DEPARTMENT OF THE

SOLICITOR GENERAL CANADA

Audit of Departmental Compliance to the Management of Government Information Holdings (MGIH) Policy

February 28, 2002

FINAL

Prepared By

IMT Solutions Inc.

2323 Whitehaven Cres.

Ottawa, Ont.

eklach@rogers.com

(613) 828-6358

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

An audit of the Department's compliance to the Management of Government Information Holdings Policy (MGIH) was conducted between October and December 2001.

An overview of work processes through information gathered by questionnaires and a Focus Group session with staff revealed that the Department has an excellent handle of its paper records. The paper medium is the Official Corporate Records copy. Most legislative and Treasury Board Secretariat policies are being met. The greatest issue for the Department is its lack of control over electronic records, especially e-mail. Staff find it impractical and difficult to convert e-mail to the paper medium. In keeping with the trend experienced by most other government departments, non-compliance and risks of non-compliance to MGIH is very likely when electronic records are involved.

Other findings can be summarized as follows:

The Department has not developed a corporate view for its Information Management Program. Knowledge and Best Practices for managing information, which are evident in the Department, are not shared. There is a lack of corporate strategy for managing electronic information holdings. The Departmental culture is not ready to embrace the responsibility of managing electronic records at the desktop with the limiting capabilities of current technologies that rely on users to add profiles/metadata descriptors to individual records for filing. Nor is the Department equipped with an adequate tool for desktop electronic records management. With respect to electronic information, the Department does not have a classification system, policies, guidelines and standard operating procedures to help staff deal with processes of record review, evaluation, classification, filing and disposal.

There is strong desire on the part of Departmental staff to embark on a technology solution to address the issues of finding and managing corporate records. However, the audit findings indicate that the Department has a great deal of preparatory work that needs to be done before investment in technology can have a return on its value. Most rules that exist in connection to MGIH do not depend on technology solutions. The base for Good Information Management Practice is a Corporate Vision articulated in a Corporate Information Management Strategy, supported by common tools throughout the organization, policies, standard operating procedures and a trained pool of staff responsible for leading information management initiatives.

2 BACKGROUND

The Department of the Solicitor General (Department) is a small policy focused organization, comprised of approximately 235 full time equivalents (FTEs), which provides policy advice and support to the Solicitor General with respect to his responsibility for the provision of direction to the following agencies: Royal Canadian Mounted Police; Canadian Security Intelligence Services; Correctional Service of Canada; and the National Parole Board; his accountability to Parliament for the agencies; for his national leadership role in the federal activities in policing, national security, corrections and conditional releases; and in his role as the Minister responsible for Aboriginal policing.

The Management of Government Information Holdings (MGIH) Policy was created in 1989 for the purpose of guiding government departments in applying federal legislation and Treasury Board Policies relating to information management.

The overall statement of the policy is a directive to manage all information holdings as a corporate resource. The approach of the policy is to support effective decision-making, meet operational requirements and protect the legal and financial interests of the government and public. As this policy aims to incorporate all requirements vested in Treasury Board policies related to information management and all Acts that deal with information management it is the definitive source for direction on how information must be managed in the federal government. The current version of the MGIH Policy is being up-dated by Treasury Board Secretariat (TBS) and National Archives of Canada (NA). Based on the exposure draft of the new policy (May 2001), it is expected that the new MGIH Policy will incorporate the requirements of the current policy and in addition include requirements under legislation and policy directives that specifically target electronic records. This audit includes a review of current compliance to the 1989 version of MGIH, and the readiness of the Department in managing its electronic records in compliance to new aspects of legislation and policies that came into force since the last issue of MGIH. This audit also covers best IM practices that have been adopted by leading organizations for compliance to legislation and policies. All major Acts and policies covered by MGIH, and on which this audit is based are summarized and provided as part of the audit working file.

3 OBJECTIVES AND SCOPE OF AUDIT

The objectives of the audit were to review and assess the current state of the Department's functions in Records Management, Forms Management, Management of the Library collection/holdings, Information Security and Access to Information and Privacy for compliance to the Treasury Board Secretariat's primary information management policy.

The scope of the audit covered all Departmental activities, controls, mechanisms, and systems related to the Department's MGIH. The audit focused on issues of compliance to central agency principals, legislation, policies, regulations and guidelines related to the MGIH. In particular,

the audit focused on the management of electronic records, accountabilities for information holdings, and management of information on the Departmental Web-site.

