharing of information with PWGSC, and the storage and retention of information in Matane facilities. Furthermore, information may be lost or misplaced during the transportation between Matane and VAC offices.

VAC has an approved electronic document and records management system (EDRMS) in principle, but does not have the funding for implementation. The Department relies on several information management systems to collect, protect, analyze and manage information. Many employees are unaware of their responsibilities with regards to information management procedures. IM has recently introduced several training initiatives, including the "Demystifying Information Management" course, to inform employees of their responsibilities.

3.2.3 IM Continuity Plan (46)

The purpose of the IM Continuity Plan is to identify steps to be taken in the event that original hard copy documents have been damaged, destroyed, lost, or become inaccessible. The plan focuses on ensuring continued operations and availability of

records following a disruption, and deals with both client records and subject records. Accordingly, the IM Continuity Plan is an important component of the BCP.

VAC's current IM Continuity Plan is not sufficiently detailed as it does not define the accountabilities and responsibilities pertaining to VAC employees. More risks are created due to the lack of best practices and guidelines from central agencies and the increased workload on the IT/IM staff as a result of the privacy complaint.

VAC is highly reliant on information systems to recreate lost or damaged hard copy files. In addition, this increases the importance of both an IT Continuity Plan and an electronic document and records management system.

Furthermore, the scanning pilot project of all of VAC's incoming mail in Matane, QC will bring about considerable changes to VAC's IM Continuity Plan. VAC and all other federal government departments' incoming documents will be scanned and stored in Matane by PWGSC and electronic copies are to be sent to the respective departments' offices. In addition, information may be lost or misplaced during the transportation from VAC offices to the facility.

3.2.4 Threat and Risk Assessments (38)

As required by the *Operational Security Standards: Management of Information Technology Security* under the *Policy on Government Security*, Threat and Risk Assessments (TRAs) aid in the determination of security requirements that federal departments must fulfill to ensure the security of information and IT assets under their control.

VAC must conduct a TRA for every new or revised program or system. TRAs can be short and simple or far more detailed and rigorous, depending on the sensitivity, criticality, and complexity of the program, system, or service being assessed.

TRAs are becoming increasingly necessary as the number and severity of threats, vulnerabilities, and incidents increase. Furthermore, IT continues to rapidly advance in support of greater interconnectedness and improved service delivery. The entire department relies on a small TRA workgroup within IT Security. For the creation of TRAs, employees must have an immense understanding of the technology and related application to the entity. In line with Transformation, IT Security is planning to increase resources to aid in the additional workload. To enhance the effectiveness of TRAs, the workgroup plans to complete follow-ups on TRA recommendations in the future.

3.3 Low Risk Entities

3.3.1 Forms Management (21)

The Forms Management Unit designs and develops VAC's forms, manages the approval process to ensure they meet all Government of Canada requirements, and manages the printing and stocking of the forms.

The Transformation Agenda will result in the significant modification of forms. In addition, the "Need-to-Know" principle will result in increased scrutiny of forms and the determination for the requirement of certain information, thus creating operational inefficiencies. In response, VAC has issued new policies and guidelines for the management of information that enhances the processes for Forms Management.

3.3.2 Advice and Guidance (20)

IMSD staff are available to provide advice and guidance on all issues related to the management of information. Some of the most common include: Access to Information, Privacy (both employee and Veteran), documentation requirements, record keeping, forms management, user requirements for IT system design, ownership of information, IM clauses for Statements of Work and contracts, retention periods, consultation on project teams.

As part of the 10-point Privacy Action Plan and to increase employee awareness, IMSD has introduced several training initiatives for the management of information like the mandatory "Need-To-Know" session (attended by 82% of staff). Additionally, "Demystifying Information Management" sessions were held for employees within Head Office.

The practice of information management requires ongoing awareness. Although, VAC employees are currently being trained, additional training will be required to ensure that VAC's best practices for information management are carried out. While Advice and Guidance is a valuable service to all areas of the department and its employees, a disruption in this service could be provided immediately upon relocation.

3.3.3 Spam Monitoring and Prevention (19)

Spam is defined as the sending or receipt of unsolicited messages. The messages sent usually have no tie-in or bearing on the workplace environment and are quite often used to sell a product or service. To effectively prevent spam infiltration and the potential extraction of viruses, many software programs have been designed for spam filtering. The Department has been very proactive in identifying and deterring spam and other malicious messages. Additionally, the Department has created a protocol to deal with all spam messages.

3.3.4 IM Clauses for Statement of Work (SOW) and Contracts (16)

IMSD ensures certain requirements are included in the contractual terms and conditions for contractors and others engaged in work on behalf of VAC. IM also ensures that appropriate arrangements are put in place for information received from other federal departments, agencies, individuals, and entities outside of the federal government.

IM employees require knowledge of contract guidelines and related legislation as VAC has a high reliance on external contractors and must ensure clauses are in place to protect sensitive information. As most of these clauses are generic, this entity is rated as low risk.

3.3.5 Editing and Translation (16)

The VAC Editors' Office provides translation services internally to the Department provided that the document does not exceed 500 words. The document must be received from a Head Office employee and is not to be circulated outside the VAC Portfolio. In addition, it edits documents in both official languages. It proposes improvements to documents and compares the English and French to ensure that the translation is accurate; the style and format are consistent; and the grammar, spelling, and punctuation are correct.

PWGSC's Translation Bureau provides large scale translation, interpretation, and terminology services to federal departments and agencies in both official languages. VAC uses PWGSC's translation services for highly sensitive documents, including cabinet documents. In some cases, due to timeline constraints VAC does not always transmit classified documents utilizing the secure method. To date, there has not been any identified breach; however, bypassing secure methods exposes sensitive and classified documents.

