IMPLEMENTING INVESTIGATION REPORT F15-03

RECOMMENDATIONS TO THE GOVERNMENT OF BRITISH COLUMBIA

David Loukidelis QC

December 2015

INTRODUCTION

This report flows from Information and Privacy Commissioner Elizabeth Denham's Investigation Report F15-03, which she issued on October 22, 2015.[1] The investigation report makes findings respecting three complaints about the processing of access requests under the *Freedom of Information and Protection of Privacy Act* (FIPPA). It also makes 11 recommendations to government on matters connected with the complaints.

Government has a significant opportunity to take meaningful action to address the deficiencies that Commissioner Denham has identified. This report addresses Commissioner Denham's recommendations and makes specific recommendations to government for reform and improvement across a range of issues that need to be addressed. These recommendations are not a panacea, but they can effect real change. I therefore strongly urge government to act on my recommendations and to do so as promptly as possible.

In addition, I urge government, as it moves forward with implementation of the *Information Management Act*, to seize the opportunity to ensure that sufficient resources are devoted in the medium term to implementation of that law, and in the long term to sound information management program and practices. This report is about freedom of information, but other critically-important public interest objectives can only be realized through modern, effective, records and information management. An underlying theme of this report is that without sound and well-resourced information management—and without executive-level commitment to information management—government cannot properly discharge its overall functions or its FIPPA duties.[2]

---

[1] 2015 BCIPC 63, [2015] BCIPCD No 63 [investigation report]. https://www.oipc.bc.ca/investigation-reports/1874. The report is entitled "Access Denied: Record Retention Practices of the Government of British Columbia". It is worth noting here in passing that, although the title refers to practices "of the Government of British Columbia", the report deals only with three specific complaint investigations, with three executive branch offices in particular being under scrutiny. As Commissioner Denham said in her introduction, at page 3: "This investigation deals with three access to information requests where political staff in two government ministries and the Premier's office failed to fulfill their duties as set out in s. 6(1) of the *Freedom of Information and Protection of Privacy Act*". This by no means undercuts the force of her recommendations, but it is noteworthy, in order to fully understand the context for the recommendations made here, that the investigation report makes findings about three cases involving political staff in three offices, not findings about the behaviour of public servants across the province.

[2] This report uses the terms information management and records management, and sometimes refers to records and information management. Nothing turns on this for present purposes.

SCOPE OF THIS REPORT

Soon after Commissioner Denham's report was released, the provincial government announced that it would retain me to provide advice on how to respond to her recommendations. The scope of this report is driven by its terms of reference and by Commissioner Denham's recommendations. The terms of reference were released on November 2, 2015 by the Honourable Amrik Virk, the Minister of Technology, Innovation and Citizens' Services (Ministry). These are the operative portions:

> 1. Advice to Government in relation to the records management findings and recommendations found in the Report, including advice on any policies, procedures, structures and/or technical measures that Government could implement to ensure compliance with records management requirements. That advice will include recommendations and guidance concerning the types of records that need not be retained under applicable records management requirements. The advice will also include any FOIPPA requirements to retain records.
>
> 2. The provision of training to Ministers and staff in their offices, including the Premier's office, and advice on records management training to be carried-out across the public service.
>
> 3. Recommendations concerning the establishment of an ongoing practice review process to ensure records management processes across Government are improved over time.
>
> 4. Any additional recommendations or advice to government he deems appropriate in light of the Report's findings and recommendations.

The terms of reference indicated December 15, 2015 as the date for completion of this report.

These are Commissioner Denham's recommendations:

1. The Ministry of Transportation and Infrastructure should release the 36 pages of records initially identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on November 19, 2014 for: "… all government records that make reference to the issue of missing women along Highway 16/the Highway of Tears and specifically including records related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."

2. Government should develop a policy for all future data migrations that requires at a minimum: 1. Hourly, daily and monthly backup of data; 2. Written directions to government's

service provider with respect to these backups; and 3. Government monitoring of the directions to ensure their compliance.

3. The Ministry of Advanced Education should release the approximately 20 email records identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on July 21, 2014 for: "Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014." The Investigations and Forensics Unit will retrieve the emails and provide them to the Ministry.

4. The Executive Branch of the Premier's office should change its access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.

5. Government should clarify access requests with applicants where necessary to ensure it does not interpret the request too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request.

6. Government should create clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request. This guidance should be incorporated into government's access to information training and should specifically include that employees should conduct searches from their desktop or laptop and not from mobile devices.

7. Government should provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records. This training should describe employees' responsibilities for records management and provide the basis for understanding an office's record keeping system.

8. Government should legislate independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met.

9. Government should configure the settings in Microsoft Outlook to prevent employees from removing items from the Recover Deleted Items folder.

10. Government should configure the settings in Microsoft Outlook so that it preserves items in the Recover Deleted Items folder for just over one month. This would ensure all government emails are captured in monthly backups.

11. Government should create a legislative duty to document within FIPPA as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its key decisions and actions.

Recommendations 1 and 3 relate to access requests made to, respectively, the Ministry of Transportation and Infrastructure (MOTI) and the Ministry of Advanced Education (AVED). They were outstanding at the time of the report's release. The central agency responsible for provincial government processing of freedom of information requests, the Ministry's Information Access Operations (IAO), has advised that responses to both of these requests have been provided to the applicants.

Recommendations 2, 9 and 10 deal with information technology matters for which the Ministry is responsible. Recommendations 9 and 10 are discussed later. Recommendation 2, dealing with data migration, can be dealt with here. As the investigation report indicates, the failure to perform monthly backups during the data migration in question stemmed from the fact that the migration took much longer than planned. Commissioner Denham recommended that government devise a policy for future migrations and ensure it is properly implemented. No discussion of this is necessary in this report. It is recommended that government devise such a plan and implement it, with appropriate monitoring, during each data migration.

In an October 22, 2015 letter, Minister Virk wrote to the Special Committee to Review the Freedom of Information and Protection of Privacy Act (Special Committee) and asked it to consider recommendations 8 and 11, on the basis they would require legislative amendments. These recommendations are addressed later in this report. Minister Virk also asked the Committee to consider "the idea that deleted electronic records remain available for response to access requests." This appears to flow from the discussion in Commissioner Denham's report about whether a search has to be made for deleted emails that exist in backup only. This report also considers the issue of deleted emails in backup storage.

This report also addresses recommendations 4 through 7 and other aspects of the investigation report that, in my view, merit consideration and specific advice to government. Recommendations 5 and 6 deal with access to information request processing, calling for guidance and training on interpreting requests and searching for responsive records. Recommendation 4 addresses the processing of access requests in the Premier's office, while

recommendation 7 raises issues relating to records management policy and practice. These are each considered later.

Work on this report began immediately after the terms of reference were issued, with the following broadly summarizing the major steps taken:

- Analysis of the Commissioner's recommendations and assessment of which of them require or merit specific advice or recommendations
- Assessment of the existing processes in minister's office and the Premier's office for processing access requests
- Review and assessment of existing FIPPA training for provincial government employees, as well as training for political staff in ministers' offices and in the Premier's office. This involved assessment of training materials, frequency of training and training methods
- Review and assessment of existing records and information management training for provincial government employees, as well as training for political staff. This also involved assessment of training materials, frequency of training and training methods
- Research into best practices in records and information law, policy and practice in relation to how transitory records are defined and managed in the context of electronic communications media, notably email.

REPORT CONTEXT

Over the last half-century democracies around the world have enacted freedom of information laws to foster openness and accountability. These laws give individuals, communities, advocacy groups, media, businesses and others rights of access to government information. The legislative goal is to enhance political debate and action, help media hold governments and public institutions to account, foster greater participation in public life, enrich political discourse and action, and directly hold governments and institutions to account. These objectives are expressly recognized in FIPPA, one of the stated purposes of which is to "make public bodies more accountable to the public" by "giving the public a right of access to records".[3] These objectives, and the rights of access, to a degree overlap with the objectives of records and information management.

As the investigation report acknowledges, while information management and freedom of information share common ground, they are not the same thing. Good information management rules and practices can foster and support openness and accountability through freedom of

[3] Sections 2(1) and s. 2(1)(a).

information laws, but freedom of information is not—and should not be—the sole aim of records and information management. Put another way, while good records management laws and practices can enhance the functioning of freedom of information laws, that is not, and should not be, the sole objective of records and information management.

Records and information management laws, policies and practices also serve a variety of other important public interest objectives. These include ensuring that the administration of public affairs is in accordance with the law, enhancing the quality and efficiency of public administration, supporting prudent operation of institutions, protecting the legal interests of institutions and the legal rights of citizens, and preserving the historical record. While accountability, an objective of freedom of information, is linked with many of these public interest objectives, accountability does not exhaust the public interest in good records and information management.

It is also important to recall that accountability is achieved through means other than freedom of information laws alone. Political debate and action are key to accountability. Accountability through the justice system is vitally important. The media hold public institutions to account. Information is critical for each of these, but information does not flow only from freedom of information mechanisms. Statutory reporting requirements, legal obligations to produce information for litigation, requests for information by elected officials and many other well-established mechanisms—some statutory, some constitutional, some by convention—ensure that information is available. These mechanisms also depend on sound records and information management laws, policies and practices, but the accountability goals they serve are no more the only reason for good records and information management than is freedom of information.

A major challenge to the efficacy of both freedom of information laws and records and information management flows from the fact that public institutions everywhere are increasingly digitized. As Commissioner Denham observes, the "retention and accessibility of records has been complicated by the adoption of new communications technologies [and] the volume and variability of records."[4] The records management and archival implications of modern electronic communications media are indeed daunting. It is difficult to understate the challenges such phenomena present for records and information management, and archives, in the electronic age.