4 AUDIT METHODOLOGY

The audit was conducted between October and December 2001. The audit methodology was based on generally accepted information management auditing procedures for the public service, and followed the Treasury Board Secretariat's *Guide to the Review of the Management of Government Information Holdings.*

The audit included a planning phase, a fieldwork phase and a reporting phase. During the planning phase, key issues to be addressed in the fieldwork phase of the audit were identified and included in an Audit Planning Memorandum. The results of the fieldwork phase of the audit are depicted in this report.

Data gathered during the audit was obtained through interviews, using questionnaires to guide the interviews, the holding of a focus group, a review of relevant documentation and systems. A list of the persons interviewed and the participants of the focus group are identified at Appendix "A".

5 AUDIT FINDINGS AND RECOMMENDATIONS

The purpose of any audit is to identify areas of potential risk to the organization. Definition of risk in the Government Information Management context could be stated as follows:

"Non-compliance to MGIH constitutes non-compliance to some IM related legislation, policy or best information management practice. Non-compliance results in loss of vital information, inability to safeguard information, and all other factors that will incur unreasonable costs and adversely affect the delivery of programs, and where these factors may cause embarrassment to the Minister and managerial staff, and/or suspend trust by the public and clients in the services that are being provided."[1]

[1] IMT Solutions Inc., *Managing Information in the Federal Government*, Ottawa, May 2000, http://www.imtsolutions.ca

5.1 MGIH Policy Requirements

5.1.1 **Requirement One** :

Institutions must:

Plan, direct, organize and control their information holdings through their lifecycle, regardless of the form or medium in which the information is held.

Summary: Not Fully Compliant

Areas of Compliance:

- The Department plans, directs and controls information holdings through their lifecycle in the paper medium only.

Areas in Need of Improvement:

- Electronic information is not under the control of lifecycle management.

Cause(s):	1. Departmental policy is to treat electronic information as convenience copies and/or transitory records. (All staff have the responsibility to make a hard copy record for storage in the Records Office. Electronic records are destroyed when no longer needed.); 2. Strong consensus among Departmental staff that the storage/disposal policy and practice is inconvenient but meets all regulatory requirements.
Potential Risks:	1. There is no guarantee that all corporate records are indeed copied and saved as a record; 2. The audit trail of records creation is lost unless all drafts and working notes are included on the Official Records—hard copy file. This includes e-mail messages and attachments. This is not always done; 3. Since electronic "copies" are not destroyed at the time of transfer of the hard copy to the Records Office, at any time there could be multiple copies of a single record for reference and use. Mistakes could be made if staff, for whatever reason, but usually for convenience, use an electronic copy for reference not realizing that the hard copy records often gain "supplemental notes" during their active life. (It is easier to write a note on a paper document than add a note to an electronic copy.) Electronic "convenience files" are the most frequent source of incomplete information used in a business decision.
Recommendations:	1. Convenience records should be assigned a retention period; 2. Policy on the use of convenience records for business decisions should be issued especially in areas where paper records are the official corporate copies, and where electronic copies are the convenience copies.

5.1.2 Requirement Two:

Institutions must:

Maintain a current, comprehensive and structured identification or classification system or systems which provide an effective means for organizing and locating information and, in composite form, comprise a corporate inventory for managing the institution's information holdings.

Summary: Not Fully Compliant

Areas of Compliance:

- Classification system is valid for paper records.

Areas in Need of Improvement:

- Electronic records are not under the control of a classification system;
- The current classification system may not be valid for electronic record holdings.

Cause(s):	1. There is a strong conviction among Departmental staff that as long as electronic records are convenience copies only, they do not need a classification system.
Potential Risks:	1. Without some sort of indexation for convenience copies, it is not possible to identify and distinguish between convenience copies that hold a different legal value. Copies of records that show the evolution of an official record—copies of versions of official drafts and copies of final official records—can't be destroyed when the content of the records relates to a case that is in the courts or falls under the Access to Information Act until the courts, or reviewing officials, are satisfied that all originals have been retained and made available. (As illustrated in the current record destruction issue at Enron and Anderson Consulting in the USA, and the well known issues of finding all relevant documents to meet an ATIP request.) Copies of various versions of "personal drafts"—personal work files as defined under the Transitory Records Authority, can be destroyed at any time. 2. Without a classification system, of some sort for electronic records, it is difficult to destroy/cull/clean one's desktop of irrelevant information that clogs up the system; 3. Allowing staff to work with files without a classification schema reinforces a negative practice, which will be hard to change once electronic records are declared as part of the Official file. (Official electronic records must have a classification/indexation schema).

Recommendations:	1. An analysis should be undertaken to identify and implement what is the best schema, what is the most acceptable method of classifying electronic records for identification and for application of disposition policies.

5.1.3 **Requirement Three**:

Institutions must:

Manage all confidences of the Queen's Privy Council for Canada in accordance with government-wide standards established by the Privy Council Office and set out in Appendix A of the standards.

