

TABLE OF CONTENTS

STATEMENT OF ASSURANCE	i
EXECUTIVE SUMMARY	1
1. INTRODUCTION.....	11
1.1 Background.....	11
1.2 Organizational Structure	12
1.3 Audit Objectives and Scope.....	13
1.4 Audit Methodology.....	14
2. FINDINGS—MANAGEMENT FRAMEWORK.....	15
2.1 Policies, Guidelines, Standards.....	15
2.2 Organization and Responsibilities	20
2.3 Strategies and Planning.....	21
2.4 Resources	25
2.5 Management Reports	27
2.6 Communicating.....	28
2.7 Human Resources Management	28
2.8 Training.....	29
3. ELECTRONIC RECORDS PROCESSES.....	31
3.1 Electronic Information Stored Outside of Application Systems	31
3.2 Application Systems	39
4. PRESERVATION OF INFORMATION AND INFORMATION OF ENDURING VALUE	45
5. COURT REQUIREMENTS	47
6. SECURITY OF ELECTRONIC INFORMATION.....	49
6.1 Processing of Classified Information.....	49
6.2 JustAccess	50
7. EDMS	53
7.1 Work Completed Toward an EDMS	53
7.2 Requirements and Considerations for an EDMS	54
7.3 Potential Benefits from an EDMS	55
7.4 EDMS Used by DLSUs	56

8. IMPACT OF ELECTRONIC INFORMATION MANAGEMENT ISSUES	57
8.1 Productivity.....	57
8.2 Corporate Memory.....	60
8.3 Access to Information and Privacy	61
9. RECOMMENDATIONS AND MANAGEMENT RESPONSE.....	63

STATEMENT OF ASSURANCE

We have completed the internal audit of the Management of Electronic Information. The overall objectives of the audit were:

- a) to review and assess the adequacy of the framework in place for the management of electronic information;
- b) to review and assess the extent to which electronic information is appropriately managed.

The internal audit was conducted in accordance with the Treasury Board Secretariat (TBS) *Policy on Internal Audit* and the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*.

- a) The audit team assessed the management control framework against criteria derived from the Treasury Board Secretariat (TBS) *Policy on the Management of Government Information (MGI)* and the *Library and Archives of Canada Act* as well as TBS audit guides.
- b) The audit team assessed the management control framework against departmental policies.
- c) The audit team assessed the management of electronic records against TBS and departmental policies.
- d) The audit team assessed the extent to which operations, procedures and computer systems are managed with due regard to economy, efficiency, and effectiveness.

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time of the audit and against the audit criteria. It should be noted that the conclusions are only applicable for the areas examined.

LIST OF ACRONYMS

ATIP	Access to Information and Privacy
CIO	Chief Information Office
CLPS	Criminal Law Policy Section
DLSUs	Departmental Legal Service Units
EDMS	Electronic Document Management System
IFMS	Integrated Finance and Materiel System
IM	Information Management
IMB	Information Management Branch
IMD	Information Management Division
IT	Information Technology
LAC	Library and Archives Canada
MGI	Management of Government Information
PDF	Portable Document Format
PKI	Public Key Infrastructure
PRI	Personal Record Identifier
PWGSC	Public Works and Government Services Canada
RDIMS	Records, Documents, Information Management System
RIMS	Records Information Management System
RO	Regional Office

EXECUTIVE SUMMARY

In the *Policy on the Management of Government Information (MGI)* issued by Treasury Board in 2003, information is identified as a valuable asset that departments must manage as a public trust on behalf of Canadians. Effective information management (IM) makes government program and service delivery more efficient, supports transparency, collaboration, informed decision-making in operations, and preserves historically valuable information. Sound IM is increasingly important for the Department of Justice as it uses information technology to record its business, do research, and serve clients and Canadians.

Information is a global term that includes records. Records include correspondence, memoranda, drawings, pictorial or graphic work, photographs, film, microform, sound recordings, videotapes, and machine readable records. Many records are in electronic form. For example, the Department of Justice keeps electronic information in e-mail messages and attachments, on shared and personal drives, in computer application systems, and on Intranet and Internet servers. In this report we will refer to both information and records as appropriate.

The Department has been producing electronic records with computer application systems since approximately the 1950s and with personal computers (PCs) and networks since the 1980s. At present, the Department has a vast amount of electronic information. It is estimated that the Department has at least 5,343 gigabytes of data.

Central agencies establish Government-wide requirements for IM with which the Department must comply. The Treasury Board *Policy on the Management of Government Information (MGI)* provides direction on how federal government institutions should manage information.

The *Policy on the MGI* specifies accountabilities for: deputy heads, senior executives, all public service employees, information specialists, the Treasury Board of Canada Secretariat, the National Archives of Canada, and others. In particular, the deputy heads are responsible for ensuring implementation of this policy; promoting a culture that values information; allocating appropriate resources to support information management; and designating a senior executive to be accountable for implementing the policy. Responsibilities of senior executives accountable for implementing this policy include: championing information management; co-ordinating the

strategic planning, resourcing, and implementation of information management activities, including training and development for staff; ensuring that the effectiveness of policy implementation is periodically assessed; and ensuring that information management accountability frameworks are in place.

The recommendations of this report are directed to the Chief Information Officer (CIO) who currently is taking leadership in information management. However, the CIO has limited authority for the implementation of the policy.

Library and Archives Canada is responsible for approving records disposition authorities, storing inactive records, and receiving information of historical value.

The IM function at the Department of Justice is primarily the responsibility of the Information Management Division (IMD), which is one of five divisions within the Information Management Branch (IMB). IMD provides functional direction on IM for the whole department and has certain line responsibilities. Regional directors of IM/IT are responsible for providing IM services in their regions. In Departmental Legal Service Units, General Counsels are responsible for IM. The Director General, Communications Branch is responsible for providing strategic advice on Web content and with Executive Council and BIT.com for providing operational governance for all departmental Web activities. Responsibility for ensuring that information posted on departmental Web sites is recorded and managed through the lifecycle in accordance with the Management of Government Information Policy is shared among the CIO, the Director General, Communications Branch and departmental managers.

The audit covered the activities relating to the management of electronic information at headquarters; the regional offices located in Edmonton, Montreal and Toronto; and the following DLSUs: Fisheries and Oceans, Health Canada, Natural Resources, Agriculture and Agri-Food, Citizenship and Immigration, and Treasury Board Secretariat.

Management Framework

The Department's current policy calls for its official records to be maintained in paper or, preferably, in electronic form. Until recently little attention was given to the management of electronic information. IMB has been aware of the need to manage electronic records, and in 2004, IMB took some initial steps to remedy the situation. At present, the official departmental records are kept in paper form.

In November 2004, IMB issued the *Information Management (IM) Policy* to ensure that information, including electronic information, under the control of the Department of Justice

Canada is effectively managed through the lifecycle. However, regarding the new policy, IMB does not have standards and directives that effectively detail the processes by which electronic information is to be managed, and IMB is yet to address other needed elements, such as training, resources, tools, and monitoring. Our interviews showed that most staff are unaware of the *Information Management (IM) Policy*. It is our view that until processes are established, the policy alone is insufficient. As relevant standards, processes, and systems are put in place, increased direction should be provided to departmental units and staff to manage electronic information.

The *Guidelines on the Use of the Corporate E-mail System* issued by IMB in September 2004 give advice on how to manage e-mail messages as records. However, the Department has not established mandatory processes for appropriate management of electronic records. Most persons we interviewed were unaware of these guidelines.

The *Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites* was last revised in March 2004. This policy addresses the management of Web sites. There is poor compliance with this policy for records management, since required software and processes to manage Web contents as records are not in place.

A lack of departmental standards affects IM in a number of ways. We found that staff members establish individual methods of dealing with electronic information. Furthermore, standards need to be established that define when the paper or electronic record constitutes the official record or when maintaining both is appropriate. In our opinion, given the widespread use of electronic information, staff productivity benefits should be referenced in new electronic IM standards and processes.

A prerequisite for improving the management of electronic information is the revision of the current file plan (classification structure for records). The current file plan is outdated even for paper records. IMB is taking steps to revise the file plan, and we were informed that the revised version will be ready in 2005.

The Department must follow records disposition authorities approved by Library and Archives Canada (LAC). The current disposition authority applies only to paper records. LAC is yet to approve a new disposition authority (to include electronic records) that has been requested by the Department.

The Department currently has an organization in place for IM but it is primarily focused on the management of paper records. IMB management recognizes that changes are necessary and has taken initial steps toward improvement such as issuing the *Information Management (IM) Policy*,

obtaining approval for a strategy, and planning the preparation of a human resources plan. The human resources plan should address the number and specific skills of the staff associated with IM in the Department. In our opinion it is likely that increased resources will be required to maintain current processes for dealing with paper files and to implement new processes for dealing with electronic records.

In 1995, the number of staff for records management was reduced throughout the Department. Although the number of total departmental staff has significantly increased since that time, there has been little change in the number of staff assigned to records management. IMD has changed its staff composition decreasing those who are qualified to deal with paper records and adding staff with qualifications to manage electronic information. This has improved the strategic capability of IMD and initiatives to manage electronic information have started.

IMB first assigned permanent resources to electronic IM in 2004/05. IMB currently has three staff on a part-time basis for a total of 1.5 FTEs in the Information Management Division. The regional offices and DLSUs have no dedicated staff for electronic IM. Staff who were previously managing paper records are tasked with managing electronic information but they have no formally assigned responsibilities for this task. DLSUs have little support and funding for IM from the Department. They rely on client staff for IT support and some use the client's Electronic Document Management System (EDMS). However, there is no assistance available from client staff to manage information in accordance with Department of Justice requirements.

A discussion of the strategic approach needed in the Department for the management of electronic information needs to take into consideration IMD's plans to implement an EDMS. An EDMS would allow staff to file electronic records in a departmental system that has the appropriate functions for records management. It is our view, however, that the implementation of an EDMS will not provide a complete solution to electronic IM issues the Department is encountering. Management should continue other efforts to improve electronic IM.

In 2004 IMB prepared two strategic reports which identified several issues and provided information for the preparation of *The Business-Driven Vision of Information Management for Justice Canada* that was presented to and approved by BIT.COM in November 2004. As a result, IMB was asked to prepare an implementation plan for the appropriate management of electronic records. In our opinion the plan should identify preliminary activities, such as processes and tools required to facilitate the management of electronic records and thus introduce an element of sustainability and potentially improve productivity. Also, links with other systems and a preliminary model of departmental IM architecture would assist in more effective and economic improvements in IM.

We were informed that the implementation plan will identify resources required. To appropriately manage electronic information will require significant funding. A preliminary estimate is approximately \$14 million. We recommend that complete costs, including regional and DLSUs costs, are estimated for the implementation plan to improve the management of electronic information.

Apart from funding, the implementation of the plan will require providing staff with training in new skills. Records management staff who are responsible for managing paper records will need further training, or additional staff with appropriate qualifications for the management of electronic information will be required. Information management is now a defined discipline with specific degrees. Training is currently available for staff on how to use software that creates or uses electronic information but not on how to manage electronic information. IMB is developing training materials that can be used online and will be made available to Regional Offices (ROs) and DLSUs.

IMB is undertaking further activities to improve IM. A pilot of the Records Document Information Management System (RDIMS), the Government of Canada shared system and EDMS, is under way. Further pilots were to be conducted before a final decision is made on how to select an EDMS or whether to adopt RDIMS for the Department. Also, activities have been initiated to centralize RIMS and iRIMS, which is a preliminary step to the implementation of a departmental EDMS.

The Toronto RO conducted a survey and found that there were several deficiencies with records management. The regional office is taking steps to correct these deficiencies such as offering more training, reviewing closed paper files, and making section directors aware that staff are not always recording case documents in iCase. Other ROs and DLSUs, which have not conducted similar surveys, have taken minor initiatives and are waiting for direction from Headquarters.

We found little statistical management information available on electronic information that may permit analysis and quantification of how electronic information is being used and stored. Yet we were informed that staff make substantial use of electronic information. Regular reports on electronic information are required.

Electronic Records Processes

In addition to application systems there are several IT services that store or process electronic information. These include e-mail; various personal, shared and other drives; removable media; departmental Intranet; Internet; scanned information; and SharePoint, a commercial network system. Of these, e-mail has become the preferred storage.

The e-mail service is very important. We were told by lawyers that 50% to 90% of their work is conducted by e-mail. Most staff members indicated that it is the preferred service for storing electronic information. We found that staff use e-mail inefficiently. Staff do not always organize their e-mail messages into folders, import messages into iCase, print e-mail messages as required, or use appropriate filters or other functions that assist in automatically organizing e-mail messages. Staff are also unclear about who is responsible for keeping the official copy of an e-mail when there are multiple recipients.

After the e-mail system, the personal drives are the most heavily used. Usually a personal drive is accessible only by the corresponding network account holder. The personal drive is used to create documents that may be printed for distribution and filing or attached to an e-mail. Shared drives are typically used for sharing information within a section. The information is not accessible to other sections. Furthermore, personal folders are set up on the shared drive for staff to use as they choose. A key issue with the personal and shared drives is the lack of standards to ensure consistency and efficient use. Other issues are similar to those of e-mail. Generally, documents or case records are not stored in such a manner that they may later easily be imported into an eventual EDMS or iCase. Most sections we visited have shared drives that contain outdated information. In our opinion, a strategy is required for the use of shared drives and for other methods of sharing information.