The situation in British Columbia illustrates this. The provincial government's Office of the Chief Information Officer (OCIO) has advised that some 284,000,000 emails are received by the

[4] Report, p. 60.

provincial public service each year, with approximately 86,000,000 being sent each year. The storage space for received emails alone amounts to some 43 terabytes[5] of data annually, with roughly 13 terabytes being required to store sent emails. This is apart from the doubtless staggering volume of other electronic information and records created each year. This matters, obviously, because, if records cannot be found because they have not been properly managed and retained in electronic form, important public interest objectives will be harmed.[6] So will the public's rights of access to records.

At all costs, the provincial government should not entertain any notion that all electronic records must, regardless of their value, be retained. This would be completely contrary to modern records and information management principles. It would also be damaging to both public administration and, perversely, freedom of information and privacy. To suggest, as some have, that all information should be kept is akin to suggesting it is good household management for homeowners to never throw away rotten food, grocery lists, old newspapers, broken toys or worn-out clothes. No one keeps their garbage. Hoarding is not healthy.

It is the same with our personal electronic records. No one could seriously suggest that it makes sense for people to retain all spam or junk email that worms its way into their personal email inbox, or to keep all other emails they receive. Nor would it be sensible for people to keep each and every email they send.

This is true even if an individual engages in a transaction that generates records. Take the example of an individual who shops at an online store and arranges to pick up the television they buy at a bricks-and-mortar location. The order confirmation is emailed to them and they print it for pickup purposes. They cannot pick the television up within the allotted window, so they email the retailer to extend the time. The retailer responds. They then email the retailer about whether the television comes with an HDMI cable. The retailer responds. Once the television is picked up, the purchaser keeps the receipt for warranty purposes. This is surely the only documentation that truly matters.[7] It would make no sense to keep all of the emails back and forth, or the printed pickup notice.

This is equally true for governments. The public policy dimensions of the management of government records and information do not change this. Government should retain only that

[5] Each terabyte is 1,000 gigabytes.
[6] Of course, if records of action or decision cannot be found, public institutions will be at a loss to know why or what was done, with possibly profound implications for the other public interests mentioned earlier.
[7] And even this documentation would not have enduring value. Once the item is thrown out at the end of its life, there would be no reason to keep the receipt any longer, as it would cease to have value.

which has value, as appropriately defined in law or policy. This is the broadly-accepted premise of modern information and records management. Nonetheless, some observers have suggested in the wake of the investigation report that all emails should be kept. Others have instead suggested that all emails should be forwarded to records management staff for vetting, to decide which should be kept and which discarded.

The practical implications of these suggestions demonstrate why neither should be adopted. LexisNexis has estimated that, when printed, each email yields on average 1.5 pages.[8] Using the above averages of emails received and sent, each year there would be roughly 426,000,000 pages of received emails and some 129,000,000 pages of sent emails, for a total of roughly 555,000,000 pages of emails. No one would suggest that all emails should be printed, but this gives a sense of the order-of-magnitude implications of the suggestions that, contrary to prudent information management principles, all emails should be kept, or should be vetted by others for retention. The same would be true even if these estimates were reduced by one or even two orders of magnitude, to 55,000,000 pages or 5,500,000 pages.

The truth is, if government tried to vet all emails to identify those that should be kept, it would grind to a halt. The enormous volume to review would alone guarantee this. So would the fact that those vetting the emails would have no real understanding of the context for each email. As Commissioner Denham observed, "it is a record's content and context that determines whether a record is transitory, rather than its form."[9] Retention decisions would at best be immensely difficult to make at all, and often would be wrong. Material that should be kept would not be and material that should not be kept would be.

This would make proper management of government information an elusive goal. It would present serious risks for access to information. It would make it more difficult for government to efficiently, accurately and completely retrieve records and process access requests. There would also be real risks for privacy, since it would result in the inappropriately lengthy retention of too much personal information. It would expose personal information to inappropriate disclosure through data breaches (and possibly expose personal information to improper uses).

The plain truth is that there is no value in retaining records that have no value. As Commissioner Denham explicitly recognizes, "The routine destruction of transitory records is necessary to

[8] https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf (accessed November 30, 2015). LexisNexis acknowledges that the page estimates are averages and certainly not surgically precise.
[9] Report, p 49.

reduce the volume of government records and the cost of managing records."[10] The key, therefore, is to find a practical way in which identify the records that have value and then retain and manage them appropriately in proportion to their present and enduring value. This is already a significant enough challenge given the evolution of information technologies and the increasing volume of information.

Consistent with this, it is recommended in the strongest possible terms that government resist any notion that all emails should be kept indefinitely, or that they should all be vetted by archivists or records managers to decide which to keep indefinitely. The prudent approach is to ensure that government's transitory records policy is appropriate, understood by all, and properly implemented.

On this point, there has to be a degree of trust that our non-partisan professional public services will manage transitory records properly when told how to do so. Governments around the world do this. It is also the only practical way to do it. The investigation report makes no findings about the tens of thousands of public servants working across the province. With proper policy, adequate guidance and training, and ongoing executive leadership, government can properly manage transitory records.

This report therefore recommends improvements to government's transitory records policy. It also recommends records management training for all public servants and political staff. Training and guidance can enhance records management practices where they matter, on the front lines. It also recommends, as government implements the *Information Management Act*, that ongoing records management practice review and improvement processes be but in place.

ACKNOWLEDGMENTS

The co-operation of public servants in the Ministry of Technology, Information and Citizens' Services in providing information I considered necessary for this report is much appreciated.

In support of the perspectives expressed in this report about transitory records and records management, I obtained assistance from an expert in archives and records management, Rick Klumpenhouwer, a partner with Cenera Associates in Calgary.

Last, consistent with Commissioner Denham's practice, the final draft of this report was provided to Minister Virk in order to permit government to check it for factual accuracy. In addition, with

[10] Report, p 49.

government's permission, I provided the final draft of this report to Commissioner Denham for her comments. The views expressed in this report remain solely mine. Any errors or omissions are mine alone.

KEY ASPECTS OF THE ACT

To properly frame this report and recommendations, it is necessary to outline key portions of that law in order to properly contextualize the recommendations made in this report.

Records and the right of access

Recommendation 7 relates to records management training for provincial government employees, including training on transitory and non-transitory records, and the process for retaining and destroying records. This raises the question of what qualifies as a "record" for FIPPA purposes, as well as what is a transitory record under government policy.

The right of access to records is an individually-exercised right, but it is a public right, aimed at achieving FIPPA's goals of openness and accountability by "giving the public a right of access" to any "record" in the custody or under the control of a public body.[11] This is not a right of access to unrecorded information, as FIPPA's definition of the term "record" makes clear:

> "record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.[12]

This non-exhaustive definition requires that information be "recorded or stored" by some "means". It is beyond debate that electronic records, including emails existing only in electronic form, are records.[13] Information in an email or an email string is electronically recorded or stored and is thus a record.

[11] Section 2(1)(a).
[12] Schedule 1.
[13] It should be noted here that there can equally be no debate that information in the form of text messages, instant messages and other electronically-generated and electronically-stored communications are records under FIPPA.

Duty to assist

Both recommendations 5 and 6 deal with important aspects of the processing of access requests. When a public body receives a request for access to records, a number of procedural obligations are triggered. The default deadline for responding to a request is 30 business days, although this can be extended.[14] The public body must then respond in writing, giving reasons for any refusal to disclose information.[15] Between request and response lie a number of important steps and obligations, with pitfalls and traps along the way. Each of these can, if not managed with care, result in delays, incomplete or inaccurate responses, or all of these. Each step should be taken, each objective fulfilled, in light of the overarching duty to assist.

Access applicants have a responsibility to provide "sufficient detail" in the request "to enable an experienced employee of the public body, with a reasonable effort, to identify the records sought."[16] This encourages applicants to think carefully about their requests, and frame them as accurately and with as much detail as possible, since this can reduce the risk of delay, or of incomplete or inaccurate responses. Public bodies, however, have significant duties under s. 6(1). This provision, which features prominently in the investigation report, reads as follows:

> The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

The "head" of every public body is responsible for compliance with most of the obligations under FIPPA and also exercises the public body's powers, duties and functions. The "head" of a ministry is the minister, but the minister's duties and functions are invariably delegated. The minister's overall responsibility under FIPPA remains, and this is symbolically important in the case of the duty to assist, which has aspirational connotations in light of FIPPA's explicit statutory objectives of openness and accountability.[17]

The duty to assist has an overarching aspect, *i.e.*, the duty to "make every reasonable effort to assist applicants". Section 6(1) also requires public bodies to respond without delay, to respond openly, to respond accurately, and to respond completely. The duties to respond accurately and completely figure prominently in Commissioner Denham's recommendations. So does the over-arching duty to assist applicants. The implications of these duties are addressed later in this report.

---

[14] Section 7 and Schedule 1 (definition of "day").
[15] Section 8.
[16] Section 5(1). Section 10(1)(a) provides that, if sufficient detail is not provided, the public body can extend the response deadline by 30 business days.
[17] These are articulated in FIPPA's purpose statement, in s. 2(1).

Retention of records under FIPPA

The last aspect of FIPPA that warrants mention has to do with records retention. Recommendation 7 in the investigation report calls for training on records management and records retention. Records management and retention are driven by the provincial government's records management law and policy framework, not FIPPA, although FIPPA itself does contain one retention requirement. Specifically, under s. 31, if personal information is used by or on behalf of a public body to make a decision that directly affects an individual, that information has to be retained for at least one year after it is used. This is to give the affected individual a reasonable opportunity to obtain access to that information.[18]

Apart from this, FIPPA affects ordinary-course records management only incidentally: where a public body has received a request for access, records caught by the request cannot be disposed of without violating s. 6(1). This is what Commissioner Denham has found more likely than not occurred in one instance.[19]

The next section discusses the duty to assist in more detail and makes recommendations for improving the processing of access requests in ministerial offices and the Premier's office.