Summary: Fully Compliant

Areas of Compliance:

- Ministerial correspondence and confidences of the Queen's Privy Council are managed according to the standards and practices stipulated by legislation and policy. ccmMercury is used as Ministerial correspondence tracking system. Records management lifecycle is applied to the records through iRIMS.

5.1.4 **Requirement Four**:

Institutions must:
Designate a senior official to represent the Deputy Head to Treasury Board Secretariat and other central agencies for the purposes of this policy.

Summary: Fully Compliant

Areas of Compliance:

- Fully compliant. The Director General, Corporate Services Directorate is the designated Senior Official under the MGIH policy.

5.2 Compliance to Legislation Related to MGIH

5.2.1 National Archives of Canada Act

Summary: Fully Compliant only for records under the control of records management:

Areas of Compliance:

- Currently, paper records are the official copy;
- Disposition Plan signed;
- Access to records by Archives staff was granted, records have been appraised;
- Records are organized under a usable classification system;
- Records created by electronic media are printed, stored in a paper medium in the records office;
- Files on loan are controlled and accounted for;
- Archival records are protected from destruction;

- Retention periods for archival records exist;
- Forms are reviewed for compliance to departmental forms policy;
- An electronic inventory of the records in the Records Information Management System (iRIMS) is implemented;
- A scanning system connected to the iRIMS will introduce staff to the management of electronic records, and will be tested shortly;
- Archival records are submitted for permanent retention to the NA;
- Ministerial correspondence is managed by ccmMercury software, which is now integrated with iRIMS. Records are well organized;
- Ministerial (non-personal) records are being transferred for permanent retention to NA (According to NA Ministerial collection inventories); and
- Ministerial Records are under the control of the Privy Council Office and not Department.

Areas in Need of Improvement:

- Lack of efficiency through reliance on a paper based system as the official record medium;

Cause(s):	1. Departmental policy identifying official records by the medium rather than by the content.
Potential Risks:	1. Difficulty in applying short retention periods to a collection of sensitive or bulky record files where a specific content item, disbursed in paper based records files, requires a longer retention period than the majority of the records; 2. Transferring all records from an electronic system, especially e-mail, to a paper based system, arranging the records, storing them and indexing them for retrieval is very resource intensive and most unreliable for integrity and completeness.
Recommendations:	1. Analysis should be conducted to identify what types of records could be retained in an electronic system as Official Records.

- Limiting Record Office hours suggest that staff keep records, or copies of records, at their desk so they can have unlimited access to frequently used records;

Cause(s):	1. Records Office is accessible only during regular working hours. Since official records can only be accessed during regular working hours larger collections of convenience records are kept by staff at their workstation.
Potential Risks:	1. Mistakes could be made if staff, for whatever reason, but usually for convenience, use an electronic copy for reference not realizing that the hard copy records often gain "supplemental notes" during their active life. (It is easier to write a note on a paper document than add a note to an electronic copy.) Electronic "convenience files" are the most frequent sources of incomplete information used in a business decision. However, convenience hard copy

	records at the work desk also inherit the issue of missing "new" information on the Official File, which is accessible only at the Records Office.
Recommendations:	1. Convenience records should be assigned a retention period; 2. Policy on the use of convenience records for business decisions should be issued especially in areas where paper records are the official corporate copies, and where electronic copies are the convenience copies.

- Possibility that not all archival records are printed and passed for control to records management;

Cause(s):	1. Lack of direction on what constitutes an Official Records under the National Archives Act.
Potential Risks:	1. Non-compliance to the National Archives of Canada Act; 2. Non-compliance under the Canada Evidence Act; 3. Non-compliance under the Access to Information and Privacy Acts.
Recommendations:	1. The Department must have a policy and standard operating procedures for the identification and storage of all records documenting the evolution of an official record as defined under the Transitory Records Authority issued by the NA; 2. The Department must ensure that records documenting the evolution of official records are available for an archival appraisal; 3. Archival records must be transferable to NA upon the expiration of the retention period assigned to the records by the Department.

- "Employee Security and Safety Instructions" ask staff to clean systems of old files. However, under the National Archives of Canada Act, no record can be destroyed without the consent of the National Archivist of Canada. To receive consent for the destruction of electronic records, NA must approve the methodology of preserving records as official copy in *another* medium;

Cause(s):	1. Lack of proof that current policy of retaining Official Records in hard copy is followed for all corporate records created in electronic media, such as e-mail.
Potential Risks:	1. NA may not grant Disposition Authority for electronic media during the next review of Disposition Plans with the Department; 2. Destruction of records documenting evolution of Official Records, business decisions etc. is in contravention of the National Archives of Canada Act, the Canada Evidence Act and the Access to Information Act.