3.3.6 Library (12)

The VAC Departmental Library provides full library services to all employees in Head Office, District, and Regional Offices. Additionally, library services are provided to the Veterans Review and Appeal Board and have limited on-site services available in Charlottetown for the general public. The library's collection focuses on topics such as military history, health and gerontology. It also includes departmental publications, other related government documents, and legislation.

The disruption of operations of this entity would have limited impact on day-to-day business as most resource material would be available through the internet, other federal organizations or public libraries. Also, the unavailability of this entity would have minimal impact on the delivery of services to our employees, Veterans or their families, and the general public.

4.0 CONCLUSION

Since the fall of 2010, the Department has responded strongly to public criticisms regarding management of information. Accordingly, significant progress has been made. Given the importance of information management and the current sensitivity even with this progress, management should be aware that some activities continue to remain high risk. In addition this risk assessment has identified some overarching risks that the review team deemed require management action:

- The absence of a fully operational and tested IT Continuity Plan exposes the Department to significant risk and could result in interruptions of service delivery.

- The absence of an approved Emergency Operations Centre places the Department at risk in the event of a major incident.

- Development of an Electronic Document and Records Management System has been approved in principle; however, funding has not been obtained. The current absence of such a system is problematic for capturing and receiving information.

- VAC is not meeting the 30 day turnaround time for Access to Information and Privacy (ATIP) Requests which is not compliant with the *Access to Information Act.*

- The current IM Continuity Plan lacks sufficient detail as to the roles, responsibilities, and associated accountabilities. The process of shipping information to and from Matane, Quebec, increases the risk for lost or misplaced information increasing the importance of a well developed IM Continuity Plan.

- The intent of Transformation is to overhaul service delivery and reduce program complexity, thus requiring additional Privacy Impact Assessments. The resulting impact will be increased workload and a possible shift in responsibilities.

Recommendation

It is recommended that the Assistant Deputy Minister, Corporate Services table the above identified risks to Senior Management Committee to determine the appropriate departmental approach to manage these risks.

Management Response

Management agrees with this recommendation. Action will be taken to schedule the IM Risk assessment at the Senior Management Committee within the next number of weeks. A recent Information Management briefing delivered to SMC on June 15th highlighted many of the concerns however; the results of this review will help inform the work that needs to be completed in the coming months.

Management Action Plan

Corrective action to be taken	Office of Primary Interest	Target date
Initial IM Briefing – Update	ITIM	June 2011
SMC Briefing – IM Risk Assessment	A&E/ADM CS	July 2011
Update IM Strategy and Develop Implementation Plan	ITIM	September 2011
Execute plan to coincide with transformation agenda	ITIM	March 2014

5.0 DISTRIBUTION

Deputy Minister

Associate Deputy Minister

Veterans Ombudsman

Chief of Staff to the Minister

Departmental Audit Committee Members

Assistant Deputy Minister, Corporate Services

Assistant Deputy Minister, Policy, Communications and Commemoration

Assistant Deputy Minister, Service Delivery

Director General, Communications

Director General, Departmental Secretariat and Policy Coordination

Director General, Human Resources

Director General, Information Technology and Information Management

General Counsel, Legal Services Unit

Executive Director and Chief Pensions Advocates

Executive Director, Ste. Anne's Hospital

Director, Briefing, Coordination and Liaison

Director, Information Management Services

Director, Security and Real Property Services

Executive Advisors to the Deputy Minister

Office of the Comptroller General (Internal Audit Registrar)

Office of the Auditor General

APPENDIX 1: RISK EXPOSURE ANALYSIS – WEIGHTED SCORE RANKING

				Key Risk Factors									
				Degree and recentness of change		Degree of complexity		Legislative and other compliance requirement		Degree of knowledge		Degree of dependency	
Rank	**Entity**	**Weighted Score**	**Significance**	**L**	**I**	**L**	**I**	**L**	**I**	**L**	**I**	**L**	**I**
High Risk Entities													
1	Business Continuity Planning (including the IT Continuity Plan)	90	3	3	3	3	3	3	3	3	3	3	3
2	ATIP Requests	78	3	3	3	3	3	2	3	2	2	2	3
3	Privacy Impact Assessments	72	3	2	3	2	3	1	3	2	3	2	3
4	Access to Information and Privacy	69	3	3	3	2	2	3	2	2	2	2	2
Medium Risk Entities													
5	IT Security Policies	60	3	2	2	2	1	2	2	2	2	2	3
6	Information Holdings	46	2	3	2	2	2	1	3	2	3	2	3
7	IM Continuity Plan	46	2	3	3	3	3	2	2	1	2	2	2
8	Threat and Risk Assessments	38	2	2	2	2	2	1	3	2	2	1	2
Low Risk Entities													
9	Forms Management (IMSD)	21	1	2	3	1	3	1	3	2	2	2	2
10	Advice and Guidance (IMSD)	20	1	2	3	2	1	1	2	2	3	2	2
11	Spam Monitoring and Prevention	19	1	3	2	2	2	1	1	2	2	2	2
12	IM Clauses for SOW and Contracts	16	1	1	1	1	1	1	3	1	2	2	3
13	Editing and Translation	16	1	2	1	2	1	1	3	2	1	1	2
14	Library	12	1	1	2	1	1	1	1	1	2	1	1

Legend:	
L = Likelihood	3 = High
I = Impact	2 = Medium
	1 = Low