DUTY TO ASSIST APPLICANTS

The public's right of access to records depends on a conscientious approach to compliance in the spirit of the statutory objectives of openness and accountability. This is reflected in the foundational duty of public bodies to make every reasonable effort to assist applicants. Again, every public body has a duty to respond without delay, respond openly, respond accurately and respond completely. Commissioner Denham deals with two of these in the investigation report, the duties of accuracy and completeness, while implicitly touching on the duties to respond openly and without delay. These are vitally important for giving real meaning to the public's right of access to records.

[18] Section 31. Schedule 1 defines "personal information" as "recorded information about an identifiable individual", other than business contact information.

[19] There is no offence under FIPPA for wilfully disposing of records in an attempt to evade or frustrate an access request. Effective January 1, 2016, it will be an offence under Ontario's *Freedom of Information and Protection of Privacy Act* to "alter, conceal or destroy a record…with the intention of denying a right…to access the record or information contained in the record" (s. 61(1)(c.1)). This is discussed further below.

Before dealing with these, however, some general comments about the processing of access requests are in order. In 2009, responsibility for processing access requests shifted to a central model, and IAO was created. It is housed within the Ministry. IAO is responsible for the processing of requests, including assessing what information may or must be withheld, with the decision on what is released ultimately remaining with the client ministry. That decision is ordinarily made by the deputy minister (noting, as an aside, that for timeliness reasons it is extremely important that deputy ministers sign off on release packages as quickly as possible).

When IAO receives an access request, it issues a call for records to the ministry in question. The ministry is responsible for searching for responsive records. A minority of ministries have in-house staff dedicated to freedom of information matters, but most do not. If there is an in-house freedom of information co-ordinator, IAO sends the call for records to that person, who then manages the search for records. For other ministries, IAO staff have developed contacts within the ministry, sometimes in different program areas in the ministry. These contacts receive the call for records and manage the search. The degree to which IAO has contact with a ministry's program areas during the search phase varies; it is primarily dependent on the ease of interpretation of the request and the need to clarify the scope of the request. If IAO believes records should exist but have not been produced—perhaps based on past experience with similar requests to the ministry—it will follow up to ask the ministry to search further.

There is a lot to be said for the centralized processing model. IAO has undoubtedly developed considerable expertise in processing access requests. Its staff perform challenging analytical functions under time pressure. These demands, and IAO's expertise and experience, deserve recognition and support. The reality, however, is that IAO, as the central freedom of information service, depends on the efforts of ministry program staff, with whom it may have little or no direct contact, in searching for records. Whether this leads to inadequate search efforts cannot and need not be determined for the purposes of this report. It is important to underscore, however, that government needs to ensure that all ministries have the expert resources in-house that are necessary to ensure every reasonable effort is made to locate records in response to access requests. Government should, more specifically, ensure that staff receive guidance and training on searching for records. This is addressed later.

Duty to assist: searching for records

The importance of the duty to search for records has been recognized since the early days of FIPPA. Commissioner David Flaherty, in interpreting the meaning of "every reasonable effort" to search for records (and otherwise assist an applicant), adopted this definition from the government's policy manual of the day:

> Every reasonable effort is an effort which a fair and rational person would expect to be done or would find acceptable. The use of 'every' indicates that a public body's efforts are to be thorough and comprehensive and that it should explore all avenues…[20]

This test—which does not impose "a standard of perfection"[21]—has been applied many times in assessing whether the s. 6(1) duty to respond "completely" has been met.[22] A public body is expected to provide evidence—usually in the form of sworn affidavits—speaking to the extent and nature of its search efforts.[23] It has the burden of proving that its search efforts have been "thorough and comprehensive", such that a "fair and rational person" would conclude that the effort discharged the duty.

It is not possible to offer detailed prescriptions in this report as to how searches should be done. There are too many variables. The circumstances of each request naturally will drive search efforts, with the nature, complexity and size of a public body affecting where and how searches should be done. Other considerations include which media are used to keep information, *i.e.*, whether both paper and electronic media must be searched (with many public bodies having several kinds of electronic media, often with different formats and search capabilities).

It is, however, possible to say that some search methods are not sufficient. As the investigation report affirms, for example, it is clearly not sufficient for someone to find responsive emails by searching through smart phones or tablets for desktop email folder contents. Among other things, it is well known that these devices do not necessarily display all emails that exist in desktop folders or other storage. It also may not be sufficient to just scan the labels of desktop folders to see if any of them has a label suggesting it contains responsive records. As the investigation report indicates, the inbox, sent and deleted items folders should be searched. Comparable efforts should be made to find responsive records of other kinds, whether in electronic or other media. Again, precisely what should be done depends a great deal on the nature of the public body's holdings, how they are kept and organized, and so on.

---

[20] Cited in Order No. 30-1995, p. 6.
[21] Order 00-26, at p. 2.
[22] Numerous orders have at the same time acknowledged that this test "does not impose a standard of perfection". See Order 00-15, at p. 3, as an example.
[23] The need to document search efforts in order to demonstrate that they fulfilled the s. 6(1) duty to search attracted comment soon after FIPPA came into force. In Order No. 30-1995, Commissioner Flaherty expressed concern, at p. 6, that a ministry had "poorly documented" how it went about searching for records, adding that public bodies should "candidly describe all potential sources and its reasons [for] any decision not to explore one or more of them"., He added that "public bodies should automatically include a description of those [search] efforts, consisting of the hours expended, the manner of searching, and any other potential sources and the reason that they were not searched.

Nonetheless, existing government training materials on the duty to search were reviewed and it is clear there is room for considerable improvement in this area. Government should therefore improve its training materials, and guidance resources, to provide better education and support for front-line staff in this vital area. The materials and guidance should inform all staff about the policy objectives of the duty to assist, the test for search efforts expected of public bodies, and practical steps they can take to help meet the duty. Employees should be given guidance on typical steps for finding records, such as tips on how to search their email accounts.

These materials should also underscore the importance of documenting all steps taken to search for records, with specific guidance on what is expected in terms of documentation. Among other things, failure to document search efforts can put a public body at a loss if the matter is appealed to Commissioner Denham's Office. The public body has the burden to prove its efforts meet the standard, but if no records are kept, it will be at best hard-pressed to meet this burden.

In addition, IAO should continue to watch for cases where it has reason to believe records should exist, yet none are produced to it. In such instances, IAO should rapidly escalate the matter to obtain appropriate direction. This should ideally come from the deputy minister for the ministry involved (or her or his immediate delegate). Government should create policy to govern such cases.

Another aspect of the duty to assist in searching for records merits mention. There has been considerable public commentary in recent years about cases in which no responsive records have been found. IAO has advised that, in the case of ministers' offices and the Premier's office, this can be the case because these are not the offices of primary responsibility for records management purposes. Put another way, these offices are not charged with the retention and management of ministry records.

Where responsive records are in the ordinary course kept within the ministry, not a minister's office or the Premier's office, it is opaque to tell the requester only that there are "no responsive records" in the minister's or Premier's office.[24] This is counter-intuitive to many people. Many people may assume that the Premier's office, given its prominence and role in modern government, keeps every record about every matter government is ever involved in. Where an executive branch office does not have responsive records due to ordinary-course records management, IAO should explain this to requesters. It should explain that the ministry's records were searched and any responsive records are included in the release package. To simply say that no responsive records exist in one office, without explaining that they exist elsewhere and have

[24] Of course, there has been considerable debate about what some call an "oral culture" in government. The above discussion deals with cases where records have been created.

been found, only raises suspicion where none should exist.[25] IAO should therefore change how it responds in such cases. Government also should enhance public understanding by publishing information about how records management is handled as between ministries, ministers' offices and the Premier's office.

Duty to assist: interpreting access requests

The above test for whether the duty to assist has been fulfilled applies to all aspects of s. 6(1), as Commissioner Flaherty made clear from the outset. This means that, in seeking to respond accurately and completely, a public body has to interpret access requests in the manner that "a fair and rational person would expect".[26] While applicants have a duty to provide sufficient detail in their requests, a public body cannot proceed as if the burden is only on applicants.

As a first step, a public body faced with an unclear request should, consistent with its general duty to assist, seek to clarify it.[27] If a request cannot be clarified or narrowed, the public body remains duty-bound to make every effort to interpret the request properly and to respond in line with that interpretation. There is no duty to expand a request, but a good faith effort has to be made to discern the intent, the goal, of the requester. Semantic games have no place in the exercise. It is not proper to read down the language of a request. This is especially so where the request is made within a context that is reasonably apparent to the public body.[28] The overriding duty, after all, is to make "every reasonable effort to assist", to meet the standard of what a fair and rational person would expect.

One way to improve this situation is through better education. Government's existing training materials and guidance fall short in this area. They should be enhanced to bring home to all staff

[25] To be clear, this recommendation only applies where a ministerial office or the Premier's office has no records because, in the appropriate course of operations, they are instead housed with the ministry. Further, in such cases IAO should document why there are no records in these offices, *i.e.*, it should document the fact that the records are held by the ministry, not the minister, in the ordinary course.

[26] The narrowness of the public body's interpretation of the request was at issue in Order No. 30-155, where Commissioner Flaherty set out the test under s. 6(1). He therefore considered the test to apply to cases where a public body is alleged to have given a request an inappropriately narrow interpretation, and other cases follow this.

[27] This can have practical benefits for both the public body and applicant. Applicants often do not really know what they are looking for, or where to look. They may not understand how government works or how it is organized. They may have unrealistic expectations as to how much information government creates or retains, perhaps even assuming an all-knowingness on the part of government. Communicating with them can help narrow requests appropriately, or focus them on better targets. It may also be possible to answer their questions directly, thus avoiding the need to process the request at all.

[28] There may, for example, have been publicity or debate about a matter involving the public body that helps with interpretation.

the policy objectives of the duty to assist in interpreting requests and educate them on IAO's role in interpreting requests authoritatively.