Recommendations:	1. Consolidation of all directives for an e-mail policy should be made available in one, clear, concise document, easily accessible at the desktop; 2. Standard Operating Procedures for identifying Corporate Records at the desktop, and directions for Corporate retention, including migration of records from one medium to another, should be developed and made available to all staff for quick reference; 3. Documentation on records migration from one medium to another must comply with the guidelines outlined in Part IV of the Canadian Standards Board's Microfilm and Electronic Images as Documentary Evidence (Can/CGSB-72.11-93). (Part IV of the Standard is a summary of international standards applicable to the management and documentation of all systems used to hold or manage official legal records, regardless of media.)

- The Department intends to scan paper records and offer them electronically to staff in the near future. However, no plans, showing how the Department is preparing for meeting the legal and archival scanning requirements under the Multi-Institutional Disposition Authority (MIDA), were provided for this Audit.

Cause(s):	1. The department has not created a plan for the scanning of records.
Potential Risks:	1. Non-compliance to MIDA's reference to Records Disposition Authority No. 96/023 could result in costs associated with changing current systems, processes or even be subject to a revoking of Disposition Authorities;
Recommendations:	1. The Department should examine closely the requirements under MIDA, and specifically, requirements under the Records Disposition Authority No. 96/023 which relates to Electronic Imaging Systems.

- There is a total under-use of Transitory Records Authority.

Cause(s):	1. Records management staff have not been trained to be able to define, identify Transitory Records in the Department.
Potential Risks:	1. Too many Transitory Records are being retained on the electronic systems and these clog up the servers and disc spaces; 2. Too many Transitory Records are retained as Corporate Records on the Official Corporate Files; 3. Too many corporate records are being destroyed before copies are retained by the Records Office.
Recommendations:	1. Training for records management staff on Transitory Records is recommended; 2. Departmental policy on the destruction of Transitory Records

	should be incorporated into all other policies dealing with the management of records, i.e. e-mail policy; 3. A methodology for identifying Transitory Records in the Department should be developed; 4. Examples of Transitory Records should be developed for distribution to staff as examples and as teaching tools for in-house training for new staff; 5. Help from NA or qualified consultants should be sought to review any training material, desktop documentation, to ensure that the concepts of Transitory Records are clearly outlined before random destruction of work files takes place.

5.2.2 Access to Information and Privacy Acts

Summary: Mostly Compliant:

Areas of Compliance:

- Excellent, recent policy on the application of Access to Information and Policy Acts;
- Recent policy on Printing and Procedures;
- Staff are cognizant of the importance of application of security rules regarding access;
- Personal information files are protected;
- Retention periods are in place;
- Records are deposited to NA according to the agreed Disposition Plan (where NA is responsible for applying the ATIP legislation);
- Official records are labeled according to security policy specifications; and
- The Department responded to 129 access requests before December 2001. This is a substantial increase from previous years, when requests averaged only 45 per year. In spite of the increased work load the Department is managing to respond to requests under the Acts.

Areas in Need of Improvement:

- Most responses under the Acts are not meeting the 30 day turnaround time requirement. Extensions are necessary of between 30 to 120 days.

Cause(s):	1. Keeping records in a paper medium contributes to a longer time frame of searching for relevant records, collating the records, and preparing relevant information for an ATIP request; 2. There are a number of additional causes that contribute to the difficulties of presenting a response to an ATIP request, however, the objective and scope of this Audit deals only with information management issues and not with the full range of issues that affect effectiveness of the ATIP mandate.
Potential Risks:	1. During the transition period, from paper to electronic, the Department will be challenged to maintain a good handle on

	linked records across varied media for presentation to an ATIP request, possibly adding time to the processes in the ATIP function.
Recommendation:	1. The Department should consider conducting a review to identify all causes for the difficulties in meeting the 30 day-turnaround time for processing ATIP requests and prepare an action plan to deal with the difficulties.
Note:	1. Implementation of recommendations for better management of records expressed in this Audit Report should help shorten the time used to search for records.

- Access to Information requests are difficult to apply to records at the desktop.

Cause(s):	1. Electronic e-mail is not under the control of records management rules or best practices; and 2. There is no linkage between paper and electronic records.
Potential Risks:	1. Locating all relevant records to an ATIP request is complicated by the high volume of business records that are held in e-mail treads. The Department is vulnerable in missing relevant records simply because staff have no control over their desktop records; 2. Since there is no linkage between paper and electronic records it is possible to miss records that are covered under a request. 3. Both situations create an environment where un-disclosure of unaccounted for information objects could potentially be interpreted by the requestor as intentional refusal to provide the requested information. Further, any disclosure of ineffective records management as a reason for the lack of disclosure of a particular information object, could be used by opposition parties in the House of Commons and by the media to discredit or embarrass the Minister.
Note:	1. Implementation of recommended information management policies and standard operating procedures outlined in this Audit Report should help to minimize the risks outlined here.