Department of Justice staff have access to Web information on the departmental Intranet and Internet. We were told that in headquarters and ROs there are about 200,000 documents on the Intranet. We were also told that the departmental Internet site has around 60 sub-sites, containing approximately 60,000 documents plus 8,100 statutes and regulations. This site is accessible to the general public. At present no official archive of Web site contents is maintained. Older versions of content are not always archived and are not linked with the departmental records management function. The Electronic Communications Division is examining standards for archiving Web content and using software such as a Content Management System (CMS), which would assist the archiving.

Several sections are scanning documents to create electronic versions for various purposes. These electronic documents exist in both text and image formats. There is a significant amount

of scanning in the Department and there are no standards for formats and resolution except for RingTail, a litigation support application system. Standards are important to ensure compatibility, to facilitate future access, and to avoid unnecessarily large files or files that are difficult to read.

Applications systems are computer softwares that apply the capabilities of a computer to the performance of tasks related to a specific business function. Most can be accessed from any departmental office. Departmental application systems fall under two types: legal systems (such as iCase, Litigation Support Systems, LOPORS, GASPARD, and LIMS) and non-legal systems (such as Information Financial Management System (IFMS), PeopleSoft, and Salary Management System (SMS)). Some application systems contain documents that may be captured by an EDMS as they are prepared. However, none of these systems are intended to be records management systems. These systems are not intended or designed to meet the requirements of departmental IM. Most do not have reference numbers to allow for linking to an eventual EDMS. These systems do not usually delete information, which minimizes the risk of information being lost. Including application systems in the departmental management of electronic information will be a complex task. It is our view that the Department needs to develop a strategy for determining the information that will be included in an eventual departmental EDMS or the alternative approaches to be used to manage the electronic information contained in application systems.

The electronic records processes we have discussed are used for sharing information. In the Department of Justice information sharing is inefficient. Each IT service and application system requires separate searches. Some sections of the Department are spread across different cities or locations. These sections make greater use of the Intranet for sharing information because the shared drives of other locations or sections are inaccessible. For this reason the Prairie Region is increasing the use of SharePoint (a commercial Web software product) for sharing information. Application systems are used for sharing information but with limited success for legal systems.

Court Requirements

There is a trend for courts to demand that original electronic records are presented as evidence. This is because the paper record may not completely and accurately represent the electronic record. In one RO we were informed that some courts are already demanding that certain records be presented in electronic format. Also, we were told that another RO had maintained additional backup tapes as a precaution in case a court requested them in a high-profile prosecution. In other countries courts are already asking for the original electronic records. We note that the *Policy on Corporate DOJ Network Backups*, December 2004 states that backup records will only be kept for one year in the National Capital Region, Regional and Satellite Offices. The purpose

of backup records is to recover data from computer malfunctions and disasters. We concur with IMB that using backup tapes is inefficient for accessing older records. Therefore, other processes are required for operations that need to store or access records that are older than a year.

Processing of Classified Information

The Department requires that Protected C and Classified information be processed in a stand-alone computer which is kept secure by physical means. This includes keeping it in a room that meets the requirements for processing and storing Classified information. With the amount of Classified information processed in the Department, this requirement is no longer practical, although it is complied with in a few cases. There is currently a requirement for easily processing and e-mailing Classified information. We found that generally Classified information is prepared and stored using IT services that are not approved to do so. The departmental IT Security Coordinator is aware of this problem and we were told that there are plans to address it.

EDMS

The Department has undertaken some pilot projects relating to electronic document management, and certain DLSUs are using systems to record and access electronic records.

The requirements for an EDMS have been discussed in several of the pilot assessment reports and in the IMB strategic reports completed in 2004. None of these reports documents complete user requirements for an EDMS. The implementation of an EDMS will be a large and complex undertaking.

An EDMS would bring significant benefits to the Department. It would save staff time, improve the quality of work, provide better access control for documents and files, and decrease the storage requirements for information by reducing duplication.

In three DLSUs we visited, some staff were using some form of EDMS either provided by the client department or developed by the DLSU. No direction can be provided to DLSUs with respect to an EDMS until the Department has taken a decision on a plan for its own EDMS and developed a strategy for the DLSUs.

Impact of Electronic Information Management Issues

Users find the existing processes (for both paper and electronic records) useful. They are able to find information although not all required information is always available. A few said they are satisfied to work with the existing processes. However, most staff members indicated they need

better processes for dealing with electronic records. There are a number of issues and risks with using paper records: using paper is time consuming; paper takes up significant space, which is costly; paper files are not accessible if they are stored in offices where the file room is closed after regular office hours; paper files are not easily accessible if they are stored in other locations or in other staff members' offices. Also, it is difficult and at times impossible to search through or physically carry copies of all the necessary documents for a large file. However, staff indicated that paper is sometimes the preferred medium.

In searching for necessary information, efficient use of time is important for staff. Information (in both paper and electronic formats) is found in various locations that require different search tools. A significant amount of paper information is also kept in electronic form; electronic information is often duplicated in different systems and IT services. When existing information is not found, there is a resulting duplication of work.

Inadequate IM processes can impact quality of work in various ways: consistency in departmental legal positions or the appropriateness of legal advice may be compromised as a result of inadequate sharing of information; lawyers have on occasion released to clients and other lawyers or presented at court the wrong version of a document; and lawyers may produce documents based on less research than is required or appropriate.

We found that corporate memory is not well maintained in the Department. Paper files are incomplete because much electronic information is not printed and some electronic information is deleted without being printed or kept in a manner that makes it practically inaccessible. Paper records are no longer adequate for tracing all the information that led up to a legal decision or that was related to an issue. Information pertinent to an issue may be divided among many locations. Currently, there is no requirement to keep electronic records once they are printed. The deletion of electronic records is a loss of corporate memory.

As noted in this report, the Department has not been complying with policies (government-wide and departmental) on the management of electronic information. We note however that the Department is waiting for Library and Archives Canada to issue a new records disposition authority regarding the destruction or disposal of electronic records and the transfer of e-records to LAC. The Department is also awaiting a directive from LAC regarding acceptable formats for the transfer of e-information.

The management response to the recommendations contained in this report was provided by the Chief Information Officer, Information Management Branch and the Director General, Communications.

The CIO, IMB also provided the following general comment.

The Information Management Branch (IMB) acknowledges the importance of the audit recommendations and is generally supportive of these. However, it cannot commit itself to completing the work required to address all the issues identified.

Based on the Strategic Information Management Framework approved by senior management before the audit, IMB will continue to work at improving the overall state of Information Management (IM) in the Department, within available resources. Actions will remain focused on areas with the highest return on investment and / or the highest business risks faced by the department.

Over the foreseeable future, investments will mainly be concentrated on raising IM awareness of employees and managers, implementing an electronic document management system, and building a core human resource capacity to support the departmental IM program.

1. INTRODUCTION

1.1 Background

In the *Policy on the Management of Government Information (MGI)* issued by Treasury Board on May 1, 2003, information is determined to be a valuable asset that the Government must manage as a public trust on behalf of Canadians. The policy states that effective information management makes government program and service delivery more efficient, supports transparency, collaboration, informed decision-making in operations, and preserves historically valuable information.

Sound information management is increasingly important for the Department of Justice as it uses information technologies to record its business, do research, and serve clients and Canadians.

Government information is defined in the *MGI* policy to include information created, received, used, and maintained regardless of physical form, and deemed to be under the Government's control in the conduct of its activities or in pursuance of legal obligations. Information is therefore a global term that includes records. Records include correspondence, memoranda, drawings, pictorial or graphic work, photographs, film, microform, sound recordings, videotapes, and machine readable records. For example, the Department of Justice keeps electronic information in e-mail messages and attachments, on shared and personal drives, in computer application systems, and on Intranet and Internet servers. In this report we will refer to both information and records as appropriate. Currently most departmental information is in records.

The Department began using computer application systems in approximately the 1950s. Since the 1980s when personal computers (PCs) first started to be used, office support software such as text processing and spreadsheets have created and stored electronic information. At present, the Department has a vast amount of electronic information. A presentation prepared in 2004 by the Information Management Branch (IMB) indicated that there were 5,343 gigabytes of data on e-mail servers and personal and shared drives. This equals 25,672 boxes of paper and is not inclusive of all electronic information.

The Department has two major types of information: legal information and non-legal information. Electronic records for both are maintained on computers within the Department, on clients' computers in Departmental Legal Service Units (DLSUs), and on computers used by legal agents.

Central agencies establish Government-wide requirements for IM with which the Department must comply. The Treasury Board *Policy on MGI* provides direction on how federal government institutions should manage information.

The *Policy on the MGI* specifies accountabilities for: deputy heads, senior executives, all public service employees, information specialists, the Treasury Board of Canada Secretariat, the National Archives of Canada, and others. In particular, the deputy heads are responsible for ensuring implementation of this policy; promoting a culture that values information; allocating appropriate resources to support information management; and designating a senior executive to be accountable for implementing the policy. Responsibilities of senior executives accountable for implementing this policy include: championing information management; co-ordinating the strategic planning, resourcing, and implementation of information management activities, including training and development for staff; ensuring that the effectiveness of policy implementation is periodically assessed; and ensuring that information management accountability frameworks are in place.

Library and Archives Canada is responsible for approving records disposition authorities, storing inactive records, and receiving information of historical value.

1.2 Organizational Structure

The information management function at the Department of Justice is primarily the responsibility of the Information Management Division, which is one of five divisions within the Information Management Branch. However, central agencies such as Treasury Board and Library and Archives Canada (LAC) establish government-wide requirements for IM with which IMB must comply. Also, the Department must meet certain information requirements prescribed by legislation.

Within the Department, BIT.COM¹ oversees IM/IT activities at a strategic level and is responsible for approving key documents for information management. The head of IMB is the Chief Information Officer (CIO). Under the guidance of BIT.COM, the CIO in collaboration

¹ BIT.COM is a senior management committee responsible for IM/IT investment that reports to the Executive Council.

with regional directors and heads of headquarters IM/IT units is responsible for championing information management and providing leadership and coordination of information management on a Department-wide basis.

In the Information Management Branch (IMB), its Business Support, Applications and Services Division is responsible for various national application systems involving electronic records. The Technology Services Division has responsibility for the national and capital region IT infrastructure that supports various IT services such as e-mail, network server drives, and Web server drives. Regional Offices manage their own IT infrastructure and network drives under the functional direction of the CIO. The Information Management Division has responsibility for information management.

Regional directors of IM/IT are responsible for providing information management services in their regions, in consultation with IMD. In Departmental Legal Service Units (e.g. Agriculture Canada, Fisheries and Oceans Canada, Natural Resources Canada), General Counsels are responsible for information management with the support of IMD.

The Director General, Communications Branch is responsible for providing strategic advice on Web content. Along with Executive Council and BIT.com, the DG, Communications Branch is also responsible for providing operational governance for all departmental Web activities, that is, for ensuring that web publishers follow relevant government policies. It should be noted however that the CIO, the DG, Communications and managers across the Department of Justice share responsibility for ensuring that information posted on departmental Web sites is recorded and managed through the lifecycle in accordance with the Management of Government Information Policy. The nature of this issue is such that a solution will require more sustained departmental participation, better defined accountabilities and roles, as well as new software and processes.

1.3 Audit Objectives and Scope

The audit reviewed and assessed:

- the adequacy of the framework in place for the management of electronic information (processes and practices related to planning, organizing, controlling, directing, and communicating, and the management of human, financial, and materiel resources devoted to information management);
- the extent to which the management of electronic information complies with the *Policy on the Management of Government Information (MGI)* and the *Library and Archives of Canada Act*;

- the extent of compliance with the *Access to Information Act*, *Privacy Act*, and the *Government Security Policy* issued by Treasury Board Secretariat (TBS);
- the adequacy of linkages with Library and Archives Canada, Treasury Board Secretariat, departmental regional offices, and DLSUs.

The audit covered the management of electronic information at headquarters; the regional offices of Edmonton, Toronto, and Montreal; and the following DLSUs: Fisheries and Oceans, Health Canada, Natural Resources, Agriculture and Agri-Food, Citizenship and Immigration, and Treasury Board Secretariat.

1.4 Audit Methodology

The methodology consisted of a review of pertinent documentation and systems, interviews with relevant staff, and appropriate testing.

The methodology employed in this audit included:

- interviews with the Chief Information Officer;
- interviews with staff of the Information Management Branch;
- visits to three regional offices;
- visits to six DLSUs;
- interviews with various departmental personnel;
- interviews with representatives from Library and Archives Canada and Treasury Board.

The fieldwork for the audit was completed in December 2006.

2. FINDINGS—MANAGEMENT FRAMEWORK

2.1 Policies, Guidelines, Standards

The Treasury Board *Policy on the Management of Government Information (MGI)* provides direction on how federal government institutions should create, use, and preserve information to fulfill their mandates, support program and service delivery, achieve strategic priorities, and meet accountability obligations prescribed by law.²

Library and Archives Canada is responsible for approving records disposition authorities³, storing inactive records, and receiving information of historical value.

The Department's current policy calls for its official records to be maintained in paper or, preferably, in electronic form. However, at present, the official departmental records are kept in paper form. Staff are directed to print electronic records and file them as paper records. Over the last few years, IMB in conjunction with most of the federal government has determined that it is no longer practical to follow this practice.

Accordingly on 3 November 2004, IMB issued the *Information Management (IM) Policy* to ensure that information, including electronic information, under the control of the Department of Justice Canada is effectively managed. This policy is a key element of governance. It applies to all information regardless of physical form, and documents principles and responsibilities. However, the audit team found that there are no directives in IMB that detail the processes by which electronic information is to be managed nor that address other needed elements, such as training, resources, tools, and monitoring. There are no appropriate standards, manuals, and procedures for the management of electronic information (e.g. file-naming standards including for multiple draft versions; naming folders; determining what to keep, what to delete, formats to use, and how to organize information). As a result, IMB offers little direction to departmental operational units with respect to the management of electronic information. Our interviews

²From the Preface, *Policy on the Management of Government Information*, Treasury Board of Canada Secretariat.