IAO plays a central role in interpreting requests and processing them. Where IAO is working with ministry staff or staff in a minister's office, its considerable expertise should be respected. IAO therefore should continue to be vigilant in detecting cases where it believes public bodies may be interpreting requests narrowly, *i.e.*, not in accordance with their s. 6(1) obligations. In such cases, the IAO analyst should escalate the matter quickly internally, with senior IAO staff in turn consulting with the deputy minister for the ministry. IAO should then give direction to staff on the interpretation IAO considers appropriate. This will help IAO resist attempts to interpret requests more narrowly than their terms or context warrant. Government should create policy to support this recommendation.

Duty to assist: deleted emails and government backups

The investigation report touches on the duty to assist as it relates to searches for, and retrieval of, deleted emails. This subject has already been touched on, but it warrants further discussion.

Email backups and the duty to assist

Recommendation 10 suggests that government should reconfigure the recover deleted items email folders across government so their contents are retained for 31 days, not the current 14 days.[29] This is to ensure that all emails in this folder are caught by monthly backups. As the investigation report notes, however, the minimum retention of the monthly backups is 13 months, after which they are deleted.

Emails in the recover deleted items folder have been deleted on the basis that they need not be retained. As the investigation report shows, emails may be inappropriately deleted. They may also be accidentally deleted. Recommendation 10 appears to be aimed at ensuring that inappropriately or accidentally deleted emails are kept for 13 months in backup.

The investigation report acknowledges that backup storage exists for disaster recovery and business continuity purposes, as well as investigative purposes, not records management purposes. This is the accepted purpose of backups in both the public and private sectors:

> Business continuation or disaster recovery plans and programs, such as those employing backup systems, allow an organization to rebuild its electronic information systems and

[29] Report, p. 59.

> to continue operations despite a significant network failure. What must be stored in order to achieve this goal and the manner and length of storage time will generally be decided by an organization's information technology professionals (with substantive input from the other disciplines—operational, records management and legal) as the individuals who will be relied on to manage the recovery. Consideration should typically be given to making the storage time period as short as possible—only that amount of time that is truly necessary to recover from a disaster.
>
> There is general consensus that regardless of the various capabilities of different backup systems, those systems are designed for the purpose of business continuity and should not be used as a substitute for records management. While the backup systems can provide the capability to recover data when necessary, those capabilities are fundamentally different from what is required for information and records management. Moreover, after a relatively short period of time, it is simply impractical for backup systems to retrieve efficiently or effectively specific, targeted information....[30]

Soon after FIPPA came into force, Commissioner Flaherty observed that "[b]ackup systems for records like e-mail are designed and intended to re-establish a whole system of records in the event of a catastrophe, not for the recovery of an individual item that may be stored therein over a certain time frame."[31] He ruled that any deleted email which exists only in backup is no longer a "record" at all within the meaning of FIPPA.[32] He found that FIPPA did not require a ministry to create a record from backup,[33] although he referred to the possibility that a public body might in rare cases be required to create a record from backup, citing the possible example of police investigating a serious crime.[34]

Commissioner Flaherty reached this same conclusion in Order No. 121-1996 and Order No. 198-1997.[35] In the first, he affirmed that deleted email existing only in backup is not a record for FIPPA purposes, and there is no duty under "normal circumstances" to create a record from backup.[36] He underscored that, "unless a particular e-mail system in fact makes it relatively easy

---

[30] L. Wagner, ed., *The Sedona Guidelines: Best Practice Guidelines &Commentary for Managing Information & Records in the Electronic Age*, 2d ed, Sedona Conference, 2007, at p 20 (citations omitted).
[31] Order No. 73-1995, at p. 7.
[32] *Ibid.*, p 5.
[33] The issue before him was whether a public body is obliged under s. 6(2), not s. 6(1), to "create a record" from backup, *i.e.,* to create a record that is then amenable to an access request under FIPPA.
[34] *Ibid.*, p. 7, where he referred to the possibility that cases involving "a serious issue of law enforcement, where the police are looking for evidence of a serious crime that might be retrieved from anywhere" could lead to a different outcome.
[35] https://www.oipc.bc.ca/orders/284. Essentially the same views were set out in Order 02-25: https://www.oipc.bc.ca/orders/710.
[36] Elsewhere in this decision he did refer to the s. 6(1) duty to assist in relation to emails in backup, but the issue before him had to do with s. 6(2).

to retrieve deleted records from a wastebasket or archived or backup tapes, then there is no obligation on a public body to make the effort".[37]

In Order No. 198-1997, Commissioner Flaherty commented on the evidence before him about whether a single specific email might exist in the backup of deleted emails. The applicant asserted that she had seen a copy of an email between two individuals, but both of those individuals swore affidavits saying that no such email had ever existed. Commissioner Flaherty accepted this evidence in concluding that this was not a case in which a search had to be done.

Commissioner Denham has, in the investigation report, clearly endorse Commissioner Flaherty's perspective, confirming that the duty to assist does not require government to search for and create emails that have been deleted and exist only in backup. As she puts it, "under ordinary circumstances, the duty to assist does not require" a search of email accounts or records backed up by the government's IT services provider.[38] This is because "[f]or a typical access request, retrieving backed up data is too costly and time-consuming an exercise to be considered reasonable."[39]

Both the investigation report and these earlier decisions are important because they hold that, other than in exceptional circumstances, government does not have to expend the considerable effort needed to search for and re-create records for FIPPA purposes.

Further, the investigation report elsewhere says that, unless there is a "reasonable belief" that the recover deleted items folder contains a responsive email, it need not be searched:

> …Emails that an employee has deleted from his or her Deleted Items folder and moved to the Recover Deleted Items folder are records that may be responsive to an access request. *However, it will only be necessary to do such a search of the Recover Deleted Items folder in instances where there is a reasonable belief that this folder may contain responsive records. The reason for this is that unlike the mailbox folders, there is no capacity within Microsoft Outlook to do an automated search of the Recover Deleted Items folder….*[40] [emphasis added]

---

[37] *Ibid.*, p. 10.
[38] Report, p. 16.
[39] Report, p. 16. The investigation report goes on to say, at p. 17, that, in "exceptional circumstances", an access applicant "may be able to overcome the presumption that a public body need not search the backup system where he or she can provide substantive evidence to demonstrate that responsive records likely exist there", although the applicant has to provide evidence that is "more than mere speculation". The report does not, understandably, elaborate on what exceptional circumstances might be, or what evidence would be needed to overcome the presumption.
[40] Report, p. 59.

Given this observation, recover deleted items folders will not in the vast majority of cases have to be searched, much less will the contents of these folders have to be reconstructed from backup.

Configuring email applications to prevent 'triple deletion'

Recommendation 9 in the investigation report is that government should configure the settings in Microsoft Outlook to prevent employees from removing items from the recover deleted items folder. This is intended to preclude the triple deleting of emails.

Other recommendations in this report will help improve the retention of emails that should not, in accordance with records management rules, be deleted. Another obvious measure for addressing triple deletion of emails is to create a rule prohibiting that practice, which government should do as soon as possible.[41]

Regarding Commissioner Denham's recommendation that email accounts be configured to prevent triple deletion, it is recommended that government work with Commissioner Denham and with Microsoft to ensure that all mailbox content, including deleted emails, is retained in backup for 13 months for the purposes of investigations and disaster recovery.

PROCESSING REQUESTS IN THE EXECUTIVE BRANCH

Ministers' Offices and Access Requests

Request processing procedures

IAO handles requests for records that may be found in ministers' offices. Each minister's office has a designated person who is responsible for the search for responsive records within the office. This person is tasked with ensuring that all staff in the office search for responsive records, in electronic or other form, and report the results to the designated person. The designated staff person gathers records and provides them to IAO. IAO reviews them to confirm whether they are responsive to the request. It then analyzes the records to determine which portions may or must be withheld under FIPPA access exceptions. IAO then provides recommendations to the

[41] This is recommended even though the investigation report makes no findings about the behaviour on this score of the many tens of thousands of professional public servants in the provincial government. It does not say that improper deletion of emails is encountered, must less widespread, in the public service. A rule of this nature is, nonetheless, warranted in order to help restore, and maintain, public confidence that emails that should be retained, because they are not transitory, are in fact being retained as appropriate.

delegated head of the ministry (again, this is usually the deputy minister). The delegate signs off, although sometimes further discussion or analysis occurs before sign-off.

As noted earlier, Commissioner Denham has found that MOTI interpreted the access request in issue too narrowly. This meant that responsive records were not produced that should have been. In relation to the request involving AVED, she has found that the chief of staff to the Minister did not conduct a proper search for emails.

It is beyond the scope of this report to determine whether other ministers' offices have also narrowly interpreted requests, much less whether the public service has done so. It is also outside of scope to determine whether inadequate searches, as occurred in the AVED case, occur elsewhere. These inquiries are not necessary in order to improve the processing of access requests within ministers' offices. The investigation report sufficiently illustrates the need to ensure that better guidance and training are provided to ministerial staff on their responsibilities in searching for records.

In addition, in order to improve public trust and confidence, government should change the process for handling access requests in ministers' offices as outlined below. This will have resource implications, but trust and confidence warrant this change, which should be maintained over at least the medium term.

IAO is staffed by career public servants who are at arm's-length from ministerial offices. IAO has significant expertise and experience in processing access requests. Ministerial office staff have not got the same degree of expertise and may not be employed in a given office long enough to be sufficiently familiar with the office's records holdings. In light of the above, therefore, government should adopt the following new procedures:

1. Each minister's office should be required to designate a permanent public servant as the person in charge of request processing within the office. The position of senior executive assistant is an example. The goal is to ensure that political staff involved in the day-to-day hurly-burly of political work are not in charge of searches for records.
2. Whenever IAO receives a request that requires the records of a ministerial office to be searched, the designated staff person in the minister's office should be responsible for contacting all staff directly, in writing (for example, by email), setting out the wording of the request and directing that staff search for responsive records and respond in a set time.
3. This should include clear direction on searching for records (and should underscore the duty to provide a complete and accurate response).