5.2.3 Canada Evidence Act

Summary: Mostly Non-Compliant

Areas of Compliance:

- Official records are managed under an existing records management policy and their organization allows for the identification of the lifecycle of records, including profiles of records such as author, date of creation, classification status, indexing number etc. Records are filed in file folders that document the audit trail of who had access to records and when;
- The Department met NA criteria for the identification of systems and their description in order to grant the Department a Disposition Authority.

Areas in Need of Improvement:

- The Department does not follow any IM standards or best practices models to ensure that work process are documented to established evidence of how the organization creates records, maintains system administration security (documentation of work processes of how the Department creates user groups), and how the Department accounts for audit trails, who had access to what record and when, what is the normal business process for using records;

Cause(s):	1. Records Management staff require training to better understand their role, responsibility and new challenges of electronic records as part of Information Management.
Potential Risks:	1. Without documentation of work processes and responsibilities, department business lines work in silos, often duplicating work being done in other areas of the same department. Such practices often come to light only when an external source of criticism reveals the waste of resources or discrepancies in departmental documentation dealing with a similar subject; 2. The Department may at some date be called to justify a business decision, a work process or handling of information under the Canada Evidence Act. The Department therefore must be ready to disclose how it manages and controls its resources, its information, systems and work practices and processes; 3. The Department may at some time be called to prove the authenticity and integrity of its records as presented to the court; 4. Without a mapping of areas of expertise, there is no knowledge sharing; 5. Records managers cannot contribute to design and evolution of IM standards and practices and mold the corporate IM view if they don't understand the legal requirements for records, in all media, to be admissible in the court of law.
Recommendations:	1. The Department should consider a development of a plan to implement documentation of systems, work processes, policies

	and standard operating procedures to protect the organization should its business practices be subjected to criticism, accusations in the media or challenged in the court of law; 2. Records Management personnel should be given opportunities to attend conferences such as the Association of Records Managers and Administrators (ARMA) and/or Association of Image and Information Management International (AIIM) and other information management conferences as part of their training and development; 3. The Department should invest in a corporate membership in organizations such as ARMA or AIIM to receive excellent material on legal requirements and best practices in records management; 4. The Department should consider obtaining or purchasing current standards on IM, such as the new Records Management standard from ISO and content management documentation from such organizations as Doculabs. 5. The Department should consider seeking help from National Archives of Canada or hire qualified consultants to train staff in documenting Departmental work processes and systems according to the general guidelines outlined in Part IV of the Canadian Standards Board's Microfilm and Electronic Images as Documentary Evidence (Can/CGSB-72.11-93).

- Screen captures of the Web Pages are not maintained to ensure that there is a record of the type of information that was made available to the public and when it was available;

Cause(s):	1. The legal issues with maintenance of Web Pages is still very new and very much still undefined.
Potential Risks:	1. Few organizations have considered the necessity of capturing an audit trail of the information that was offered on their Web Pages. However, protection from legal class action suits for dispensing "misinformation" or "inaccuracies" etc. is as relevant for Web pages as it is for any other government publication.
Recommendations:	1. "Screen captures" of the Departmental Web Pages, with date stamps, is highly recommended. (To have proof what was on the Web at any time)

- Paper records created in a mixed media environment are often orphaned records. Orphaned records are records which are not linked to relevant information in other records of the same medium or records in other media, and which are not presented in context of their creation.

Cause(s):	1. The lack of links between records occurs when all records in all media are not classified by the same classification schema or when no cross-indexation is done between disparate classification systems.
Potential Risks:	1. Orphaned records can be misinterpreted and misrepresented in the court of law to the disadvantage of the institution that created/issued the records; 2. The lack of links between records is not missed until an ATIP request or other business need identifies "incompleteness" in a collection of known records.
Recommendations:	1. A classification system for all media records should be developed; 2. Staff should be made aware of the consequences of allowing the existence of "orphaned' records.

5.2.4 Canadian Copyright Act

Summary: Fully Compliant

- Areas of Compliance:
- Material published to the Web and publications in the paper medium are found to give credit to the author and Department. The Departmental Internet Web page posts a notice asking all users to abide by the rules of the Canadian Copyright Act and credit the author and Department when using government information.

5.2.5 Emergency Preparedness Act and the Emergencies Act

Summary: Fully Compliant

- Essential Records are identified and managed according to the rules set out in the legislation.