³ To meet legislative requirements, the National Archivist issues Records Disposition Authorities to enable government institutions to dispose of records which no longer have operational value, either by permitting their destruction (at the discretion of institutions), by requiring their transfer to the National Archives, or by agreeing to their alienation from the control of the Government of Canada.

showed that most staff are unaware of the *Information Management (IM) Policy*. It is our view that until processes are established, the policy alone is insufficient.

Proper management of electronic information is necessary in order to comply with legislative requirements and government-wide policies. Furthermore, with the increasing importance of electronic information, it is good business practice to decrease dependency on paper. Given the widespread use of electronic information, it will be important for policies and related documents to explicitly indicate the impact of efficient electronic information management on staff productivity. For example, delays in processing and lack of access to electronic information impact staff productivity significantly. (For further discussion on the impact on productivity, see “Productivity”)

The *Guidelines on the Use of the Corporate E-mail System* issued by IMB on 4 September 2004 give advice to departmental staff on how to organize e-mail and manage e-mail messages as records. However, because the Department has not established standard processes for appropriate management of electronic records, the guidelines also offer staff the option of printing e-mails. Most persons we interviewed were unaware of these guidelines. Also, although guidelines can be useful, they are not mandatory for employees. We found that the e-mail and records section of the guidelines was confusing. Nor do the guidelines mention important departmental computer systems such as iCase and LOPORS where staff should be storing certain e-mail records. The iCase system contains case documents and LOPORS contains opinions of national significance. We found that staff were not always importing e-mail messages or other documents into these systems.

Effective records management practices directly impact productivity. Standards, reference documents, and processes need to explicitly illustrate the link between sound records management and improved productivity. In our opinion, increased staff awareness of the productivity benefits to be gained would result in improved staff compliance with required records management practices.

The *Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites* was last revised on March 5, 2004. This policy addresses the management of Web sites for communications, records management, security, and privacy. There is poor compliance with this policy for records management, since required software and processes to manage Web contents as records are not in place.

A lack of departmental standards affects information management in a number of ways. We found that staff members establish individual methods of dealing with electronic information. As a result, they store information in a form that in the future will be more difficult to collect into an

Electronic Data Management System (EDMS). The implementation of an EDMS forms part of the Department's future plan for information management. Although some units have established standards for some electronic information management, compliance is typically poor. Also, there is a need for staff to be trained in organizing information so that it will not require reorganizing in the future. Furthermore, standards need to be established that define when the paper or electronic record constitutes the official record or when maintaining both is appropriate.

The Department has many application systems, both legal (e.g. iCase, LOPORS, LIMS) and non-legal (e.g. administrative support systems such as PeopleSoft), that contain a large amount of electronic information. These application systems do have standards for the information they contain but these systems are designed to meet the requirements of specific operations and not of departmental information management.

Currently IMB is able to establish guidelines for regional offices (ROs) and DLSUs but does not have the authority to enforce them. Ultimately, for the Department to manage electronic information effectively, departmental standards will be required that can accommodate the special requirements of different units. We understand that the Department is developing accountability frameworks that could address this issue. We note that the DLSUs we visited have a clear understanding that information of the DLSUs is under the control of the Department of Justice.

A prerequisite for improving the management of electronic information is the revision of the current file plan (classification structure for records). The current file plan is outdated even for paper records. IMB is taking steps to revise the file plan and we were informed that the revised version will be ready in 2005. DLSUs are also aware that their current file plans need revision and they plan to revise them in coordination with IMB. A few have already revised their file plans. For these few a further revision may be required when the departmental file plan is available.

Treasury Board's *MGI* policy requires the use of electronic systems as the preferred means of creating, using, and managing information. The policy also requires that information collected or made available electronically is accurate, complete, relevant, and clear, and accessible and usable over time and through technological change. The Department has partially met this requirement with regard to information managed in application systems but not with respect to other information management. We found that the Department is not meeting these key requirements.

The Department must comply with disposition authorities set by Library and Archives Canada (LAC) and provide LAC with information of historical value in a format acceptable to LAC. The current disposition authorities apply only to paper records. LAC is yet to approve the disposition

authorities, which include electronic records, that has been requested by the Department. LAC is in the process of defining standards for electronic information.

Recommendations and Management Response

1. It is recommended that the Chief Information Officer ensure that:

- a) Standards for the management of electronic information including e-mail are issued so that the information can be easily managed as departmental records.**

The Information Management Branch is in the process of completing a Guideline on Managing Departmental Information. The implicit “standard” for the long-term management of information created in Outlook is RDIMS, the Government of Canada shared services initiative for electronic document and records management. Information Management Branch has received the endorsement of BIT.COM and funding from the Corporate Reserve to implement a pilot project for RDIMS. However, the current timeframe for implementing RDIMS, department-wide, is four to five years.

- b) As relevant standards, processes, and systems are put in place, increased direction is provided to departmental units and staff to manage electronic information.**

The RDIMS implementation strategy includes components for increased training and communication to staff in their accountabilities for information management. Training and communication will occur concurrent with the implementation of RDIMS in business units.

- c) As relevant standards, processes, and systems are put in place, the implementation of the *IMB Information Management (IM) Policy* is monitored.**

The Information Management Branch has developed a review guide to assess how well business areas, including LSUs, are managing paper records. As RDIMS is implemented, the guide could be modified to include the management of electronic records. However, in order to appropriately monitor understanding of, and compliance with, the IM policy framework, the Branch must develop a business case to adequately resource what is essentially a new function.

d) Reference to productivity gains is made in standards and when communicating these standards to staff.

There are no reliable industry standards for assessing productivity gains at this time. However, as we develop standards, the Information Management Branch will communicate to all employees the effectiveness of electronic document and records management, based on the best information on productivity gains available at the time.

e) Accountability frameworks for the management of electronic information are developed.

The Information Management Branch is employing the departmental IM/IT Project Management Framework to ensure sound management of the RDIMS project. The Framework requires a project charter, including a clear statement of roles and responsibilities, as well as a project plan and a full accounting of project costs.

f) The approval of the revised current disposition authorities by LAC is pursued.

The Branch has negotiated an MOU with Library and Archives of Canada for the development of a comprehensive Records Disposition Authority. Work identified in the MOU will soon be underway, with completion of the project forecast for 2008/09.

2. It is recommended that:

a) The Chief Information Officer direct that electronic records are kept in a format or can be converted to a format that may be acceptable to LAC.

See response to 1f) above.

b) The Chief Information Officer, in consultation with the Director General, Communications, direct that Web content is kept in a format or can be converted to a format that will be acceptable to LAC.

The CIO will raise with the LAC the issue of appropriate format for any records identified for transfer. The negotiation of a comprehensive Records Disposition Authority for the Department will provide an opportunity to do so.

3. It is recommended that the Director General, Communications collaborate with the CIO to ensure that information posted on departmental Web sites is recorded and

managed through the life-cycle in accordance with the MGI policy, *Department of Justice Information Management Policy*, and the *Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites*.

Efforts to ensure appropriate life-cycle management of web content are dependent upon, and must follow, the acquisition of the appropriate content management applications and their subsequent implementation. It should be noted that the introduction of an Enterprise content management application will exceed existing budgets for intranet and internet in the Department. In addition, a review of two of the three policies cited (The Policy on the Management of Government Information, and the Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites) is underway; the relevant directives and standards cited in the succeeding policies will be observed once these take effect.

(We make no recommendation on application systems information here. See “Application Systems”.)

2.2 Organization and Responsibilities

The Department currently has an organization in place for information management but it is primarily focused on the management of paper records. IMB management recognizes that changes are necessary and has taken initial steps toward improvement such as issuing the *Information Management (IM) Policy*, obtaining approval for the *Strategic Framework for the Management of Information in Justice Canada* from BIT.COM, and planning the preparation of a human resources plan. The CIO has advised us that he is seeking the cooperation of headquarters’ sectors, regions and DLSU heads to implement the policy. It should be noted that the CIO has limited authority for the implementation of this policy. Also, IMB has begun to make organization and staff changes in IMD. The organization and staff skills of regional offices as well as staff skills of DLSUs also need to be reviewed to improve the management of electronic information.

General responsibilities for information management are outlined in the *Information Management (IM) Policy*. Detailed responsibilities need to be assigned for those managing information management operations. Most staff we interviewed, including those responsible for records in the regions and DLSUs, had no formal assigned responsibilities for the management of electronic information. However, many staff take personal responsibility for managing their electronic records; they use individual methods and these efforts are insufficient.

Recommendations and Management Response

- 4. It is recommended that the Chief Information Officer continue efforts to implement a revised organization of the Information Management. In line with this, the CIO should review with the regions the organization and staff skills required and with DLSUs the staff skills needed to improve the management of electronic information.**

The CIO will initiate a discussion, involving Regions, HQ and Legal Service Units, on a standard information management organization later in the current fiscal year.

2.3 Strategies and Planning

Any discussion of the strategic approach needed in the Department for the management of electronic information needs to take into consideration plans to implement an EDMS in the Department of Justice. An EDMS would allow staff to file electronic records in a departmental system that has the appropriate functions for records management. Staff would view, access, or delete information according to their system authority. In the “EDMS” section of this report we discuss in detail the requirements, considerations, benefits and work completed to date on an EDMS for the Department. It is our view, however, that the implementation of an EDMS will not provide a complete solution to all electronic information management issues the Department is encountering. Management should continue other efforts to improve electronic information management.

In 2004 IMB took a number of important steps in this regard. IMB prepared two strategic reports, the *Electronic Document and Records Management Strategy* (April 2004) and *Assessment of Department of Justice’s Capacity to Fulfill the Requirements of the Policy on the Management of Government Information* (Draft Report, November 2004). IMB also prepared *The Business-Driven Vision of Information Management for Justice Canada* for presentation to BIT.COM.

The *Electronic Document and Records Management Strategy* report identified several issues, many similar to those we describe in this report, and provided preliminary cost estimates for improvements. It did not provide a complete list of cost categories nor outline the preliminary steps required for the current application systems to later collect information for or link the information to an EDMS. The *Assessment of Department of Justice’s Capacity to Fulfill the Requirements of the Policy on the Management of Government Information* identified several issues, described a strategy, provided preliminary cost estimates for improvements, and made recommendations. Its primary conclusions were that the Department is not in full compliance

with most of the *MGI* policy and that compliance can be improved by allocating additional funds and assigning more emphasis to information management. This report did not provide a complete list of cost categories.

The Business-Driven Vision of Information Management for Justice Canada was presented to BIT.COM and approved in November 2004. As a result IMB was asked to prepare an implementation plan for the appropriate management of electronic records. IMB was not required to financially justify on a cost-benefit basis the implementation of the strategy.

BIT.COM did not require IMB to prepare a business case for an EDMS. However, a business case contains elements key to the success of a project. Since this will be one of the largest IM/IT projects undertaken in the Department, it is important that the considerations (other than financial justification) usually addressed in a business case, such as scope, responsibilities, and work to be undertaken by stakeholders, be documented to ensure a clear understanding of the project's achievement goals. Also, the implementation of an EDMS and improved processes to manage electronic records will require mandatory activities on the part of staff and these activities need to be identified. Furthermore, preliminary activities also need to be identified, such as processes and tools required to facilitate the management of electronic records and thus introduce an element of sustainability and potentially improve productivity. Neither a computer application systems architecture nor an information management architecture has been developed. Links with other systems and a preliminary model of departmental information management architecture will assist in more effective and economic improvements in information management.

IMB is undertaking further activities to improve information management:

- A pilot of the Records, Documents, Information Management System (RDIMS) is under way. RDIMS is the EDMS preferred by TBS and provided by PWGSC⁴. Approximately 40 staff in IMB are using RDIMS in order to become familiar with its capabilities. We were informed that so far there were good experiences reported by other departments using RDIMS.
- A second pilot project was to be initiated in the summer of 2005 for 15 users in the Human Resources Section in the Ontario RO. This pilot was intended to last a year.

⁴ In collaboration with Treasury Board, Public Works and Government Services Canada (PWGSC) has established a standing offer with suppliers for RDIMS, a computer system to manage electronic records.

- Other pilots were to be conducted before a final decision is made on how to select an EDMS or whether to adopt RDIMS for the Department.
- Activities have been initiated to centralize RIMS and iRIMS, (a version of RIMS), which is a preliminary step to the implementation of a departmental EDMS.

The regional offices we visited are waiting for direction from Headquarters and have no formal plans for improving the management of information. However, they are nonetheless taking some steps to improve the management of information:

- The Edmonton RO has been using a commercial product, SharePoint, developed for sharing documents and for other information management purposes. The version of SharePoint currently in use does not keep copies of prior versions of documents. The regional office is planning to upgrade to a version that will keep track of content of information. This will facilitate improved management of one type of information in the regional office. This regional office is also filing removable electronic media such as CDs in separate folders so they can eventually be stored under proper environmental conditions for long-term conservation.
- The Toronto RO conducted a survey and found that there were several deficiencies with records management. The regional office is taking steps to correct these deficiencies such as offering more training, reviewing closed paper files, and making section directors aware that staff are not always recording case documents in iCase.

The DLSUs we visited are waiting for direction from Headquarters and have no formal plans for improving the management of information. They also wish to assess the impact of the implementation of iCase before other major changes are made. However, they are taking some steps to improve the management of information:

- The Fisheries and Oceans DLSU is using the client's RDIMS on a pilot basis. (See "EDMS Used by DLSUs".)
- All three DLSUs have revised or plan to revise their file plans.
- All three DLSUs plan to improve the access to electronic versions of opinions.