4. Each member of the minister's staff should be required to respond directly to the assigned staff member, reporting in writing on the search and sending responsive records directly to the assigned staff member, who will then send them to IAO.
5. If any member of a minister's staff has questions about the scope of a request, or about whether a record is responsive, those questions should be directed in writing to IAO. IAO should have the final say on how the request is to be interpreted and whether a record is responsive.
6. IAO should be required to report any failure by a ministerial staff member to respond or any failure to co-operate with IAO. This report should be made to the Premier's chief of staff and to the deputy minister for the ministry.
7. Each minister's office should be required to ensure that IAO at all times has a current list, with contact particulars, for all staff in the office.
8. IAO should be authorized to, where it considers it necessary in a given case or on an *ad hoc* basis, have access without notice to ministerial office files for the purpose of ensuring that all responsive records have been identified and produced to IAO. This includes the government email accounts, but not personal emails in them, of ministerial staff.
9. Rules will be needed to ensure there is no collection of constituency records of a minister (as opposed to ministerial records, *i.e.*, records of the ministry as a public body).

Training and guidance

The Premier's office has advised that all ministerial staff hired starting in 2013 have received access and privacy training, although this is not mandatory. Government should take the following measures to enhance training:

1. Training should be mandatory for all new ministerial staff. Each time someone is hired, that individual should be required, during orientation, to take access and privacy training.
2. The training should be done by IAO on an in-person basis, in groups if necessary.
3. Existing training materials should be significantly enhanced in the areas of the duty to assist and records management (notably regarding transitory records, discussed below).
4. As further described below, the materials should be designed to help ensure that staff understand and comply with the duty to assist. Another goal is to ensure appropriate practices in relation to transitory records. A third goal is to ensure a sufficient understanding of records management rules and practices. This is also important for the proper management of records other than emails.
5. Reference materials, or guidance, on all of these matters should be provided to ministerial staff for their reference.

6. Staff should be made aware of IAO's contact centre number, so they can reach out with any compliance questions.
7. The director of executive operations in the Premier's office should be responsible for ensuring that training is performed and for keeping records of this.
8. Ministerial staff should be required to take refresher training periodically, at least every two years.

Regarding the guidance materials for ministerial staff on interpreting requests and searching for records, new materials should be created to ensure that existing (and new) ministerial staff have a proper understanding of what is expected of them. This guidance material can align with the guidance material recommended below for public servants.

The guidance material should also make it clear to ministerial staff that the minister's office is part of the ministry as a public body and is not exempt from FIPPA. The guidance should address constituency records of the minister in her or his role as a member of the Legislative Assembly, since these are not generally considered to be ministry records for FIPPA purposes. This will help staff understand where the lines are drawn.

Last, the guidance should help staff understand that personal email accounts are not to be used for government business and, if they nonetheless are, that these records are not excluded from FIPPA and must be produced for request-processing purposes.

The recommendations for training for ministerial staff should also apply to staff in the Premier's office. On this point, as noted at the outset of this report, the terms of reference contemplate providing training to staff in both ministers' offices and the Premier's office as early as practicable in 2016. This should be done *after* the enhanced training materials are prepared, which should be done as soon as practicable.

A final recommendation is necessary here. Political staff who are employed in ministers' offices are appointed under the *Public Service Act*. This means they are subject to government policies on acceptable use of technology and on records management.[42] They are also subject to a code of conduct for political staff. They should be required to certify in writing that they are aware of their responsibilities under FIPPA, including regarding the duty to assist, and are aware of applicable records management policies and rules, particularly those relating to transitory records and also the prohibition against triple deletion of emails.

[42] A recommendation is made later to clarify records management policy on transitory records for all employees, including political staff.

Premier's Office and access requests

Commissioner Denham comments critically in the investigation report on the existing process in the Premier's office for responding to access requests. At the time of the investigation, the request handling process in that office was entirely verbal, and was conducted on a face to face basis or by phone, with only minimal (and not permanent) records kept of what was done to search for and produce responsive records. The Commissioner expressed the concern that this would result in responsive records not being found and in response delays.

Since the investigation report's release, the Premier's office (Executive Branch) has instituted a new process for responding to a call for records in response to an access request. Responsibility for managing access requests for the Premier's office (Executive Branch) no longer rests with political staff. A designated public service employee in the Deputy Minister's Office is now tasked with management of requests for the Executive Branch as well as the Deputy Minister's Office. Once a request is received, this person sends a call for records electronically to all staff. Responses and records are provided directly to the designated staff person in the Deputy Minister's Office. All communications relating to the call for records are retained, thus documenting the process. Once records have been retrieved and provided to the designated staff member, that person forwards them to IAO for processing.

Other branches of the Premier's office are the Premier's Correspondence Branch, Cabinet Operations and Intergovernmental Relations Secretariat. Each of these branches receives a call for records directly from IAO and has a staff member who is responsible for the management of requests and who responds directly to IAO. In each case the designated person is a public service employee.

In the case of the Intergovernmental Relations Secretariat, IAO notifies the designated staff person electronically of the call for records. This person in turn issues a call for records to staff. This person responds directly to IAO. Records are kept of the search process.

The same process is followed in Cabinet Operations. If the request is for Cabinet minutes or other Cabinet documents, the designated staff person is often able to personally locate, retrieve and send responsive records to IAO. If the request goes further than Cabinet documents, the staff person electronically issues the call for records to other staff, receives records and provides them to IAO. This process is also documented.

Last, correspondence in the Correspondence Branch is organized and filed using the provincial government's CLIFF electronic document application. This means the designated staff person in this branch is able to personally locate, retrieve and send to IAO any responsive correspondence.

Sign-off for all access request packages involving records within the Premier's office resides in the Deputy Minister's Office.

Consistent with the above recommendations respecting ministers' offices, this is the approach that would have been recommended had changes not already been made. The above recommendations about IAO authority and access to records in a minister's office should, in addition, be implemented in relation to the Premier's office. So should the recommendations about FIPPA and records management training for political staff in the Premier's office, and their agreement to be bound by records management rules.

The discussion so far has focussed on recommendations that aim to assist government with enhancing certain aspects of its freedom of information processes. The investigation report also raises two significant records and information management issues, and these are dealt with in the next section.

RECORDS & INFORMATION MANAGEMENT

Despite its brevity—it has only six sections— the *Document Disposal Act* is the foundation for the provincial government's management of records. It will be replaced by the *Information Management Act* next year, which is when the *Document Disposal Act* turns 80.

The *Document Disposal Act* requires records to be managed and retained according to records schedules approved by the Select Standing Committee of the Legislative Assembly on Public Accounts and Economic Affairs and then the Legislature. A record must be retained in accordance with any applicable schedule, and may only be disposed of when the schedule permits.[43] Records schedules approved under the *Document Disposal Act* therefore govern the retention and disposition of government records.

Part 12 of the provincial government's Core Policy and Procedures Manual delegates to the Chief Information Officer both responsibility and accountability for records and information management. These are stated objectives of the information management policy contained in the manual:

[43] Section 3(2)(c).

- Assign responsibility and accountability for the management of information within the custody, or under the control of, government.
- Assure compliance with legislation, policies and standards.
- Create and retain a full and accurate record documenting decisions and actions.
- Provide relevant information in a timely, useable, cost-effective, and accurate manner.
- Preserve government information in a manner that retains the information's authenticity, reliability, accessibility and integrity for as long as required.
- Support transparent and effective access to government information within legally established privacy and confidentiality restrictions.[44]

The manual also states the following policy:

> Government must appropriately provide access to, manage, preserve and dispose of its records in compliance with the *Document Disposal Act*, the *Freedom of Information and Protection of Privacy Act*, and other relevant legislation, policies and standards, in order to:
>
> 1. ensure government accountability;
> 2. provide evidence of its activities and organizational structure;
> 3. document its responsibilities, rights and entitlements; and
> 4. preserve records of enduring value.[45]

The Government Records Service (GRS), which is housed in the Ministry, became a centralized service to government in 2009, at the same time as the processing of freedom of information requests was centralized in IAO. GRS provides a wide range of records and information management services to ministries, including these:

1. Development and maintenance, with approvals under the *Document Disposal Act*, of the government's records classification systems. These are the Administrative Records Classification System (ARCS) and the Operational Records Classification System (ORCS).
2. Support services to ministries in applying and maintaining ORCS and ARCS.
3. Creation of policies and procedures relating to records management.
4. Support services to ministries in developing records schedules for approval and in implementing them.
5. Managing administration of the electronic records system (TRIM), maintaining its standards, and managing TRIM implementation projects.

[44] Section 12.3.3, Part III: Managing Information: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1233.
[45] *Ibid*.

6. Help-desk and advisory support for government employees using automated records management systems or performing other records management functions.
7. Developing and delivering records management training, including integrating freedom of information training.

GRS supports ministries in developing records schedules for approval under the *Document Disposal Act*. It does not enforce the proper implementation of government records management policies, whether through audit or inspection. In addition to specialized employees (*e.g.*, archivists, trainers, and off-site records storage employees), GRS staffing includes only four records officers who provide direct support to ministries. Each of them is responsible for a portfolio of ministries and each records officer has a staff of three records analysts. Records officers work with ministry officials at the executive director or assistant deputy minister level to advocate for records management. They also provide records management advice and support to other levels of ministry staff in meeting their records management responsibilities. Each ministry decides how much to invest in records management in addition to the central GRS resources. While some ministries have a dedicated or part-time records manager or coordinator, most do not.

IMPROVING TRANSITORY RECORDS POLICY

Several aspects of the existing records management framework are discussed below, with specific recommendations for improvements in key areas. The next section outlines how the investigation report deals with transitory records issues, setting the stage for the recommendations below for improving transitory records policy.

Transitory records and the investigation report

The investigation report raises the issue of what qualifies as a transitory record. This stems from Commissioner Denham's finding that the "broad interpretation given to transitory records" by the Premier's deputy chief of staff resulted in her retaining almost no sent emails.[46] She found that this "frustrates the Premier's office's ability to comply" with the s. 6(1) duty to assist applicants. She also found that, because of this, the Premier's office had not fulfilled its duty to assist the applicant who had requested the sent emails.