5.2.6 National Library Act

Summary: Fully Compliant

Areas of Compliance:

- Excess books and publication are submitted to the National Library according to the provisions of the Act;
- Plans for the transfer of electronic versions of publications to the National Library are in place;
- All materials published by the Department are easily accessible to decision makers and are available to the public on the Web page; and
- Grey literature is maintained in the Departmental library.

5.2.7 Official Languages Act

Summary: Fully Compliant

Areas of Compliance:

- There is visible respect by staff for the two official languages of Canada, English and French;
- Staff are capable of communicating and working using records in the official language of their choice; and
- Both official languages receive the same treatment.

5.2.8 Privacy Act and Regulations

Summary: Fully Compliant

Areas of Compliance:

- Personal Information Banks identified in the TBS InfoSource;
- Personal information is accessible by those with a need and right to know, according to defined rules set in legislation; and
- Retention period of at least two years after last use is applied to personal records".

5.3 Compliance to Policies related to MGIH

5.3.1 Strategic Direction for Government Information Management

Summary: Fully Compliant

Areas of Compliance:

- Technology is managed as a corporate resource;
- Information in databases is managed as a corporate resource; and
- There is a plan and intent to manage all electronic information objects as a corporate resource.

5.3.2 Disseminating Electronic Information Practical Guide on Databases for Management

Summary: Fully Compliant

Areas of Compliance:

- Integrated Justice Information Secretariat heads Steering Committee on an integration plan of linking key systems such as the Case Analysis Tracking System, and the Forensic Identification Section Computer Administration System. Interface development is underway to link the National Crime Data Bank, the Canadian Firearms Registration System, the Violent Crime Linkage Analysis system, and the Automated Finger print Identification System. This collaboration is inter and intra-departmental in scope. Therefore, all partners in the judicial system of the government will share information.

5.3.3 Enhancing Services Through the Innovative Use of Information and Technology

Summary: Mostly Compliant

Areas of Compliance:

- There are plans to migrate from a paper-based system for official records to an electronic system that will comply with legislation and policies governing Information Management. Plans for managing electronic records are not complete, but they will include the use of ccmMercury and iRIMS for the management of all records.

Areas Needing Improvement:

- There is no evidence that a formal functional requirements study has been conducted to establish what type of technology would best serve the business of the Department;

Cause(s):	1. The current systems were purchased for use by the records management staff only. There was no need to do a full Department-wide functional requirements study; 2. Up-grading of the records management software RIMS resulted in the current iRIMS. Up-grading of the Ministerial correspondence tracking system DOMUS, resulted in the current version called ccmMercury. The new versions of both systems were integrated at the Department with the hope that the integrated system will manage electronic records as well as paper records. The decision to integrate the systems already in place was also based on the best economy for an interim decision.
Potential Risks:	1. The current integrated system may not meet client expectations; 2. The current system is not expected to satisfy all requirements for the management of e-mail; 3. Additional costs may need to be expended to fill functionality not offered by the current system, e.g. version control, audit trail, report generation, content management etc.
Recommendations:	1. Integrated Justice has hired a consultant to do a study of the best methods of organizing information and search and retrieval. Findings of that research should be used to evaluate the functional requirements identified and testing these against the current system; 2. Should the current system not meet the required functional requirements, evaluation of other options, including the recently revised RDIMS package backed by Treasury Board Secretariat, should be undertaken by the Department.

5.3.4 Government Security Policy

Summary: The scope of this audit did not include a review of security as an audit of the Department's compliance to the Government's Security Policy was conducted in October 2000.

5.3.5 Access to Information Policy and Privacy Policy

Summary: Fully Compliant

Areas of Compliance:

Access Register and Index to Personal Information is maintained.

5.3.6 Forward to MGIH

(Requires the planning, direction and control of all government information as a corporate resource.)

Summary: Mostly Compliant

Areas of Compliance:

- Corporate records in the paper medium and electronic records in databases are maintained as corporate resources; and
- There are plans to migrate to electronic based systems and taking control of electronic information at the desktop.

Areas in Need of Improvement:

- Lack of a comprehensive e-mail Policy. (Current documentation, referencing the use of e-mail and direction for printing of records, needs to be either expanded, or a new stand-alone e-mail policy should be issued);

Cause(s):	1. The current e-mail policy consists of several directives found in different documents and located for access in different locations of the Department.
Potential Risks:	1. Staff may not be aware of all the different rules governing the management of records under the Departmental e-mail policy; 2. Staff may not know how to write e-mails so that they can be easily classified, filed and found; 3. Staff may not know who is responsible for filing e-mail, the writer or the receiver; 4. Staff may not know how to treat an e-mail tread and how to attach attachments for classification purposes.
Recommendations:	1. E-mail directives need to be consolidated into one document; 2. The e-mail directive needs to be more comprehensive and written in a clear concise style; 3. Standard operating procedures for handling e-mail for capture as

	Corporate Record, keeping as convenience copy or disposal need to be provided to staff and made available at the desk top.