Recommendations and Management Response

5. It is recommended that the Chief Information Officer ensure that:

- a) An implementation plan to improve the management of information including the management of electronic records is prepared as requested by BIT.COM and monitored.**

Information Management Branch has developed an implementation plan for RDIMS. BIT.COM has accepted it as a general plan for the project. The plan will be refined as the project progresses.

- b) Preliminary activities needed for improving the management of electronic information are identified in the implementation plan.**

Specific activities such as providing business units with information management training, clarification of roles and responsibilities, are currently being worked into the RDIMS implementation plan.

- c) The implementation plan is coordinated with regional offices and DLSUs.**

Clarifying accountabilities, roles and responsibilities is essential to a successful RDIMS implementation. Documentation, for discussion with all parties implicated in the project rollout, is currently under development and we anticipate confirming roles, responsibilities, service levels and timing of implementation with Regional Offices and other stakeholders in the fall of 2006, as part of the development of the Project Charter and refined project plan. If the project receives full approval, IMB will make every effort to coordinate its activities with the business areas affected by the implementation.

- d) Solutions for improving management of electronic information take into account information processed by application systems, IT services, and other processes dealing with electronic information used in the Department.**

The proposed MOU with Library and Archives of Canada will address the disposition of departmental records, regardless of medium. The development of a revised Records Disposition Authority will provide the opportunity to ensure full life-cycle management (including legal destruction) of structured data, such as that associated with applications such as IFMS and PeopleSoft, as well as unstructured data in RDIMS.

6. It is recommended that the Chief Information Office ensure that for EDMS topics usually addressed in business cases are documented and presented to BIT.COM.

Many of the components of a business case are included in the RDIMS Implementation Strategy. In addition to providing BIT.COM with briefings on the RDIMS implementation, the project must submit relevant information on budget, milestones achieved and overall project health to the BIT.COM sub-committee, the Investment Review Committee, to receive yearly approval to continue implementation.

2.4 Resources

In 1995, the number of staff for records management was reduced throughout the Department. Although the number of total departmental staff has significantly increased since that time, there has been little change in the resources assigned to records management. However, IMD has changed its staff composition: it has decreased the number of staff who are qualified to deal with paper records and increased the number of staff with qualifications to manage electronic information. This has improved the strategic capability of IMD and initiatives to manage electronic information have started.

IMB first assigned permanent resources to electronic information management in 2004/05. IMB currently has three staff on a part-time basis for a total of 1.5 FTEs in the Information Management Division. Two staff members were hired in the spring of 2005: one as a dedicated project manager for RDIMS; another one as an information administrator for RIMS, who will later work on RDIMS.

The regional offices and DLSUs have no dedicated staff for electronic information management. Staff who were previously managing paper records are tasked with managing electronic information but they have no formally defined responsibilities for this task. DLSUs have little support and funding for information management from the Department. They rely on client staff for IT support and some use the client's EDMS. However, there is no assistance available from client staff to manage information in accordance with Department of Justice requirements. While the CIO works collaboratively with regional managers of IM/IT on a variety of issues, the resources associated with IM in the regions are the responsibility of the heads of ROs. The heads of DLSUs are responsible for their DLSU client resources.

For the present the licenses to use the RDIMS system are available at no cost. However, IMB is required to cover other costs related to technical support, additional hardware, conversion,

linkages with other systems, training and implementation. The Information Management Division has a budget of \$25,000 O&M for training users involved in the RDIMS pilot.

We were informed that the implementation plan will identify resources required. To appropriately manage electronic information will require significant funding. A preliminary estimate is approximately \$14 million. Apart from funding, the implementation of the plan will require providing staff with training in new skills. Records management staff who are responsible for managing paper records will need further training, or new staff with appropriate qualifications for the management of electronic information will be required. Information management is now a defined discipline with specific degrees.

IMB has plans to fund some initiatives such as the development of policies and guidelines, and a new file plan for records classification. Departmental funding will be required for eliminating the backlog in retention and disposition of paper records, selecting and implementing an EDMS, and ensuring staff are available who have appropriate information management skills.

Regional Offices and DLSUs will also require additional resources to improve the management of electronic information. In particular, we were told that the DLSUs have not always been well supported or funded by IMB in the past. DLSUs receive most of their support staff and O&M funds from the client. The clients will not readily provide funding for initiatives that are intended to improve Department of Justice information management. Furthermore, some clients are in the process of acquiring or have already acquired their own EDMS systems, which they do or plan to make available to the DLSUs. (For a more detailed discussion, see “EDMS used by DLSUs”.)

In addition to initial development and implementation costs, there will be costs for training, providing technical and changed business processes support, monitoring the status of the management of electronic information, and enhancing processes and systems over time. Also, there will be costs associated with developing appropriate linkages with or replacement of existing systems or processes.

Recommendations and Management Response

- 7. It is recommended that the Chief Information Officer ensure that complete costs, including regional and DLSU costs, are estimated for the implementation plan to improve the management of electronic information.**

Please see response for Recommendation 1e).

2.5 Management Reports

We found little statistical management information available on electronic information. There is no regular information that may permit analysis and quantification of how electronic information is being used and stored. There are no regular reports produced that contain numbers of additions or deletions of records; type of access; age of information; or type of media, IT service, or system used. Responsibility Centre and information managers do not have reports to assess the management of electronic information. There are no regular reports on service levels, performance measurement, and workload statistics. Yet we were informed that staff make substantial use of electronic information. Consequently, management has limited knowledge about the type and quantity of electronic information, activity related to it, and its impact on productivity. The total number of gigabytes used by an IT service or system is periodically identified for use in presentations. IT staff consider the disk space used by information on servers for equipment capacity planning purposes. Some application systems such as iCase can produce comprehensive statistical reports, but we were told that these are not being used for information management.

In August 2004 the Ontario regional office prepared an analysis report entitled *E-mail and File Management in the Ontario Region, A Discussion Paper*. This was followed up by a survey on records management conducted in 2005. The report and survey indicated significant issues with the management of e-mail and records. For example, more than 50% of lawyers did not as a regular practice print out e-mail messages to put on the paper file; many users did not use iCase to prepare documents; and many paper files were not closed. The Ontario RO is implementing changes to deal with these issues.

Recommendations and Management Response

8. It is recommended that the Chief Information Officer consider options for preparing reports on electronic information.

The Information Management Branch does provide high-level reports on various aspects of information creation, use and storage for BIT.COM. Specific reports might be developed on information management practices, for use by program managers, in future. Until such time as the Department receives a Records Disposition Authority from the Library and Archives of Canada for the legal destruction of electronic records, the customized reporting may not be worth the effort required to design and produce them.

2.6 Communicating

The Information Management Division maintains information on the IMB Intranet site and sends out notices when new policies or guidelines are issued. Nonetheless, we found most departmental staff are unaware of policies and guidelines. Staff require training, increased support, and appropriate tools (software, standards and processes) to benefit from new policies or guidelines to improve information management. Staff are unlikely to spend the time to read about information management without further support.

Recommendations and Management Response

- 9. It is recommended that the Chief Information Officer ensure that as tools and training become available for the improved management of electronic information, policies, standards, and guidelines are effectively communicated to staff.**

The Information Management Branch will ensure that a communication plan accompany the release of policies, guidelines and standards, on a go-forward basis.

2.7 Human Resources Management

In the *Strategic Framework for the Management of Information in Justice Canada* (November 2004), IMB identified the need to change and increase resources for the management of electronic information and planned to undertake the development of a human resources plan. The human resources plan should address the number and specific skills of the staff associated with IM in the Department. In our opinion it is likely that increased resources will be required to maintain current processes for dealing with paper files and to implement new processes for dealing with electronic records.

One issue is that records management staff are classified in the CR (Clerical and Regulatory) category. We were told that the SI (Social Science Support) category is more appropriate for these staff given the changes to information management as a result of the increased use of electronic information. However, according to Treasury Board, the SI classification cannot be used for records management staff. IMB continues to attempt to hire appropriately qualified candidates to meet its needs and is also pursuing changes to classifications and levels for records management staff across the Department. In DLSUs the issue of staffing of information management positions is more complex because support staff are provided by the client. Also, since DLSUs have fewer staff than Headquarters and ROs, it may not be possible for DLSUs to

ensure that staff with the required skills are assigned. Headquarters may need to provide assistance to DLSUs.

Recommendations and Management Response

10. It is recommended that the Chief Information Officer, in collaboration with heads of ROs and DLSUs, ensure that efforts to hire or assign appropriately qualified staff for IM staff are implemented.

The proposed IM Human Resources study (see response to Recommendation 4) would address standard IM organizations, position levels, and required competencies.

2.8 Training

Training is available for staff on how to use software that creates or uses electronic information (e.g. text processing, spreadsheets, applications, Intranet, Internet) but not on how to manage electronic information. In headquarters the training on office support software is provided by a contractor and does not address departmental requirements to manage electronic information. Staff need training on how to manage e-mail messages and folders efficiently, how to familiarize themselves with departmental IM requirements, and how to work efficiently with electronic information.

The regional offices and DLSUs are delivering informal, ad hoc training sessions (e.g. on the use of e-mail). In our view it is not efficient for each office to develop its own training materials. . IMB is developing training materials that can be used online and will be made available to ROs and DLSUs.

A survey was conducted in Toronto that was useful in identifying some of the training needs for the Ontario RO. Other offices have not conducted similar surveys.

We were told that there are issues with training in the Department. There has been a rapid growth in the number of employees in recent years and some offices have experienced high staff turnover. Staff often do not attend training sessions because of scheduling constraints or lack of interest. In some cases, responsibility centres do not have the funds to provide employees with the five days of professional development they are entitled to. As a result, there are many employees in the Department who have not received appropriate training.

We noted that in the Fisheries and Oceans DLSU users are not given access to its EDMS unless they attend a training session. It is our view that the Department may need to make some important training, such as training on information management, mandatory. An opportune time to train staff is when they initially join the Department.

It is our view that both Information Management Division and information management staff in ROs and DLSUs need to address training issues.

Recommendations and Management Response

11. It is recommended that the Chief Information Officer ensure that:

- a) as part of the improvement of the management of electronic information, appropriate training is made available to staff;**
- b) attendance at training is monitored.**

The Branch anticipates the introduction of an on-line IM orientation course, intended for all staff later in the current fiscal year. Participation rates will be monitored.

12. It is recommended that the Chief Information Officer seek to make key courses mandatory if staff are not attending the required courses.

Agreed.

3. ELECTRONIC RECORDS PROCESSES

3.1 Electronic Information Stored Outside of Application Systems

In addition to application systems there are several IT services that store or process electronic information. These include e-mail; various personal, shared and other drives; removable media; departmental Intranet; Internet; scanned information, and commercial network systems (e.g. SharePoint). Of these, e-mail has become the preferred storage system followed by the personal drive and the shared drive.

E-mail

The e-mail service is very important. We were told by lawyers that 50% to 90% of their work is conducted by e-mail. Most staff members indicated that it is the preferred service for storing electronic information. Users can organize information in folders as they choose; the search function is easy to use; most sites have no limits on storage; and information can be accessed by remote access without requiring a Public Key Infrastructure (PKI)⁵ service. E-mail is also the preferred service for sharing information. Messages and attachments can be easily sent to one or several recipients.

The Department currently has no standards for consistency and efficient use of e-mail. We found the following issues that contribute to inefficiency:

- Unclear subject lines or not creating a new subject line when necessary.
- Replying unnecessarily to messages, thereby creating extra messages to be deleted or stored as well as additional work on sending and reading the replies.
- Not keeping to the necessary minimum the number of recipients.
- Inefficiently managing e-mail exchanges on the same subject with multiple persons.
- Inefficiently organizing and naming folders.

⁵ The Department uses PKI (public key infrastructure), an encryption service that enables users to establish secure connections for remote access to the departmental network. PKI also has other users for secure data processing. PKI uses a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

- Not organizing messages in such a way that they can be efficiently retrieved once an issue or case is no longer active.
- Not organizing messages for knowledge transfer.
- Lawyers sending queries to many colleagues to avoid time-consuming and sometimes ineffectual electronic searches.
- Not printing e-mail for the paper file.
- Not importing e-mail to iCase.
- Using e-mail to send and receive documents that are only available on the shared drive because they are not accessible to staff in other offices.

Many lawyers receive a significant number of e-mail messages. We found that software tools that identify duplicate received messages or attachments are not available to improve staff productivity. Also, most users are unaware of functions such as filters, flags, and e-mail receipt notification. Users are also unclear about who is responsible for keeping the official copy of an e-mail when there are multiple recipients.

We also found that issues with e-mail impact corporate memory. E-mail messages contain significant corporate memory but the messages are only accessible to the holders of individual accounts or their assistants. E-mail messages of general interest are not available to others who may benefit from them. E-mail messages that are not imported to iCase cannot be searched by authorized users. In any event e-mail messages are rarely imported to iCase.

We also found that public e-mail folders have been set up but are generally not used. If they are replaced with another sharing method, they should be deleted when no longer required.

Generally, e-mail messages are not stored in such a manner that they may later be easily imported to an EDMS or into iCase. Only a few lawyers make use of folders that contain the RIMS number of the departmental file that the e-mail message corresponds to. The inclusion of the RIMS case file number would facilitate the automatic transfer of messages from the e-mail system to an eventual departmental EDMS.

(We have made recommendations with respect to e-mail in “Policy, Guidelines, Standards” and “Training.”)