As the investigation report recognizes, consistent with law and practice in many other jurisdictions at home and abroad, the provincial government's records management and

[46] Report, p. 52.

retention scheme permits the routine destruction of transitory records. The right of access extends only to records that exist—*i.e.*, those in the custody or under the control of a public body—at the time an access request is made that covers them. If a record has already been destroyed because it has properly been identified as transitory, it obviously cannot be disclosed in response to a request that is made after its destruction. It is thus important to ensure that only truly transitory records are destroyed. It is also vitally important that transitory records be properly identified given the broader public interest considerations mentioned earlier.

Commissioner Denham observes, consistent with what is said earlier in this report, that the content, not the medium of communication, determines whether a record—including an email—is transitory. She calls for "an informed and reasoned approach" in making that determination "on a case-by-case basis."[47] The definition and interpretation of what is a transitory record is therefore important. Conceptual clarity and appropriate implementation are key to a records management framework that treats transitory records appropriately. Because of the central role played by transitory records in the investigation report, and the implications for sound records management, it is necessary to discuss transitory records policy at some length.

Origins of modern records management approaches

The purpose of a policy authorizing employees to dispose of transitory records can only be understood in light of the origins and nature of government's record management system.

In spite of the immense changes in information technology over the past 25 years, government records management practices in British Columbia and elsewhere have largely been based on principles and methods developed in the C19th and expanded to an industrial scale after World War Two. The basic principle is that no government records, however they are created and kept by government officials, can be destroyed *unless* destruction has been approved by an appropriate authority that represents the interests of government accountability and community history, not ideology and political interest. The principle has its roots in the development of modern democratic government, where records of the state are seen as the repositories of the people's rights and interests as embodied in the government.

Before World War Two, governments, and the archives they had established to keep their records for the long term, needed to review and approve the destruction of a relatively small amount of records. To support the massive military and economic initiatives required by the war effort, governments greatly expanded their mandates and activities. The size and scope of state activity

[47] Report, p. 52.

continued to expand after the war as the administrative state grew. As a result, at the same time that the volume of government records grew exponentially, qualitative aspects of record-keeping—how they are created, organized and accessed—declined. Of particular concern was the significant increase in the creation and use of duplicate documents, facilitated first by photocopiers and later by electronic transmission technologies that sped up distribution of information but also led to record duplication.

All of these factors spurred the development of records management regimes in British Columbia and elsewhere that attempted to impose order on government records through classification schemes, using records schedules that outline retention and disposal rules that apply a lifecycle management process perspective. To reduce processing effort, governments differentiated between operational records schedules and classifications, which required customized analysis and approval of every new records series, and general schedules and classifications that could be applied to common administrative records.

In British Columbia, this thinking lies behind the development of the ARCS (Administrative Records Classification System) and ORCS (Operational Records Classification System) methodology in the 1980s. To control duplication, records managers at first established centralized file rooms to support access to single copies of documents and to discourage the distribution of multiple copies among agencies. Central filing diminished in practice, and became less relevant, as electronic records became the dominant record medium. Instead, ARCS and ORCS schedules designate an "office of primary responsibility" for each series of records, thus designating copies held by other offices as duplicates.

Even with these measures in place, records management programs in all governments could not provide full control over records disposition, especially for digital records. Part of the reason for this is that records managers and archivists, for both theoretical and practical reasons, have avoided getting involved in the actual creation and management of records during their active (or primary) phase of use, preferring to apply schedules and retention policies only at the point when records become largely inactive for their original purposes. One consequence of this, in a system that prohibits destruction of records except by records schedule, is that government agencies were reluctant to destroy even obviously insignificant documents, such as duplicates of records, even though they might have proliferated across government. This resulted in duplicates, and records of obviously temporary value, being retained electronically, to be handled by records management downstream as part of the full scheduling process.

In turn, this led policy-makers to ask whether a policy and process could be developed that would facilitate—in fact, encourage—agencies to reduce redundancy and increase the quality of their

record holdings at the creation and capture stage. This was the impetus behind the concept of transitory records and transitory records policy. The latter essentially identifies types of records that may be destroyed without third-party approval, case-by-case or in accordance with a records schedule.

It is now generally agreed that the purpose of a transitory records policy is to authorize officials to cull documents as part of a routine process of drafting, version control, and consolidation before they are captured in a records management system. The policy is thus mainly concerned with identifying the kinds of information that should be considered insignificant, and destroyed, from the kinds of information that have value and, rather than being destroyed, must be captured in the scheduling system and retained. The difficulty lies in providing clear guidance that results in practical and consistent identification of information that may be disposed of, yet does not direct, or allow, government to destroy information that has such value that it ought to be retained.

Against this historical backdrop, the next section makes recommendations to assist government in revamping, as it should, its transitory records policy and guidance. These recommendations flow from a review of transitory records policies in leading jurisdictions that have systems of government similar to ours.

It should first be said that the timing for reform is auspicious because the *Information Management Act* is coming into force next year, necessitating development of new information management policies under that Act. Government should revise its transitory records policy in priority to other policies. In the meantime, government should move now to publish interim guidance for public servants on handling emails under the existing transitory records policy.

Transitory records policy standards

The starting point is to consider sources for a standard to be used in determining the effectiveness and quality of a transitory records policy. The International Standards Organization standard, Information and Documentation—Records Management (ISO 15489), does not deal with transitory records specifically, but a survey of key publications discloses the following notable, non-exhaustive, themes:

- Transitory records, or “ephemera”, are of immediate use and meant to be discarded shortly after they are created.
- Transitory records are not and should not be captured in a records management (scheduling) system.

- Transitory records are not defined by specific formats or media.
- Commonly-identified types of transitory records are drafts and copies.
- Determining whether or not records are transitory, regardless of the medium or type of record, is very often contextual.[48]

Comparative assessment of various transitory records approaches

Because transitory records management is now a widely accepted component of records management, there are many examples of policies from which, after comparative analysis, the components of a modern, workable transitory records policy can be drawn. The policies of several jurisdictions, all of which have freedom of information and privacy laws, were assessed: Alberta, Saskatchewan, Manitoba, Ontario, Canada, Australia, Queensland, New South Wales, and New Zealand. The key components of transitory records policy discussed below are drawn from these jurisdictions.

Transitory records

The first issue to consider is whether a transitory records policy should have a statement of purpose. Canadian policies do not, but others do. The goal of the transitory records policy of the federal Australian and the New Zealand governments is said to be to permit destruction of records as a "normal administrative process", as part of "sensible administration."[49] Australian policies come closest to expressly stating the root purpose of these policies, *i.e.*, to help mitigate the growth in records volume, which can overwhelm records scheduling and lifecycle management systems. In other words, transitory records policy is a way to encourage government agencies to do what they should be doing naturally as good record-keepers, culling records as part of their "normal administrative processes."

[48] See, for example, E. Shephard and G. Yeo, *Managing Records: A Handbook of Principles and Practice* (London: Facet Publishing, 2003, rpt. 2009) [*Shephard and Yeo*], pp 108-111, where they are dealt with, under "capturing records into a records management system", as ephemera, drafts, and copies. It is acknowledged that the entry for "ephemera" in L. Duranti and P. Franks, eds., *Encyclopedia of Archival Science* (New York: Rowan & Littlefield, 2015) is from the perspective of archival value, and emphasizes how such documents may provide significant insights into organizational or social history.

[49] The New Zealand government policy, in stark contrast to the approach in almost all other jurisdictions, still requires agencies to schedule and get approval for the destruction of transitory records. Quite how practical this is given the vast quantities of emails and other electronic records that are created each year is not clear.

Definitions of transitory record

Generally speaking, definitions of transitory records aim at determining whether records have functional utility for the record-creating agency or, in varying degrees, utility in ensuring accountability for actions. These are typical characteristics of transitory records:

- They are only useful for a limited or short time
- They will not be required again
- They are required only to support a routine action or to prepare a subsequent record
- They are not required to meet mandates, to sustain operations and administration, or provide evidence of an activity.

These characteristics are necessarily broad and ultimately are dependent on functional context. To further assist in identifying transitory records, therefore, transitory records policies have consistently identified a number of types or categories of records most likely to be transitory. Some of these are relatively self-evident, while others at best serve as (in reference to a list of specific examples) criteria to assist in transitory records identification. Last, some transitory records policies contain exclusions from coverage, *i.e.*, they identify types of records that must never be treated as transitory. These aspects are dealt with in the next section.

Facilitative or short-term value records

Records of no interest, or of only minor interest (and even then only for a brief period), are sometimes referred to as “ephemera”, as opposed to being called “transitory”. This category is generally considered to include the following, with the list often being determinative in identifying records in this class:

- Routine administrative notices distributed to all staff regarding holidays, staff events, fire drills, and the like
- Issues not requiring an office to act
- Personal messages
- Routing or transmission instructions (*e.g.*, addressing or routing instructions marked on a re-useable inter-office envelope)
- Appointments, calendars (with exceptions)
- In-transit or logistics status updates (*e.g.*, emails or texts like “I’m on my way”, “just sent it”, calendar invitations and communications to confirm an already-scheduled meeting)
- Opened envelopes not needed to identify sender and date
- Typing correction or formatting instructions

- Computer system batch or control reports.

The following are generally excluded from the above category of "ephemera":

- Work unit activities documentation (*e.g.*, work schedules and assignments)
- Information that helps explain the history of a relationship, decision or project
- Formal communication about official business
- Decision records, instructions, and advice
- Documentation of initiation, authorization or completion of a transaction
- Documentation that is evidence of a significant action
- Facilitating instructions that have policy or procedural implications, or were part of the transaction
- Computer audit logs.