- Lack of classification system that would be easy for users to use at the desktop;

Cause(s):	1. Classification of records is still mostly done by the records management staff; 2. Electronic records at the desktop are not being classified.
Potential Risks:	1. Current classification system may not be suitable for electronic records, or may not be acceptable to staff who will need to use it for electronic records; 2. Development of functional classification systems takes a long time, due to the need of consensus from all business lines; 3. Without an adequate, tested classification system no technology is capable of solving the major issues associated with managing electronic records.
Recommendations:	1. An analysis needs to be conducted to identify what type of classification system is effective and can be implemented with the least possible resistance from staff that will need to apply it to electronic records.

- Excessive records on the system clog up the servers. There are also issues with finding the right information when too much information exists. Security controls, and application of ATIP is also difficult to apply in systems that are over flowing with surplus information.

Cause(s):	1. Lack of plan on how to teach/introduce the concepts of the Transitory Records Authority to ensure that records that can be destroyed are destroyed.
Potential Risks:	1. When servers get full, back-end clean-up means deletion of data on the servers; 2. Difficulties in applying ATIP; 3. Compliance to National Archives of Canada Act is at risk.
Recommendations:	1. Records management staff must learn the legal concept of Transitory Records; 2. Policies and standard operating procedures related to Transitory Records must be written and made available to staff; 3. Examples of Departmental Transitory Records should be made available as illustrative help.

5.3.7 Government of Canada Internet Guide 3rd Edition

Summary: Work in Progress towards Compliance

Areas of Compliance:

- Information published on the current Departmental Web page is mostly published information, which exists in other media as well; and
- Plans for the transfer of electronic versions of publications to the National Library are in place.

Areas in Need of Improvement:

- Official publications, including publications to the Web, must be deposited with the National Library, regardless of their media or if they were published on the Web. This could become an issue once publishing to the Web increases. Transfer of electronic records to the National Library has not begun.

Cause(s):	1. There is no policy or direction to ensure that all staff in the Department are aware that there is a requirement to deposit to the National Library copies of any published documents to the Web.
Potential Risks:	1. Currently all documents found on the current Internet Web Page are treated as a "copy" yet no policy exists to identify them as such. 2. Staff supplying documents for posting to the Web pages need to understand the difference between a "publication" and a copy of a "record".
Recommendations:	1. A policy for managing content on Web Pages needs to be developed. 2. Terminology used for records and published material needs to be standardized.

5.3.8 Managing Internet and Intranet Information for Long Term Access and Accountability, Implementation Guide

Summary: Mostly in Compliance, Work in Progress

Areas of Compliance:

- Meetings are being held to discuss and plan how a new Website will be designed and managed.

5.3.9 Common Look and Feel for Internet

Summary: Mostly Compliant, Work in Progress

Areas of Compliance:

- There is a plan to implement the Common Look and Feel in time for the December 2002 deadline.

5.3.10 Government – on – Line (GOL)

(The Department has two Web pages. One is the Departmental Web page, and the other is a shared Public Safety Portal Website.)

Summary: Partial Compliance, Departmental Web page Work in Progress towards Compliance.
Portal Website Work in Progress towards Compliance

Areas of Compliance:

Departmental Web Page:

- General information about the business of the Department is provided on the Web Page for accountability to the Canadian public; and
- Unlike other government departments, the Department will not use its Web Page to provide interactive services to the public. Therefore, the Department is under less pressure to get ready for GOL by the due date of January 2004.

Public Safety Portal Website:

- The Deputy Solicitor General is a champion of a government-wide GOL initiative for the Public Safety Cluster Portal. The Public Safety Portal currently involves 11 partner federal departments and the 4 Portfolio Agencies. The portal will be dedicated to public safety information (i.e. anthrax, terrorism, boating safety, recalls etc.);
- Departmental representatives participate in GOL Conferences and GOL planning;
- The Public safety Portal has been identified by the Department as the key service for Canadians. It is on track for its phased-in launch dates prior to 2004;
- Focus group sessions have been conducted in order to obtain user input into the design of the Website;
- Common Look and Feel will be incorporated into the design;
- There are plans for implementing lifecycle management and content management into the Website; and
- There is a plan in place to test and evaluate user experience once the Website is developed.