Personal, Shared, C Drives, and Other Server Drives

After the e-mail system, the personal drives are the most heavily used. Personal drives are the P drive in headquarters and the regional offices. The DLSUs use different letters to identify personal drives. Usually a personal drive is accessible only by the corresponding network

account holder. The personal drive is used to create documents (such as letters, memos, or reports) that may be printed for distribution and filing or attached to an e-mail. Some lawyers scan the documents into image files and then e-mail the images to clients to safeguard the document from modifications. Image documents are difficult for a recipient to alter.

Shared drives are typically used for sharing information within a section. The information is not accessible to other sections. Sections usually store administration reference information (e.g. policies, forms, procedures) on the shared drive. Shared drives are also used to store legal reference information, opinions, and case information. Furthermore, personal folders are set up on the shared drive for staff to use as they choose. Typically, a folder is set up for the General Counsel and his or her assistant, which is not accessible to other staff. The rest of the shared drive has no integrity controls and anyone in the section can access, create, or delete documents.

A key issue with the personal and shared drives is the lack of standards to ensure consistency and efficient use. Other issues are similar to those of e-mail:

- Users do not know the best methods for naming folders and documents. Also, staff indicated that they have not received training on how to organize folders consistently and effectively.
- The shared drive requires ongoing management (e.g. organizing folders, updating information). This is not occurring. It is very time consuming to organize and update the information on these drives.
- Most users do not sufficiently understand the search function.
- There are different practices with regard to the printing of paper files, importing of documents to iCase, and deleting of printed documents.
- Generally, documents or case records are not stored in such a manner that they may later easily be imported into an EDMS or iCase. Very few users place the RIMS case file number in the folder or document name.

Most sections we visited have shared drives that contain outdated information. We were told that these sections wished to update and reorganize these drives. Most staff do not use the shared drive. In a few sections staff do not use the personal drive but use the shared drive for their personal folders. The risk with this practice is that any information on the shared drive could be changed or deleted by anyone else in their section. Also, sections often use the first name of staff members to identify their personal folders on the shared drive. With staff turnover, it is not always obvious to whom the folder belonged. Few staff make use of the shared drive for sharing information.

In our opinion, a strategy is required for the use of shared drives and for other methods of sharing information (e.g. EDMS, iCase, SharePoint).

Generally, there is no permanent storage of information on the C drive, and staff are aware that all other drives have regular backup except for the C drive.

The regional offices use other server drives for special purposes such as storing old Caseview information. (This system is now replaced with iCase.) Some DLSUs use other server drives to store opinions or local databases.

Recommendations and Management Response

13. It is recommended that the Chief Information Officer ensure that:

a) A strategy is prepared for the use and management of shared drives.

The Information Management Branch currently provides support, when requested, to business units to assist them in establishing taxonomies to organize records on shared drives. However, the ongoing management of information on shared drives is the responsibility of the business unit.

b) Standards and guidelines are issued for the use of personal and shared drives to ensure the consistent and efficient use of these drives and to meet departmental information management requirements.

A Guideline on Managing Departmental Information is currently under development and will be available for all staff presently. The Guideline will explain how to organize and manage information on shared and personal drives.

14. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads ensure that:

a) The strategy for the use and management of shared drives is implemented.

The Guideline on Managing Departmental Information will apply to all staff of the Department once approved. However, members of DLSUs typically store information on the drives of the host department and may be subject to whatever policies and guidelines these departments currently have in place.

b) Information is stored in personal and shared drives in such a manner that it can later easily be imported to an eventual departmental EDMS.

Organizing information according to the Guideline will make a transition to RDIMS relatively simple for a business unit.

(A recommendation on training is made in “Training”.)

Removable Media

The term removable media refers to storage devices that can be used to easily move data between computers with the appropriate device readers. Floppy disks, compact discs (CDs), DVDs, and USB flash drives are all removable media.

The main removable media in the Department of Justice are CDs. The Department uses a relatively small number of CDs (some commercial) and fewer DVDs. Many of these media should be managed as records because they contain legal information (including litigation information), backup for certain data, and data from former staff (i.e. e-mail messages, personal drive folders, and personal folder from the shared drive). Some of these media are commercially purchased and contain published legal reference information. CDs or DVDs that are used for temporary storage (e.g. to take information out of the office for presentations or as backup) are not critical. We were informed that CDs or DVDs containing information received from clients for litigation purposes are transitory records and should be returned to the client or destroyed when a case is completed. However, we found that staff are keeping the media. Some litigation cases last many years. Interviewees at the regional offices indicated that they are unclear on what they are required to keep with respect to these cases.

There is no standard format for recording information on CDs and DVDs nor a standard procedure for storing this media. The media are not always attached to a case file or kept in a separate folder. Media placed in envelopes in a paper file, not kept under environmental controls, or labelled with regular pens are likely to degrade and become unreadable over time. Also, the files containing electronic media are usually not identified in RIMS. Some offices have started addressing these issues. The risk is there is no certainty that these media contain information that duplicates information stored in printed form and there are no backup copies of the media.

Other media such as video (some commercial) and sound tapes and diskettes appear to contain duplicate or less important information.

The use of USB flash drives has begun and is increasing. These devices can contain large amounts of information (usually in the range of hundreds of megabytes). Some are encrypted and others are not. Users prefer USB flash drives because they hold more information and can be used to transfer data to computers that do not have a CD/DVD unit. We were informed that flash drives are used for transitory records but there are no standards for their use.

Recommendations and Management Response

- 15. It is recommended that the Chief Information Officer ensure that standards for the management of removable media are developed and request that headquarters and regional office directors and DLSU heads implement the standards.**

Such standards exist and it will simply be a matter of choosing the optimum communications method to inform regional offices and DLSUs of them.

Intranet and Internet

Department of Justice staff have access to Web information on the departmental Intranet and Internet.

The Intranet Web content is updated by Headquarters, all regional offices, and some DLSUs. Most DLSUs have set up a sub-site for their use on their host department's Intranet site. The Department of Justice Intranet is available to all departmental staff to access Web applications, reference information, and links to other sites of interest posted by departmental sections and ROs. We were told that in headquarters and ROs there are about 200,000 documents on the Intranet with about 25 documents changing each day.

We were also told that the departmental Internet site has around 60 sub-sites, containing approximately 60,000 documents plus 8,100 statutes and regulations. Approximately 25 documents change each day. This site is accessible to the general public.

An Extranet where the Web publications are outside the departmental firewall is in development. This will be accessible by other government departments. Initially, the Intellectual Property Secretariat, Federal Prosecution Service (FPS), and Agent Affairs Unit will provide content to the Extranet.

According to the *MGI* policy, the *Communications Policy of the Government of Canada* and the *Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites*, information contained on the Internet, Intranet, and Extranet sites must be managed as records.

However, at present no official archive of publications on Web sites is maintained. Older versions of content are not always archived and are not linked with the departmental records management function. Staff in the Electronic Communications Division, Communications Branch, which coordinates and leads the content of the Intranet and Internet, are examining standards for archiving Web content. It seems that since there is a significant daily rate of changing content, a practical solution is to use software such as a Content Management System (CMS).

Most Intranet sub-sites are not up-to-date and the search function needs improvement. Management of Web content is a relatively new function for staff. Staff who were already assigned other responsibilities have now been given the additional responsibility of managing Web content. As a result there is little time for archiving content. The Edmonton RO is conducting a pilot of a CMS that among other benefits would archive Web content.

Recommendations and Management Response

16. It is recommended that the Director General, Communications and the Chief Information Officer collaborate to develop and implement standards to facilitate the management of Web publications as departmental records in accordance with the MGI policy.

Upon the phased-in implementation of Enterprise content management and document management applications, the Director General, Communications and the CIO look forward to the implementation of standards for information management, including web publications and other web content.

The cost of implementing these applications is a significant factor in how effectively the Department can enforce a complete information management accountability framework.

SharePoint

SharePoint is a Web-based Intranet-like system that allows users to set up Web sites for use as collaborative work spaces. Offices in various locations can use SharePoint to share information. A pilot project on using SharePoint is currently under way in the Prairie Region. In the Prairie RO, there are 40 Web sites and about 350 users. Users in the Prairie Region indicated the following benefits. They stated that SharePoint:

- provides faster access than paper and wider access than the shared drive;
- decreases e-mail and has calendar functions;

- notifies subscribers of changes to content by e-mail;
- has a low overhead for administration;
- provides discussion groups;
- decreases duplication of information.

It should be noted, however, that the current version of SharePoint does not keep copies of prior versions of documents nor does it attach a reference number that would allow a link to a records management system.

Also, in the Ontario regional office a group in IT and another group in FPS are using SharePoint.

Scanned Information

Several sections are scanning documents to create electronic versions. These electronic documents exist in both text and image formats. The use of scanning is increasing. Information is scanned for various purposes:

- for RingTail (a litigation support system)
- for several other litigation support systems (Summation, SuperText, Supergravity) that will eventually be replaced by RingTail
- to import information into iCase
- to create electronic documents that clients cannot modify

There is a significant amount of scanning required in the Department and there are no standards for formats and resolution except for RingTail (TIF 300 DPI, which may be black and white, grey, or color). Standards are important to ensure compatibility, to facilitate future access, to avoid unnecessarily large files or files that are difficult to read because of a low resolution.

Recommendations and Management Response

- 17. It is recommended that the Chief Information Officer ensure that standards for the scanning of documents are developed and request that headquarters and regional office directors and DLSU heads ensure their implementation.**

Standards exist for importing scanned information to Ringtail, the departmental standard application for litigation support and evidence management. Developing more generic guidance for scanning information for business purposes may be considered as part of a future direction for the RDIMS project. Scanning is currently not in scope for the project. Including this requirement in the RDIMS project will require additional funding.

Issues With Sharing Information

All of the electronic records processes we have discussed are used for sharing information. In the Department of Justice information sharing is accomplished on an ad hoc basis. The preferred method is e-mail. Some information contained in shared drives is useful but most is out-of-date or needs reorganizing. Access to information in shared drives is limited to those staff members who work within the section to which the shared drive belongs. The Intranet allows information to be shared across sections. However, certain requirements must be met in order to post information on the Intranet (e.g. bilingual content, site administrator controls). These requirements introduce time delays.

Some sections of the Department are spread across different cities or locations. These sections make greater use of the Intranet for sharing information because the shared drives are inaccessible. For this reason the Prairie Region is increasing the use of SharePoint to share information.

Some application systems are used for sharing information but with limited success. (See discussion in “Application Systems”).

Recommendations and Management Response

18. It is recommended that the Chief Information Officer provide guidance and appropriate tools to improve processes for the sharing of information.

The Branch is currently assessing possible technology/applications for collaboration and information sharing.

3.2 Application Systems

Application systems are computer software that apply the capabilities of a computer to the performance of tasks related to a specific business function. Departmental application systems fall under two types: legal systems and non-legal systems. Legal systems are those such as iCase, LOPORS, GASPARD, LIMS, and RingTail. Non-legal systems are those used for administrative support, finance, human resources, security, accommodation, and other services. Departmental application systems contain a significant amount of electronic information. Some application systems contain documents that may be captured by an EDMS as the documents are prepared. However, none of these systems is intended to be a records management system. They do not

have the required controls such as records integrity, security, ability to store and search various formats of documents, use of the departmental file plan, and built-in disposition schedules. These systems are designed to meet the requirements of specific operations and not of departmental information management.

These application systems allow information sharing according to access rights. Most do not have reference numbers (e.g. RIMS case file number, PRI (employee number)) to allow for linking to an eventual EDMS. These systems do not usually delete information, which minimizes the risk of information being lost. However, sometimes it is necessary to delete information and this must be done in accordance with approved disposition schedules.

In this section we discuss some key systems from the perspective of the management of electronic information. Our intent is to illustrate the complexities of including application systems in the departmental management of electronic information. (Note that it is not the intent of this audit to provide recommendations for specific application systems)

iCase

The iCase system contains significant information and is a key departmental resource. As a significant body of knowledge, it is important that it be accessible. iCase has approximately 3,700 users and contains the records of 401,550 cases; 233,940 of those cases (approximately 58%) have at least one document. iCase stores 3.2 million documents.

Data in iCase is incomplete. Although iCase is mandatory for recording time, it is not mandatory for recording legal documents. Some lawyers do not create documents in the system or copy them to iCase, and therefore the information is not available for sharing. Legal agents, who handle about 50% of criminal prosecution cases, do not prepare documents with iCase. Legal agents also assist the Department with civil litigation and therefore have electronic records related to civil litigation.

The process of transferring e-mail messages into iCase files has been cumbersome and is often not done. We were informed that a function to more easily import e-mail messages into iCase would be implemented in the fall of 2005.

WordPerfect documents are not accepted by iCase, yet WordPerfect is the standard software for some DLSUs. Converting documents to MS Word is not a preferred solution. DLSUs that work with both formats noted that the conversion process may corrupt documents immediately on conversion or after further use.

iCase is not considered particularly user-friendly for viewing closed files, so many users keep their files open for easier access.

iCase is not yet implemented in Atlantic Region, Northern Region, and many DLSUs. If DLSUs begin to use iCase to create documents, this will cause a major change in their operations. The Department will need to develop strategies for DLSUs that already use their client's EDMS to coordinate the various systems with an eventual departmental EDMS.

There are no standards for naming documents. Individual creators of documents assign whatever name they choose. The iCase manager informed us that document-naming standards should be developed by the Department, and once developed, iCase will conform to those departmental standards. These departmental standards have not been established.

Records that are contained in iCase include the RIMS case file number. This will allow for their eventual transfer to or linking with a departmental EDMS if required.

Caseview

Caseview is the predecessor of iCase. When iCase was implemented, information that was in Caseview remained in Caseview and we were told that there is no easy access to this information. We were informed that Caseview information will be made more easily available in the future.