External publications and advertising

Publications are generally not considered to be records unless they are created and distributed by government itself as a government publication. External publications therefore are not captured in records management systems. An example would be the office copy of a daily newspaper to which a public body has subscribed.

Advertising brochures, catalogues, flyers, spam email, advertising email, junk mail, and the like are, in any medium, transitory, unless the information was part of a government transaction (*e.g.*, a government procurement process).

Drafts

A category covering drafts or working versions of final documents is common to all transitory records policies that were surveyed. GRS publishes guidance on drafts, Managing Drafts and Working Materials.[50] It identifies activities where draft documents are likely to be kept, notably drafts of legislation and Cabinet or Treasury Board submissions. As the guidance assumes, drafts can document the opinions and ideas considered, and the decisions made, in creating a final record. These may record the creation or evolution of final records, but beyond this observation, the conditions and exceptions attached to this category in various policies range widely in content and scope. This reflects the fact that this is one of the more difficult aspects of transitory records policy to fashion, and also to implement.

[50] http://www.gov.bc.ca/citz/iao/records_mgmt/guides/drafts_working_papers.pdf (accessed December 1, 2015).

Some commentators differentiate between "working drafts" not considered by anyone other than the author and "approval drafts", in which others have annotated comments or approvals.[51] The latter may not be transitory, depending on the nature of the comments. For approval drafts, deciding what is transitory and what is a valid representation of the record as it was actually used at a particular time or in a specific context requires extensive analysis, especially if versioning becomes complicated. Moreover, it might be said, "final" documents, like building plans or database files, are constantly revised and overwritten, yet keeping previous documentation or changes may be of significance for accountability purposes. These revisions or changes are not transitory but are essential records of the progress of a matter or project.

All policies reviewed define drafts or working papers as documents generated for the purpose of producing a final document. At the same time, there is some recognition that many drafts can be significant records. How does an official decide if a draft can be considered transitory? Almost all policies support this decision-making with examples. However, in the policies surveyed there were examples of drafts that are considered to be transitory respecting which there is agreement, but also many where there is potential disagreement (sometimes within the same policy).

It is commonly agreed, however, that drafts containing only editing, stylistic or formatting changes are transitory records. Some jurisdictions, such as Ontario, take the view that, if comments in a draft are incorporated into the final version, the comments in the draft are transitory. In New South Wales, rough notes or calculations are transitory. Yet there is also fairly broad agreement that the following are *not* transitory:

- Drafts of documents that indicate new decisions or formal approvals, or contain significant or substantial changes or comments that provide insight into the evolution of the final version
- For policy, legislation, legal or research documents, drafts that are a record of changes that were made and why
- Drafts containing significant or substantial changes or annotations
- Working records and notes used as part of an investigation or project.

Despite the challenges in grappling with policy respecting this category of transitory records, it is clear government has to take up that challenge.

[51] Shephard and Yeo at pp 109-110.

Duplicates or copies

This category covers what many consider the most obvious class of transitory records: documents that are (relatively) exact reproductions of an original document. At the same time, all policies that were reviewed recognize that records duplicated elsewhere sometimes may not be transitory and thus need to be kept, with the following being prominent examples:

- Not transitory: Duplicates of incoming messages and correspondence from both internal and external sources that "should properly be captured" as an authority record because of the significance of who has received them in government. For example, email sent to an official from another internal official source, or an external source, and that relates to the recipient's functions (while also being kept by that official or external source as outgoing email)
- Transitory: Convenience copies kept locally for quick reference (New South Wales, Ontario, Alberta, Saskatchewan). This would cover reading or day files, if outgoing and incoming records are kept as official records elsewhere
- Transitory: Duplicates where the master version has been filed in an official filing system (Alberta, Saskatchewan). (It has to be recognized that determining whether the master version has been officially filed can be a challenge.)
- Transitory: Copies of records that support the development of other documents but are not themselves of value for retention. An example is a summary or extract of a record that is already retained in the agency's records management system (Australia). Another example would be a precis, for convenience, of a report that is itself retained in the records management system

Some policies provide criteria such as the above, but also list typical duplicate documents that can be considered transitory (Ontario, Alberta):

- Photocopies of originals
- Electronic copies (messages and documents)
- Printouts of electronic or microform documents
- Copies of distributed manuals, polices, guidelines, directives
- Reading, day, or chronological files.

Provincial government transitory records policy

This section discusses the provincial government's existing transitory records policy in light of the above overview and makes recommendations for improvement.

GRS's Recorded Information Management Policy Manual stipulates that "government records" consist of "any and all recorded information created or received by government offices in the course of business activity and maintained as evidence of those activities, regardless of their digital or physical format".[52] The manual affirms that "government offices" include "offices that are part of any ministry", and that this includes the offices and records of ministers in developing, administering or implementing programs of government.[53] As regards records management, all "government employees, including consultants and elected officials, are responsible for managing the government records they create and receive in the course of their work, in accordance with legislation and policy identified in this document and elsewhere."[54]

Consistent with the above-noted *Document Disposal Act* provisions, government policy prohibits the disposal of records except in accordance with a records schedule.[55] The key here is Transitory Records Schedule (102901),[56] which defines transitory records as follows:

> Transitory records are records of temporary usefulness that are not an integral part of an administrative or operational record series, that are not regularly filed with standard records or filing systems, and that are only required for a limited period of time for the completion of a routine action or the preparation of an ongoing record.
> Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions. Originals or copies required for statutory, legal, fiscal, administrative or operational purposes will be retained in a regular filing system and disposed of separately in accord with the *Document Disposal Act*. This schedule covers the following types of transitory records.
>
> 1.1 Convenience Copies
>
> Extra copies of records created and retained only for the convenience of reference, including photocopies.
>
> 1.2 Unnecessary Duplicates
>
> Stocks of publications, pamphlets, blank forms, informational material, etc. which have no further usefulness.

[52] Government Records Policy, section 2.2.1. http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/rim101.pdf.
[53] *Ibid.*, sections 2.1.1 and 2.1.3.
[54] *Ibid.*, section 3.4.
[55] Records Destruction Policy, section 2.1. http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/rim501.pdf.
[56] http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/transitory_records.html.

> 1.3 Working Materials and Drafts
>
> Rough notes, steno work materials, word processor diskette copies, calculations, preliminary drafts, rough research notes, and similar materials used in the preparation of correspondence, reports, memoranda, statistical tabulations, or other records.
>
> Once the finished record has been produced, documented, and incorporated into a regular filing or records system, these working materials become transitory records.
>
> NOTE: This schedule does not cover working materials and drafts that are described or specified in some other records schedule. For example, this schedule does NOT cover working materials relating to the preparation of legislation or audit reports. Disposition of records relating to legislation and other specified working papers will be approved separately in accord with the *Document Disposal Act*.[57]

Two other records schedules are of importance. The Electronic Mail Schedule (102903) says this about email:

> Electronic mail records contain recorded information that may be either transitory or required for ongoing purposes. If an electronic mail record meets the criteria for a transitory record (see special schedules 102901 and 102902), it may be disposed of when no longer required.
>
> If an electronic mail record is required for ongoing legal, fiscal, audit, administrative or operational purposes, transfer it to a storage medium (paper file, microfiche, or an electronic information system) suitable for retention of ongoing records.[58]

As the Electronic Mail Schedule alone shows, from a user's perspective the most obvious issue with British Columbia's transitory records policy is that it is not one but a series of policy documents with additional and sometimes overlapping scope depending on medium or circumstance. This may cover the bases in terms of logical policy coverage, but is not conducive to effective understanding by users and thus does not promote sound implementation.

Next, the Transitory Records Schedule, which is where most users would first look for applicable rules, is of limited utility in modern terms. Its description of draft materials, for example, provides blanket authority to destroy all draft material once a final document is completed. Viewed in light

[57] http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/transitory_records.html (accessed November 27, 2015).
[58] http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/electronic_mail.html (accessed December 1, 2015).

of the standards and policies of other jurisdictions, and GRS's own explanation, this is problematic. It could result in destruction of any document produced during the course of preparing a final decision or position, no matter how significant the draft might be in the process.

The Electronic Mail Schedule is laudable insofar as it attempts to give specific guidance on email, but it is redundant in light of the Transitory Records Schedule (although the latter requires, again, clarification and updating to address email and other issues). Having a separate schedule for email risks, however, singling out email as something apart. Combined with the schedule's emphasis on transitory emails, this will confuse users.

The Transitory Electronic Data Processing (EDP) Records Schedule (102902) also addresses only one type of record. Its opening portions have an apparent emphasis on the transitory, even though such records may, depending on context, have played a significant role in decision-making and action and thus not be transitory:

> Transitory EDP records are records of temporary usefulness that are not an integral part of an administrative or operational record or data file, and that are only required for a limited period of time for the completion of a routine action or the preparation of an ongoing record or file. Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions. Originals or copies required for statutory, legal, fiscal, administrative or operational purposes will be retained in a database or data file and disposed of separately in accord with the *Document Disposal Act*.
>
> NOTE: This records schedule covers word processing records, including disks and diskettes, if the records come within the general definition of transitory EDP records. See also the special schedule for word processing records (102904).
>
> NOTE: This records schedule does *NOT* cover generation data groups, image backup copies (used for system recovery purposes), or backup copies of specific data sets. These are NOT transitory records and disposition will be approved separately in accord with the *Document Disposal Act*.
>
> NOTE: This records schedule does *NOT* cover electronic mail unless records created by electronic mail clearly fit within one of the categories described below. For electronic mail see special schedule (102903).

> There are three categories of transitory EDP records: (1) input records; (2) processing records; and (3) output records…[59]

Last, GRS's guidance on implementation of the transitory records policy relies heavily on a user's analysis of the significance of the actions that are documented. The list of non-transitory records found in that guidance document could be seen to contradict the permission in the Transitory Records Schedule to dispose of all "preliminary drafts". This has to be clarified to eliminate confusion.