Areas in Need of Improvement:

- Better Management of Departmental Web Page;

Cause(s):	1. Departmental Web Page is not a priority because the Department does not provide any interactive services to the public; 2. The Public Safety Portal Website is considered to reflect the Department's commitment to public service.
Potential Risks:	1. Few organizations have considered the necessity of capturing an audit trail of the information that was offered on their Web Pages. However, protection from legal class action suits for dispensing "misinformation" or "inaccuracies" etc. is as relevant for Web Pages as it is for any other government publication. 2. Staff supplying documents for posting to the Web Page need to understand the difference between a "publication" and a copy of a "record" if they are to meet disposition requirements under relative legislation.
Recommendations:	1. Lifecycle management needs introduction; 2. Content management needs introduction; 3. Screen captures, with time stamps of Web Pages should be considered; 4. Policy to identify what records will be systematically placed on the Web.

6 ANALYSIS OF ADDITIONAL FINDINGS DURING THE AUDIT

The Preliminary Audit findings point overwhelmingly to the excellent control over paper records and to the security adherence in the Department. Further research and analysis however show that the Department has not developed a Corporate View for its Information Management Program. Common corporate functional requirements have not been developed and Branches are working, planning, and implementing information management projects in isolation or with other departments, but not with their own Departmental colleagues. There is a lack of strategies for managing electronic information holdings at the desktop. A review of desktop practices, as described by staff attending the Focus Group Session, indicates that staff have a hard time following the current rules, which are simple in comparison to those that need to be in place in the future. The Departmental culture is not ready to embrace the responsibility of adding profiles/metadata descriptors to individual records for their automated retrieval. Nor is the Department equipped with adequate policies, guidelines and standard operating procedures that apply to the management of electronic records to help staff deal with processes of record review, evaluation, classification, filing and disposal.

The Focus Group Session participants where able to describe actual work practices that help the organization function better. For example, staff at Integrated Justice follow a policy where participants of meetings, conferences or special events are required to report in writing on the nature, purpose and outcome of the meeting, conference etc. Other staff members have developed their own type of classification system to help them organize electronic records at the desktop. By sharing such knowledge and experiences, staff from different Directorates and

Divisions, learn the In-house Best Practices, which have the highest level of success and lowest level of risk when implemented corporately.

7 CONCLUSION

The Department is faced with the same issues and problems surrounding the handling of electronic information as most other federal government departments. There is strong desire on the part of Departmental staff to embark on a technology lead solution to address the issues of finding and managing corporate records. However, staff want a solution that will not require them to do "records management" work. Our findings indicate that the Department has a great deal of preparatory work that needs to be done before investment in technology can have a return on its value. Most rules that exist in connection to MGIH do not depend on technology solutions. Good Information Management Practice, which includes policies and standard operating procedures, as practiced in the public and private sectors—internationally and in Canada—depend on a planned approach in converting from a paper based environment to an electronic environment. The approach must ensure respect for existing norms and established culture, while at the same time transferring practices into sustainable rules and practices, which will endure regardless of the technology changes in the future. As a start, our recommendation is for the Department to develop a long term IM strategy that will incorporate cultural change, knowledge transfer practices and best desktop processes that can be transferred into usage when technology is employed for managing electronic records.

APPENDIX A

Persons Interviewed in the Audit:

Debi Cuerrier, Director, Administration Division, Corporate Services Directorate
George Holmes, Records Management Clerk, Ministerial Correspondence Unit, Corporate Services Directorate
Gerry Leger, Director, Systems Division, Corporate Services Directorate
Dan Lemieux, Records Systems and Operations, Corporate Service Directorate
Heather Moore, Chief, Ministry Library and Reference Centre, Corporate Services Directorate
Am Peca, Scheduling and Records Improvement Officer, Corporate Services Directorate
Eva Plunkett, Director General, Corporate Services Directorate
Duncan Roberts, ATIP Co-Coordinator, Access to Information Unit, Strategic Operations Directorate
Karen Savoie, GOL Project Manager, Corporate Services Directorate
Duane Wilson, Review Officer, Corporate Services Directorate

Focus Group Participants:

Anne-Marie Doupagne, Head, Ministerial Correspondence Unit, Corporate Services Directorate
Kimberly Fever, Senior Policy Analyst, Corrections Directorate
Nicole Lafleur, Administrative Assistant to Executive Director, Integrated Justice Information Secretariat
Am Peca, Scheduling and Records Improvement Officer, Corporate Services Directorate
Diane Thompson, Administrative Assistant to DG, Corrections Directorate
Eleanor Willing, Senior Marketing and Communications Advisor, Integrated Justice Information Secretariat
Duane Wilson, Review officer, Corporate Services Directorate