RIMS

RIMS is the system used to manage paper records. The Department currently uses different versions of RIMS, and RIMS data is decentralized to the regions and the DLSUs. IMB has already determined that a prerequisite to implementing an EDMS is to centralize RIMS and upgrading it to iRIMS. Consequently, the whole Department will use the name iRIMS system and one or more databases. Work on the centralization and upgrading of RIMS to iRIMS was well underway. Furthermore, existing RIMS information can be converted or linked to an eventual departmental EDMS by using the RIMS number assigned to each case file.

Litigation Support Systems

Several litigation support databases are in use (Summation, Supertext, SuperGravity) and they are being converted to a single system, RingTail. These databases contain evidence information compiled by clients to be presented to court and they keep track of reference documents used to prepare legal arguments. They also record comments that are made by departmental staff on the

documents. The litigation support databases and RingTail are used when paper records are too extensive for effective reference. For RingTail, the Department has procedures and standards for electronic document transfer. In other cases, we were informed that when a client provides records in electronic format to the Department, the client decides on the database to be used. Paper records provided by the client are scanned by the Department and returned to the client when the case is completed. One database is set up for each case except in the RingTail system, which keeps all cases in one database. In one region there were 66 databases.

Copies of the databases are sometimes kept on CDs or DVDs but not always. The copies are considered transitory records because other copies exist with the client or elsewhere. Transitory records can be deleted once they are no longer required. Generally, the CDs and DVDs are not destroyed when the records are no longer needed. As long as the transitory records are required, they must be managed as records. This is not always happening. Departmental staff add comments to the documents contained on the databases. Unlike the original information contained in the databases, these comments are not transitory records and must be kept by the Department. Once the cases are completed, it is unclear to us how the comments may be used if they are not linked to the original records.

RingTail is an important litigation support system. It contains 864,505 documents and 84 active legal cases, and has 348 active users.

RingTail maintains a RIMS file number on its case records. This is not usually done by other litigation support systems. Current staff know which record pertains to which case, even if a RIMS file number is not attached to the record. However, automatic linking of records to an eventual EDMS will not be easy, especially many years after a case has become inactive and staff have changed.

Other Legal Systems

There are several other legal systems and we discuss a few of these below.

LOPORS is used for recording legal opinions of departmental importance and by some DLSUs to record local opinions and other documents. Some opinions of departmental importance may not be contained in LOPORS. LOPORS records RIMS case file numbers. LOPORS has 3,566 registered users and contains 29,000 documents. Contributions to the national portion of LOPORS are voluntary and many documents are not submitted to LOPORS.

There are other repositories for legal opinions including Intranet Web sites and databases. Legal opinions are given in various ways: verbally (lawyers usually keep a written record by making a

handwritten or a typed note on a file), by formal memos, and by e-mail. Legal opinions constitute the highest output of the DLSUs and are also prepared in ROs and at headquarters. Few e-mail opinions are captured in application systems and controlled as records. Most substantive opinions are on paper documents and their electronic version may or may not be in a system.

GASPARD is used for a variety of information including some legal opinions. The legal opinions data has a field for the RIMS case file numbers but these are not being entered. Other data other than legal opinions do not include a data field for recording the RIMS case file numbers.

LIMS is a new system that will replace FOLIO by December 2005. LIMS will be used to access consolidated statutes and regulations. Access will be provided through the Internet and Intranet. At present LIMS only contains statutes. Regulations often contain tables and their format is more complex. FOLIO was published in CDs and physically distributed to subscribers. This process did not provide up-to-date information because updated CDs were only periodically issued. The content of FOLIO is also accessible through the departmental Internet site. With LIMS it will be possible to access older versions of statutes (back to December 2002) and of regulations (back to December 2005). There is no process for maintaining records of previous versions of statutes and regulations. There are commercially printed published versions of this older information but they are not departmental records.

Non-Legal Systems

The Department uses a variety of other stand-alone application systems such as:

- Integrated Finance and Materiel System (IFMS) for managing and recording financial information.
- PeopleSoft, for human resources management, which has a PRI (employee number) that could be linked to an eventual EDMS.
- Salary Management System (SMS) for salary management, which has a PRI (employee number) that could be linked to an eventual EDMS.
- Inventory systems for managing departmental assets.
- E-forms system for storing blank forms widely used in the Department.
- Library systems for managing the library collections.
- Accommodation systems for managing accommodation including a Computer Aided Design system that records data and graphs on accommodation.

The coordination of some of these applications with an eventual EDMS was discussed in IMB but no requirements were defined. These application systems may require a different records management process than an EDMS system since they contain records and data elements and not documents.

In concluding this section on application systems, it is our view that the Department needs to develop a strategy for determining the information that will be included in an eventual departmental EDMS or the alternative approaches to be used to manage the electronic information contained in application systems.

Recommendations and Management Response

- 19. It is recommended that the Chief Information Officer ensure that a strategy is developed and implemented for the management of electronic information contained in application systems.**

The Information Management Branch is collaborating on the development of a departmental Knowledge Management Strategy that will address the role of various applications in ensuring an effective use of IM/IT resources in support of law practice in the department. In addition, the proposed MOU with Library and Archives Canada (see response to Recommendation 1, part f) will address life cycle management issues for all records, including those in applications.

4. PRESERVATION OF INFORMATION AND INFORMATION OF ENDURING VALUE

The *MGI* policy requires that information collected or made available electronically be accessible and usable over time and through technological change according to disposition authorities approved by Library and Archives Canada. Furthermore, information of enduring value must be transferred to the Library and Archives of Canada.

There are no departmental standards or processes for preserving electronic records. In this regard information falls into two categories: information held in application systems and other information. There are a number of issues associated with these two categories of information:

- Information in application systems is usually converted to new systems (and therefore kept for future use) but not always. Some new systems start recording data as of their implementation date, and old data is kept in the old systems, which may be kept in a format that will become inaccessible over time. Typically application systems do not keep a history of when records are updated during the course of regular business operations, so the history is lost. To date, systems with legal information such as iCase and LOPORS store records indefinitely. At some time, information may need to be separately archived. In other cases it may need to be disposed of but this will require an approved disposition authority, which does not yet exist.
- Generally, for other electronic information, inactive records may be kept or deleted. Each user or IT service administrator decides on deletions. Also, legal agents return only paper records to the Department and not electronic records. Removable electronic media is not kept in such a way to ensure that it can be read over time when required. (Refer to “Removable Media”) For example, some offices still have some data on 5.25-inch diskettes. Use of these diskettes was discontinued about ten years ago and current computers are unable to read them.

The Department does not have a process to transfer electronic records to Records Management sections. Therefore, electronic records are retained throughout the Department. Only some removable media is transferred to the Records Management sections. The removable media include a few CDs from Litigation Support, diskettes, CDs of other data, sound tapes, and video (VHS) tapes. Over time these electronic media need appropriate environmental controls for

preservation, as they can be damaged when stored together with paper records and not placed inside a media case. We found that regional offices are making efforts to store removable media so that it is better preserved.

Also, there is no approved schedule for the destruction of electronic records or the transfer of e-records to LAC. IMD indicated that as soon as LAC issues an authority covering electronic records, with workable guidelines on how to transfer these records, IMD will comply. In some cases, electronic records are kept longer than required. In other cases, electronic records are deleted or stored in formats that may not be readable in the future as old software ceases to be supported or available.

Recommendations and Management Response

- 20. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads preserve non-transitory electronic information.**

As the Information Management Branch works with the Library and Archives of Canada to develop a comprehensive Records Disposition Authority, we will seek to clarify the retention periods on all information, including electronic information, and provide guidance to business units on what to preserve and how.

- 21. It is recommended that the Chief Information Officer ensure that information of enduring value is transferred to Library and Archives Canada.**

The Information Management Branch currently transfers paper records identified to have archival value to the Library and Archives of Canada on a regular basis. Once the Library and Archives of Canada (LAC) identifies the electronic records of the Department of Justice it deems to have archival value, and once the LAC identifies preservation format and transfer standards, Information Management Branch will comply with this recommendation.

5. COURT REQUIREMENTS

There is a trend for courts to demand that original electronic records are presented as evidence. This is because the paper record may not completely and accurately represent the electronic record. Electronic records are more difficult to modify because they typically contain more information (e.g. e-mail headers, audit trails, additional copies for records, access controls of the record) than the printed versions. Also they can be searched electronically to ensure all existing relevant records have been presented; whereas with a paper record a document can simply be removed from a file. Furthermore, the original electronic records have more information and are more credible. In one RO we were informed that some courts are already demanding that certain records be presented in electronic format. Also, we were told that another RO had maintained additional backup tapes as a precaution in case a court requested them in a high-profile prosecution. In other countries courts are already asking for the original electronic records.

We note that the *Policy on Corporate DOJ Network Backups*, December 6, 2004 states that backup records will only be kept for one year in the National Capital Region, Regional and Satellite Offices. Therefore, other processes are required for operations that need to store or access records that are older than a year. The purpose of backup records is to recover data from computer malfunctions and disasters. We concur with IMB that using backup tapes is neither fast nor efficient for accessing older records. Furthermore for business continuity planning purposes managers need to be made aware of the above policy on network backups. Many staff we interviewed indicated that they were of the opinion they could retrieve records that were older than a year from backup tapes if required.

Recommendations and Management Response

22. **It is recommended that the Chief Information Officer appropriately inform managers that backup tapes are kept for only one year.**

This requirement is clearly documented in the backup policy, and Information Management Branch will choose an appropriate method to communicate it to all employees.

6. SECURITY OF ELECTRONIC INFORMATION

6.1 Processing of Classified Information

The Department requires that Classified information be processed in a stand-alone computer that is kept secure by physical means. This includes keeping it in a room that meets the requirements for processing and storing Classified information. Also, the Department requires that Classified information be transmitted electronically by secure fax instead of by e-mail. With the amount of Classified information processed in the Department, these requirements are no longer practical.

We found that unapproved methods for processing and transmitting Classified information are being used such as network servers, e-mail and C: drives. If network servers and e-mail are used for transmitting Classified information, these must be secure to the appropriate level. Also, C: drives must have the proper security safeguards.

While many staff are aware of security requirements for handling Classified information, they do not always know the security levels that apply or do not always follow the required procedures because they consider these to be impractical.

Recommendations and Management Response

- 23. It is recommended that the Chief Information Officer, in collaboration with the Director, Security Operations, Telecommunications & Accommodations Division, identify and implement a practical approach for the processing of Classified electronic information.**

There is no practical approach for processing classified information without a massive one-time and ongoing investment. IMB is studying the possible options to determine just what is required. However, we expect to confirm that massive investment is required. To give but one example, it should be noted that the CSE spent years and millions attempting to develop the Classified Message Handling System (CMHS) (secure e-mail system) and failed. PSEPC is leading another attempt, the Secure Communications Interchange

Program (secure e-mail system) and DOJ's interest in the project has been registered but we likely will not get access to it until the 2009/10 time frame.

The current process in DOJ is clear and must stand until the Department is able to undertake a significant investment. The DOJ network is designed to process Protected B information. Program managers having an ad hoc requirement to process Protected C or Classified information are to contact the IT Security coordinator for guidance. Program managers who have an ongoing need to process classified information should initiate and sponsor a project to create the appropriate secure system as was done for the Secure Systems Model or alternatively handle the data on physically secured stand alone devices.

6.2 JustAccess

The Department has several offices that are not directly connected to the departmental network. These offices include satellite offices of headquarters, ROs, as well as DLSUs and their satellite offices. Staff in these offices must use a secure connection that allows the processing of Protected B information. Currently, the Department is using JustAccess (implemented in June 2005) and a PKI service offered by PWGSC. Users connect to the departmental network to access the departmental Intranet, read regular information notices, access PeopleSoft for booking leave or checking their leave balances, and access other departmental systems. This method of remote connection works well for very few staff. Most staff indicated that it is cumbersome to use and they are frustrated with it, even though the service was improved.

Problems staff encounter with the remote connection service include:

- To use the service staff need a valid certificate (on a diskette). If they do not use the service for thirty days, the certificate expires and they need a new one, which can take weeks to obtain. In some cases they are asked to go to the East Memorial Building (for Ottawa/Gatineau sites) to obtain the certificate. In other cases a staff member from headquarters visits the DLSU or satellite office to issue new certificates. The expiry of the certificate is a security control enforced by PWGSC for all their federal government clients. IMB is aware of the problem and has advised that it will continue to have discussions with PWGSC to seek a solution.
- Users need to use a diskette that must be kept in a locked cabinet. They mentioned that it takes too much time to unlock the cabinet to get the diskette, sign on the network, and then sign on to the system they wish to use. If they make errors, it takes longer to sign on. As mentioned above, IMB is aware of the problem and is seeking improvements. One

improvement, the single sign-on (whereby users do not need to sign on more than once), was to be implemented in June 2005.

- Users are not sufficiently aware of the proper security requirements or assume that the new service (JustAccess) still has the limitations of the old system. For example, several users indicated that they are disconnected after 60 minutes of inactivity and need to sign on several times a day. However, the new disconnect time is three hours. Some users are using client facilities that are approved to process Protected A information for which the security controls are lower. Also, they mentioned that the support from the Justice Help Desk for connection problems was slow.
- When users are logged on to the departmental network using JustAccess, we were told they can access their C drive but not local client server drives. In our view this is an important security measure.

Recommendations and Management Response

24. It is recommended that the Chief Information Officer ensure that:

a) Efforts to reduce the time required by users to gain access to JustAccess continue.

IMB has augmented its IT Security staff strength and suggested process improvements to PWGSC staff.

b) Users are made aware of the reasons for the existing security controls.

This information will form part of the IT Security awareness program.

7. EDMS

This section details work completed toward an EDMS for the Department, key requirements and considerations, potential benefits, and client EDMS in use by DLSUs.

7.1 Work Completed Toward an EDMS

The Department has undertaken some pilot projects relating to electronic document management and certain DLSUs are using their own or client systems to record and access electronic records:

- We were informed that approximately ten years ago in the Atlantic Regional Office, there was a project using PCDocs to record electronic documents.
- In 2002, the Magellan project was conducted in the Montreal office. The project continued for one year and seven lawyers participated. Two screens were used: one for the document record and another one for the document. Upon completion of the pilot project, a report was written. The report indicated that significant tasks were involved in setting up the business rules for the document management system and the procedures relating to the use of the computer system.
- In 2002, IMB conducted a pilot of an EDMS at the Criminal Law Policy Section (CLPS). The initial scope was extremely ambitious and was later reduced. There were several difficulties with the pilot, including technical difficulties. Furthermore, Classified information (which was frequently used by CLPS) could not be processed. An assessment report was written and the pilot was stopped.
- Three DLSUs we visited were using some form of EDMS. (See “EDMS used by DLSUs”)
- RDIMS, which is an EDMS, was used on a trial basis at headquarters and in the Ontario RO after our visit.

7.2 Requirements and Considerations for an EDMS

The requirements for an EDMS have been discussed in several of the pilot assessment reports and in the reports completed in 2004 (referred to in “Strategies and Planning”). None of these reports documents complete requirements for an EDMS.

Key requirements and considerations for an EDMS include:

- An EDMS should not be an additional information management system but should replace or be integrated with some of the existing services or systems.
- Some existing IT services and systems should be considered in conjunction with an EDMS to increase productivity. For example, the simplification of the multiple databases for legal opinions could be considered.
- Workflows and how they will be improved should be considered. Lawyers do not have the time to do more administrative work.
- Duplicate documents and the storing of documents in different places should be reduced.
- Data should be captured and assigned to the proper records classification reference number initially, given the volume of records.
- The system must be easy to use, intuitive, and have easy links with e-mail and iCase.
- The EDMS software is only part of the solution. Other requirements include assigning staff to support and manage the EDMS and implementing standards.
- The Department must achieve a balance between assigning resources to an EDMS and improving the record keeping in related systems and IT services.
- Searches should provide options for separating data searched by type (such as legal, policy, administration) to decrease the number of search results. It will not be helpful to have an EDMS system in which documents can be stored, if the system stores information that is not easily searchable.
- The improvement of the management of electronic information will be an expensive and complex undertaking that should be properly funded.
- The cost estimates should be complete and include funds for upgrades, changes, enhancements, training, and technical and administrative support.
- There should be good references on how to use the system such as user guides and a Help function.
- The use of multiple or large screens should be considered for those who need them. This permits the display of multiple documents, a document and a record, or multiple pages of a document. This would decrease the need for paper, since one of the advantages of using paper is that full pages of the same document can be viewed side by side.

- There should be a determination of what mandatory activities will be required such as adding metadata to files and documents.
- Some lawyers will prefer to continue to work with paper versions of documents. Changing user habits will be a challenge.
- It will take a few years to implement an EDMS. Existing and new IT systems and services that will eventually provide data to the EDMS may need to be modified, and procedures may need to be developed so that the automatic transfer of records is possible. Also, before an EDMS is implemented, some immediate improvements, such as setting up and enforcing standards, should be considered for existing IT tools.
- The IMB implementation strategy should consider how the electronic records of DLSUs will be kept. Some already use the EDMS system of the client and all would require a permanent online connection between the DLSU and the departmental network. The DLSUs have concerns about a central departmental EDMS, given unsatisfactory experience in the past with computer connections to headquarters. Furthermore, the EDMS may need linkages with other client software and the Department will need client approval to install any software at DLSUs.
- Some DLSUs may want their data to be inaccessible to departmental staff outside the DLSU. For example the TBS DLSU mentioned that their data on union negotiations is highly sensitive.

7.3 Potential Benefits from an EDMS

An EDMS would bring significant benefits to the Department. It would:

- save staff time by reducing paper handling, providing better search capability, and decreasing the need to search for information in different locations (Time saved will depend on the type of work of staff members and how effectively they use the EDMS. Most legal assistants, paralegals, lawyers, and other staff indicated they would save time.);
- improve the quality of work by decreasing unproductive time, allowing faster access to information, providing more confidence that more complete and reliable information has been made available;
- provide better access control for documents and files;
- decrease the storage requirements for information by reducing duplication.

7.4 EDMS Used by DLSUs

Three DLSUs we visited were using some form of EDMS.

Agriculture Canada has been using a custom system based on Lotus Notes since 1998. It is used to keep records of files and electronic documents. Use of the system was mandatory at one time but that is no longer the case. Users indicated they were satisfied with the system. The system is not used by all staff and each lawyer decides what information to record in it. The system has 2,000 files and 39,111 documents. The DLSU's official files are still in paper form.

Fisheries and Oceans has been using the client EDMS (Foremost and DOCSOpen) for about three years. The system is a pilot of which six DLSU lawyers are part. The DLSU does not have a formal project management framework for the pilot or monitoring of how much the system is used. There are 7,054 files in Foremost and there are 26,277 documents in DOCSOpen.

Natural Resources has been using DOCSOpen for about seven years. The Senior Counsel has directed staff to use DOCSOpen for legal opinions, but there is no monitoring of its use. Most users are not satisfied with the search function. There are too many search results and the documents are not organized by area of law. However, DOCSOpen is used by staff and they told us it saves time. There are no standards on how to use it. Anyone in the DLSU can use it. The DLSU has recorded 22,000 documents in the system.

No direction can be provided to DLSUs with respect to an EDMS until the Department has taken a decision on a plan for its own EDMS and a strategy for the DLSUs.

Recommendations and Management Response

25. It is recommended that the Chief Information Officer proceed with the implementation of an EDMS.

The CIO agrees with this recommendation but notes that BIT.COM was informed that an estimated cost for implementing an EDMS for the department would be in the range of \$16M. The initial implementation plan for RDIMS confirmed a similar cost. At the current investment rate, it is unlikely that RDIMS will be fully implemented in the Department of Justice before 2014.

8. IMPACT OF ELECTRONIC INFORMATION MANAGEMENT ISSUES

In this section we are focusing on how current issues and risks with electronic information management affect the key business aspects of productivity and corporate memory. Key ATIP issues are also addressed.

8.1 Productivity

Paper Versus Electronic Records

From our interviews we estimate that on average staff currently access electronic information 70% of the time and paper 30% of the time. Issues with electronic information management, therefore, have a significant impact on productivity.

Staff we interviewed indicated existing IT services and application systems had the following benefits:

- Users find the existing IT services and application systems useful.
- Most staff can find the information they need (in electronic or paper form), although they do not have access to all required information.
- A few said they are satisfied to work with the existing systems and paper files.
- Many working with legal files said that an improved iCase system could meet their requirements.

Many staff members indicated they preferred working with electronic records. We found a number of productivity issues with respect to current information management processes. More issues will arise with regard to electronic information management specifically as the amount of electronic information increases.

There are a number of issues with using paper records:

- Using paper is time consuming. Documents must be printed, handled, filed, tracked, stored, and manually retrieved when needed.

- Paper takes up significant space, which is costly. The Department must justify space required that is greater than the PWGSC standard and pay for it. Space used for records is taken up by filing rooms, cabinets, and free space around the cabinets. That represents 14,528 m² of space (13.3% of departmental usable space). Space can be as expensive as \$600 m² per year in Toronto. Although we do not present exact costs here, the rents paid for space used by paper records is significant.
- Paper files are not accessible if they are stored in offices where the file room is closed after regular office hours.
- Paper files are not easily accessible if they are stored in file rooms on other floors or in other staff members' offices. In practice, some staff do not promptly give files to records management but keep files in boxes in their offices, sometimes for years.
- Paper files are occasionally misplaced and documents can be removed from paper files.
- For a large file it is difficult and at times impossible to physically carry copies of all the necessary documents
- Controlling access to specific files is difficult. Conflict-of-interest situations arise when lawyers who previously worked in private legal firms in an adversarial role to the Department have access to certain files.

Issues of organization and disposition of paper records need resolution because the same issues apply to electronic records.

Staff indicated that paper is sometimes the preferred medium:

- Some lawyers prefer paper; some print documents to take home.
- Paper is used for handwritten notes, and comments are also written on paper documents.
- Some paper files can usually be read (visually scanned) faster than their electronic version.
- Some sections such as Human Resources are very much paper-oriented for the bulk of their filing such as job classifications, competitions, and employee information.
- Unless electronic signatures are available, some information may need to be in paper. For example, TBS requires that job descriptions be signed.

Searching for Information

The nature of the work in the Department is that typically time is of the essence. In searching for necessary information, efficient use of time is important for staff. Information (in both paper and electronic formats) is not found in one location. Searching a large paper file is time consuming and the required document may be missed. With respect to electronic information, staff must decide what system or service to use to look for the required information. Also, different IT

services and systems have different search routines and searches may be limited to a specific server. A system may contain a large quantity of information. However, lawyers sometimes do not have access to certain information because of certain restrictions. We were told that some lawyers would like access to information that is currently inaccessible.

We found that searching for information affects staff productivity in the following ways:

- There is duplication of work. Staff are unable to access or have insufficient time to find information on similar work previously done by others. Staff told us that they had found relevant information weeks or months after they had completed a task.
- The Department has many different systems that maintain separate information. Information may be in the e-mail system; on personal, shared or other drives; in the paper file; and in various application systems. Each has a different search function. Users may have difficulty remembering how to use the various systems.
- Duplication of information results in more documents or records for staff to search through. Most paper information is also kept in electronic form. Electronic information is often duplicated in different systems such as e-mail, personal drives, shared drives, certain legal systems, and Web sites. There is much duplication in the e-mail system, as a user will have information stored in both sent and received messages, and the same message will be stored by various recipients. The same document may also be kept in different formats such as WordPerfect, Word, and Portable Document Format (PDF). Staff do not have the time or tools available to work on decreasing duplication.
- No one electronic system contains complete information. The paper file is also incomplete because not all e-mail messages or drafts may have been printed and filed. As a result, staff keep their own copies of required information, adding to the duplication.

Quality of Work

Inadequate information management policies and processes can impact quality of work in various ways:

- Consistency in departmental legal positions or the appropriateness of legal advice may be compromised as a result of inadequate sharing of information. This is in conflict with the departmental objective to speak with one voice. Also, lawyers may use a legal opinion from LOPORS, but another system may contain a more recent opinion that was not available in LOPORS, or even, a contradictory opinion.
- Without standards, lawyers have on occasion released to clients and other lawyers or presented at court the wrong version of a document. This type of error can occur because

documents are shared (i.e. multiple updaters) and an individual lawyer may not be aware that a more up-to-date version of a document is available. Also, deadlines are tight.

- A lack of access to required departmental information may affect the quality of work since lawyers must do more research or re-create existing information.

8.2 Corporate Memory

We found that corporate memory is not well maintained in the Department. Paper files are incomplete because much electronic information is not printed and some electronic information is deleted without being printed. Paper records are no longer adequate for tracing all the information that led up to a legal decision or that was related to an issue. Information pertinent to an issue may be divided among many locations. If information on an issue is stored on paper, portions of the information may be stored in many files and documents that can encompass several years of information. In the case of electronic records the records may not be complete. They may be maintained on different IT services/systems and may be difficult or inefficient to access.

Staff are not sufficiently aware of what can be deleted (e.g. e-mail messages with multiple recipients). With regard to some messages that have multiple replies, staff may delete intermediate messages even though the final e-mail does not always contain complete information from all the exchanged e-mails. Each staff member makes the individual decision to keep or delete a specific draft of documents. Some keep all versions and others keep only the final or key versions.

In some offices data belonging to former staff (i.e. e-mail messages, personal drive folders, and personal directories on the shared drive) are kept for a few weeks and then deleted. In other offices staff spend a limited time organizing their electronic information before they leave. The information is placed in the C drive for their replacement or given to their assistant. Often data belonging to staff is transferred in bulk from their e-mail account, personal drive folders, and personal folder in the shared drive to removable media or an electronic folder used to keep the information of former staff. Reviewing and organizing several years of data is a cumbersome and practically impossible task and typically not well done. A process whereby staff regularly review their electronic information and transfer it to an appropriate system or section to be stored as corporate records would be better.

Currently, there is no requirement to keep electronic records once they are printed. The deletion of electronic records is a loss of corporate memory.

Recommendations and Management Response

- 26. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads ensure that electronic information is stored in such a manner that it may be easily retrieved in the future, and monitored as appropriate.**

Information Management Branch will ensure that departmental employees are aware that, until the complete implementation of RDIMS, corporate records that cannot be stored as paper should be maintained on shared or personal drives, or be maintained as active records within the appropriate applications.

8.3 Access to Information and Privacy

We were told by departmental staff that generally all paper records are searched in response to Access to Information and Privacy (ATIP) requests. However, some of the staff who receive requests from the ATIP Office informed us that they do not always search electronic records, as official departmental records are stored in paper form.

Within the Department, the Access to Information and Privacy Office sends information requests by e-mail to contact persons in relevant departmental sections. These contact persons in turn send e-mails to staff who may have relevant information pertaining to the request. These staff members are required to provide the contact person with all relevant information. Consideration could be given to improve the retrieval process; for example, the contact person could work directly with originators or area experts to review and retrieve electronic holdings. ATIP has indicated that guidelines will be revised accordingly to ensure that departmental staff are apprised of that requirement.

9. RECOMMENDATIONS AND MANAGEMENT RESPONSE

The CIO, IMB provided the following general comment.

The Information Management Branch (IMB) acknowledges the importance of the audit recommendations and is generally supportive of these. However, it cannot commit itself to completing the work required to address all the issues identified.

Based on the Strategic Information Management Framework approved by senior management before the audit, IMB will continue to work at improving the overall state of Information Management (IM) in the Department, within available resources. Actions will remain focused on areas with the highest return on investment and / or the highest business risks faced by the department.

Over the foreseeable future, investments will mainly be concentrated on raising IM awareness of employees and managers, implementing an electronic document management system, and building a core human resource capacity to support the departmental IM program.

1. It is recommended that the Chief Information Officer ensure that:.....18

a) Standards for the management of electronic information including e-mail are issued so that the information can be easily managed as departmental records.

The Information Management Branch is in the process of completing a Guideline on Managing Departmental Information. The implicit “standard” for the long-term management of information created in Outlook is RDIMS, the Government of Canada shared services initiative for electronic document and records management. Information Management Branch has received the endorsement of BIT.COM and funding from the Corporate Reserve to implement a pilot project for RDIMS. However, the current timeframe for implementing RDIMS, department-wide, is four to five years.

- b) As relevant standards, processes, and systems are put in place, increased direction is provided to departmental units and staff to manage electronic information.**

The RDIMS implementation strategy includes components for increased training and communication to staff in their accountabilities for information management. Training and communication will occur concurrent with the implementation of RDIMS in business units.

- c) As relevant standards, processes, and systems are put in place, the implementation of the IMB *Information Management (IM) Policy* is monitored.**

The Information Management Branch has developed a review guide to assess how well business areas, including LSUs, are managing paper records. As RDIMS is implemented, the guide could be modified to include the management of electronic records. However, in order to appropriately monitor understanding of, and compliance with, the IM policy framework, the Branch must develop a business case to adequately resource what is essentially a new function.

- d) Reference to productivity gains is made in standards and when communicating these standards to staff.**

There are no reliable industry standards for assessing productivity gains at this time. However, as we develop standards, the Information Management Branch will communicate to all employees the effectiveness of electronic document and records management, based on the best information on productivity gains available at the time.

- e) Accountability frameworks for the management of electronic information are developed.**

The Information Management Branch is employing the departmental IM/IT Project Management Framework to ensure sound management of the RDIMS project. The Framework requires a project charter, including a clear statement of roles and responsibilities, as well as a project plan and a full accounting of project costs.

- f) The approval of the revised current disposition authorities by LAC is pursued.**

The Branch has negotiated an MOU with Library and Archives of Canada for the development of a comprehensive Records Disposition Authority. Work identified in the MOU will soon be underway, with completion of the project forecast for 2008/09.

2. It is recommended that:.....19

- a) The Chief Information Officer direct that electronic records are kept in a format or can be converted to a format that may be acceptable to LAC.**

See response to 1f) above.

- b) The Chief Information Officer, in consultation with the Director General, Communications, direct that Web content is kept in a format or can be converted to a format that will be acceptable to LAC.**

The CIO will raise with the LAC the issue of appropriate format for any records identified for transfer. The negotiation of a comprehensive Records Disposition Authority for the Department will provide an opportunity to do so.

3. It is recommended that the Director General, Communications collaborate with the CIO to ensure that information posted on departmental Web sites is recorded and managed through the life-cycle in accordance with the MGI policy, *Department of Justice Information Management Policy*, and the *Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites*.19

Efforts to ensure appropriate life-cycle management of web content are dependent upon, and must follow, the acquisition of the appropriate content management applications and their subsequent implementation. It should be noted that the introduction of an Enterprise content management application will exceed existing budgets for intranet and internet in the Department. In addition, a review of two of the three policies cited (The Policy on the Management of Government Information, and the Department of Justice Web Sites Policy and Procedures for Internet, Intranet and Extranet Sites) is underway; the relevant directives and standards cited in the succeeding policies will be observed once these take effect.

- 4. It is recommended that the Chief Information Officer continue efforts to implement a revised organization of the Information Management. In line with this, the CIO should review with the regions the organization and staff skills required and with DLSUs the staff skills needed to improve the management of electronic information.21**

The CIO will initiate a discussion, involving Regions, HQ and Legal Service Units, on a standard information management organization later in the current fiscal year.

- 5. It is recommended that the Chief Information Officer ensure that:.....24**

- a) An implementation plan to improve the management of information including the management of electronic records is prepared as requested by BIT.COM and monitored.**

Information Management Branch has developed an implementation plan for RDIMS. BIT.COM has accepted it as a general plan for the project. The plan will be refined as the project progresses.

- b) Preliminary activities needed for improving the management of electronic information are identified in the implementation plan.**

Specific activities such as providing business units with information management training, clarification of roles and responsibilities, are currently being worked into the RDIMS implementation plan.

- c) The implementation plan is coordinated with regional offices and DLSUs.**

Clarifying accountabilities, roles and responsibilities is essential to a successful RDIMS implementation. Documentation, for discussion with all parties implicated in the project rollout, is currently under development and we anticipate confirming roles, responsibilities, service levels and timing of implementation with Regional Offices and other stakeholders in the fall of 2006, as part of the development of the Project Charter and refined project plan. If the project receives full approval, IMB will make every effort to coordinate its activities with the business areas affected by the implementation.

d) Solutions for improving management of electronic information take into account information processed by application systems, IT services, and other processes dealing with electronic information used in the Department.

The proposed MOU with Library and Archives of Canada will address the disposition of departmental records, regardless of medium. The development of a revised Records Disposition Authority will provide the opportunity to ensure full life-cycle management (including legal destruction) of structured data, such as that associated with applications such as IFMS and PeopleSoft, as well as unstructured data in RDIMS.

6. It is recommended that the Chief Information Office ensure that for EDMS topics usually addressed in business cases are documented and presented to BIT.COM.25

Many of the components of a business case are included in the RDIMS Implementation Strategy. In addition to providing BIT.COM with briefings on the RDIMS implementation, the project must submit relevant information on budget, milestones achieved and overall project health to the BIT.COM sub-committee, the Investment Review Committee, to receive yearly approval to continue implementation.

7. It is recommended that the Chief Information Officer ensure that complete costs, including regional and DLSU costs, are estimated for the implementation plan to improve the management of electronic information.....26

Please see response for Recommendation 1e).

8. It is recommended that the Chief Information Officer consider options for preparing reports on electronic information.....27

The Information Management Branch does provide high-level reports on various aspects of information creation, use and storage for BIT.COM. Specific reports might be developed on information management practices, for use by program managers, in future. Until such time as the Department receives a Records Disposition Authority from the Library and Archives of Canada for the legal destruction of electronic records, the customized reporting may not be worth the effort required to design and produce them.

- 9. It is recommended that the Chief Information Officer ensure that as tools and training become available for the improved management of electronic information, policies, standards, and guidelines are effectively communicated to staff.28**

The Information Management Branch will ensure that a communication plan accompany the release of policies, guidelines and standards, on a go-forward basis.

- 10. It is recommended that the Chief Information Officer, in collaboration with heads of ROs and DLSUs, ensure that efforts to hire or assign appropriately qualified staff for IM staff are implemented.....29**

The proposed IM Human Resources study (see response to Recommendation 4) would address standard IM organizations, position levels, and required competencies.

- 11. It is recommended that the Chief Information Officer ensure that:.....30**

- a) as part of the improvement of the management of electronic information, appropriate training is made available to staff;**
- b) attendance at training is monitored.**

The Branch anticipates the introduction of an on-line IM orientation course, intended for all staff later in the current fiscal year. Participation rates will be monitored.

- 12. It is recommended that the Chief Information Officer seek to make key courses mandatory if staff are not attending the required courses.30**

Agreed.

- 13. It is recommended that the Chief Information Officer ensure that:.....34**

- a) A strategy is prepared for the use and management of shared drives.**

The Information Management Branch currently provides support, when requested, to business units to assist them in establishing taxonomies to organize records on shared drives. However, the ongoing management of information on shared drives is the responsibility of the business unit.

- b) Standards and guidelines are issued for the use of personal and shared drives to ensure the consistent and efficient use of these drives and to meet departmental information management requirements.**

A Guideline on Managing Departmental Information is currently under development and will be available for all staff presently. The Guideline will explain how to organize and manage information on shared and personal drives.

- 14. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads ensure that:34**

- a) The strategy for the use and management of shared drives is implemented.**

The Guideline on Managing Departmental Information will apply to all staff of the Department once approved. However, members of DLSUs typically store information on the drives of the host department and may be subject to whatever policies and guidelines these departments currently have in place.

- b) Information is stored in personal and shared drives in such a manner that it can later easily be imported to an eventual departmental EDMS.**

Organizing information according to the Guideline will make a transition to RDIMS relatively simple for a business unit.

- 15. It is recommended that the Chief Information Officer ensure that standards for the management of removable media are developed and request that headquarters and regional office directors and DLSU heads implement the standards.....36**

Such standards exist and it will simply be a matter of choosing the optimum communications method to inform regional offices and DLSUs of them.

- 16. It is recommended that the Director General, Communications and the Chief Information Officer collaborate to develop and implement standards to facilitate the management of Web publications as departmental records in accordance with the MGI policy.....37**

Upon the phased-in implementation of Enterprise content management and document management applications, the Director General, Communications and the CIO look

forward to the implementation of standards for information management, including web publications and other web content.

The cost of implementing these applications is a significant factor in how effectively the Department can enforce a complete information management accountability framework.

- 17. It is recommended that the Chief Information Officer ensure that standards for the scanning of documents are developed and request that headquarters and regional office directors and DLSU heads ensure their implementation.....38**

Standards exist for importing scanned information to Ringtail, the departmental standard application for litigation support and evidence management. Developing more generic guidance for scanning information for business purposes may be considered as part of a future direction for the RDIMS project. Scanning is currently not in scope for the project. Including this requirement in the RDIMS project will require additional funding.

- 18. It is recommended that the Chief Information Officer provide guidance and appropriate tools to improve processes for the sharing of information.39**

The Branch is currently assessing possible technology/applications for collaboration and information sharing.

- 19. It is recommended that the Chief Information Officer ensure that a strategy is developed and implemented for the management of electronic information contained in application systems.....44**

The Information Management Branch is collaborating on the development of a departmental Knowledge Management Strategy that will address the role of various applications in ensuring an effective use of IM/IT resources in support of law practice in the department. In addition, the proposed MOU with Library and Archives Canada (see response to Recommendation 1, part f) will address life cycle management issues for all records, including those in applications.

- 20. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads preserve non-transitory electronic information.46**

As the Information Management Branch works with the Library and Archives of Canada to develop a comprehensive Records Disposition Authority, we will seek to clarify the

retention periods on all information, including electronic information, and provide guidance to business units on what to preserve and how.

21. It is recommended that the Chief Information Officer ensure that information of enduring value is transferred to Library and Archives Canada.....46

The Information Management Branch currently transfers paper records identified to have archival value to the Library and Archives of Canada on a regular basis. Once the Library and Archives of Canada (LAC) identifies the electronic records of the Department of Justice it deems to have archival value, and once the LAC identifies preservation format and transfer standards, Information Management Branch will comply with this recommendation.

22. It is recommended that the Chief Information Officer appropriately inform managers that backup tapes are kept for only one year.....47

This requirement is clearly documented in the backup policy, and Information Management Branch will choose an appropriate method to communicate it to all employees.

23. It is recommended that the Chief Information Officer, in collaboration with the Director, Security Operations, Telecommunications & Accommodations Division, identify and implement a practical approach for the processing of Classified electronic information.49

There is no practical approach for processing classified information without a massive one-time and ongoing investment. IMB is studying the possible options to determine just what is required. However, we expect to confirm that massive investment is required. To give but one example, it should be noted that the CSE spent years and millions attempting to develop the Classified Message Handling System (CMHS) (secure e-mail system) and failed. PSEPC is leading another attempt, the Secure Communications Interchange Program (secure e-mail system) and DOJ's interest in the project has been registered but we likely will not get access to it until the 2009/10 time frame.

The current process in DOJ is clear and must stand until the Department is able to undertake a significant investment. The DOJ network is designed to process Protected B information. Program managers having an ad hoc requirement to process Protected C or Classified information are to contact the IT Security coordinator for guidance. Program managers who have an ongoing need to process classified information should initiate and

sponsor a project to create the appropriate secure system as was done for the Secure Systems Model or alternatively handle the data on physically secured stand alone devices.

24. It is recommended that the Chief Information Officer ensure that:.....51

a) Efforts to reduce the time required by users to gain access to JustAccess continue.

IMB has augmented its IT Security staff strength and suggested process improvements to PWGSC staff.

b) Users are made aware of the reasons for the existing security controls.

This information will form part of the IT Security awareness program.

25. It is recommended that the Chief Information Officer proceed with the implementation of an EDMS.....56

The CIO agrees with this recommendation but notes that BIT.COM was informed that an estimated cost for implementing an EDMS for the department would be in the range of \$16M. The initial implementation plan for RDIMS confirmed a similar cost. At the current investment rate, it is unlikely that RDIMS will be fully implemented in the Department of Justice before 2014.

26. It is recommended that the Chief Information Officer request that headquarters and regional office directors and DLSU heads ensure that electronic information is stored in such a manner that it may be easily retrieved in the future, and monitored as appropriate.61

Information Management Branch will ensure that departmental employees are aware that, until the complete implementation of RDIMS, corporate records that cannot be stored as paper should be maintained on shared or personal drives, or be maintained as active records within the appropriate applications.