Given the above, the following section sets out recommendations for reform of government's transitory records policy. Implicit in the recommendations is the overall need to consolidate and revamp the policy on transitory records

Reform of transitory records policy

Transitory records policies require those who create records or handle them to make often difficult judgements as to what is or is not a transitory record, with that decision very often being based on specific circumstances, not just formalistic categories of records or content. This sensitivity to circumstances means it is very important to clearly state the objectives of the policy, as is done in Australia. There should be an affirmation that government needs to create records of key activities and decisions and retain certain records that it obtains elsewhere.[60] The policy statement should explain why this is important because this will help communicate why identification of transitory records is done. A purpose statement should include elements such as those found in this version:

> Government recognizes the need to create records of its activities and decision-making and to retain these in its records management system. The purpose of this transitory records policy is to enable government employees to identify and dispose of records that do not have value as a record of government's activities and decision-making. This is part of normal administrative processes. It is intended to promote the quality of government's records holdings.

The following section sets out recommendations for various elements of a new transitory records policy. As the thrust of the discussion suggests, it is not recommended that government legislate

---

[59] http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/transitory_edp_records.html. (accessed November 30, 2015). The remainder of the schedule discusses several categories of so-called electronic data processing records, such as transmittal copies, information gathered through automated data processes, and intermediate processing copies.

[60] Also see the discussion below about the duty to document.

a definition of transitory records, or set it out in regulation. The latter approach is more flexible than legislation, but policy is the most flexible of all. It is not clear, given the structure and language of the *Information Management Act*, what advantage would be gained by amending that Act, or attempting to make a regulation under it, to define transitory records. Another consideration is that the policy on transitory records is only one piece, albeit a critically-important one, of the entire puzzle. As noted earlier, one of the weaknesses of the existing framework is that multiple policies touch on transitory records, with this fragmentation likely to cause confusion. Separating the definition of transitory records—which would in any case be very difficult to draft in accepted legislative language—from the remainder of the policy framework could equally create uncertainty.

The first point is that the new policy should make the determination of whether any record should be destroyed or retained essentially a process of answering the following series of cascading questions:

- Is the function or activity for which the record was produced and used significant?
- Is the record significant in relation to the transaction or activity it was created and used to support?
- Does the information, in relation to other captured (or to be captured) records, best document the function or activity it was created or used to support?

Some or all of the following questions are used to provide criteria and rationales in many transitory records policies, and these could usefully inform government's development of a new transitory records policy.

1. Is the function or activity for which the record was produced and used significant?

The significance of the function or activity that the final document supports and of which it is a part is key to determining the retention and preservation of any government record (always assuming, of course, that this is limited to a government function or activity, not a personal matter). However, it is not the goal of a transitory records identification process to determine the relative significance of the function or activity that is being documented. That is the objective of the records management process after the records are captured into the system, with retention and disposition being driven by that analysis. Officials therefore should not need to consider the significance of the function and activity when identifying what is transitory.

For example, the activity of routine maintenance of a government building is generally considered less significant than development of new legislation. Yet, because that process is a government activity, some evidence of that activity needs to be captured, with records management schedules determining whether and how long records documenting these activities are retained.

2. *Is the record significant in relation to the transaction or activity for which it was created and used in support?*

If all functions and activities are essentially equal for the purpose of identifying transitory records the next step would be to analyze the relative significance of the document in terms of its contribution to or participation in the function or activity. For practical purposes, it is assumed that, if it is necessary to create or receive a record to further or complete the transaction or activity, the record is significant enough for the limited purposes of a transitory records policy. The real question revolves around the quality, the value, of the record or information in relation to the function and activity.

3. *Does the information, in relation to other captured (or to be captured) records, best document the function or activity it was created or used to support?*

This question helps delineate the boundaries of both the scope and content of a transitory records policy. Regardless of the function or activity, and assuming that the record was created and used for a purpose, it is simply a matter of determining whether it provides unique, or the most effective, evidence of a function or activity. This would mean that information that is irrelevant to a particular activity, or that duplicates information better held elsewhere, is transitory. On the other hand, even if the record, in its format or content, is of poor quality, it should not be considered transitory if it is the only record.

The following discussion should be read in light of this important consideration: the scope of the transitory records policy should be limited to identifying records which, in relation to records captured elsewhere, best document the functions or activities they were created or used to support. With this purpose and this scope established, the following section sets out recommendations for specific categories of records in a new transitory records policy.

Email

It is convenient to first pause and address some of the qualities that are arguably inherent in email or the way in which we perceive and use it. Email as a communications medium has an almost instantaneous quality to it. Emails can have a casual, almost conversational, quality to them. Email is also often used for trivial or mundane matters. As illustrated earlier, many if not most personal emails are impermanent, in the sense that they are not worth keeping. Yet many of us use email for both business purposes and personal uses, and these different uses can blur into each other, sometimes in the same email, and at a higher level in ways that may influence our perceptions of the permanence or ephemerality of email. All of these factors may lead some to view email as inherently ephemeral.

With apologies to Marshall McLuhan, the medium and the message must not be confused: they are not the same thing. No one treats the paper on which a letter is written as the message. It is the letter's content that matters. It is therefore important that public servants not treat emails as different from other kinds of records, as somehow inherently ephemeral, insubstantial, or without value.

The prevalence of email as a communications tool within government means that it should be specifically addressed in the transitory records policy. This should be done to help employees understand that emails may or may not be transitory, depending on the content and context of each email.[61] The policy should therefore affirm, consistent with observations earlier in this report, that email is a business communications tool, a medium of communication. The policy should clarify that whether an email is transitory depends on its content and context, and that the other factors mentioned in the policy must be considered in making this decision. In addition, guidance on handling email should be published, as discussed below.

The transitory records policy, and guidance and education for public servants, also should make it clear that email accounts are not records management systems. The email folders in someone's email account must not be treated as a filing system. This is not where government records should be kept, certainly not once an activity or transaction is complete. The place for government records is in government's records and information management system.

[61] Commissioner Denham has expressed similar views: "My office has found that some government ministries and program areas apply a liberal interpretation to what constitutes a transitory record, basing the determination on the medium of communication, such as email, rather than on the content of the communication, such as whether it is a record of action or decision-making. I believe that the determination of whether a record is transitory is technology neutral, and depends solely on the content of the record or communication." Investigation Report F14-01, pp. 17-18.

Drafts

As noted above, drafts represent perhaps the most difficult issue in a transitory records policy. There can easily be confusion about whether drafts can be considered transitory.

Again, many transitory records policies recognize that the process of creating a document, and the decisions and considerations involved in that process, sometimes need to be documented and retained. From this perspective, drafts can be the product and, to a varying degree, the record of the record-creating process itself.

A transitory records policy as it relates to drafts should be fashioned in light of the three questions set out above, including the question of the significance of a record in relation to a particular activity. It cannot be assumed that all drafts, because they are only working or background documents, are never significant and thus are always transitory. The real question is whether a given draft document meets the standard of being the best evidence or documentation of a process. This requires, in turn, consideration of the following two questions.

1. *Which decisions and changes in the drafting process are significant?*

For example, decisions on simple formatting, presentation, or typographical errors would be insignificant and drafts containing information only about these decisions and actions could be considered transitory. However, proposals and decisions on content documented in the draft should generally not be.

2. *Which draft information best documents the significant decisions and changes?*

This consideration would identify drafts that uniquely and most effectively document important decisions and changes in the final document. This kind of information can, if it is duplicated or rolled-up into later documents, be considered transitory.

It is convenient to note here as well that, if an activity or transaction is not completed, as in the routine building maintenance example above, and no final document is produced and distributed, the latest draft should likely be regarded as the final document (with any earlier drafts being assessed in line with the process outlined here).

Copies of records

This category covers what many consider to be the most obvious of transitory records: documents that are (relatively) exact reproductions of an original document. Yet current capacities to distribute and reproduce messages and documents electronically have created what many records managers see as an epidemic of duplicated and redundant information.

At the same time, duplicates can, by virtue of the context in which they exist, including their distribution or location, contain evidence of activities or decision-making. As an example, an email that is by definition a duplicate can, by its presence in a particular official's inbox, document that the official had knowledge of a significant action or decision. Someone in this position must ask not only whether the record is a duplicate, but also whether it documents the official's participation in the activity or decision-making process and thus has such value that it should be retained.[62]

The last point is that government should continue to use its system for designating an office of primary responsibility for records, as a tool for identifying whether a specific office is keeping the master copies of widely-distributed copies of materials.

Short-term value records

The existing policies for advertising, promotional material and unsolicited material should be consolidated here, along with the policies covering transitory electronic data processing records.

What to avoid

Whatever form a new, consolidated and comprehensive transitory records policy takes, it is important to avoid provisions that could perpetuate misinterpretation. These are important examples of what should be avoided:

- Permitting disposal of records of a "routine action or communication" might be fine as a general objective, but could permit too broad an interpretation on the ground to be useful as a specific provision
- No provision should be included that permits disposal of "automated records" defined as those *not* "directly and specifically reviewed by an individual." Such a provision could usefully authorize disposal of spam email and junk mail, but it could be interpreted to allow deletion

[62] Of course, this could in principle be addressed by ensuring appropriate preservation of metadata, both in email or paper format, as long as receipt can be confirmed.

of emails by an official who only was copied but did not read the material. Evidence that someone received an email may be important

Guidance on applying transitory records policy

The current GRS guidance on transitory records provides useful examples of what can and cannot be identified as transitory under the existing policy. This will have to be updated, however, to support new transitory records policy. GRS should also regularly review and update the guidance to keep abreast of new issues, new types of information and new information systems in government. Updates to the guidance should be informed by users' experience as they communicate it to GRS, when seeking specific guidance in particular cases. There needs to be, in other words, an effective feedback loop to inform guidance on transitory records.

As noted above, the prevalence of email, and interpretive challenges associated with its proper assessment for records management purposes, require meaningful guidance on handling email. GRS already offers a suite of useful online guidance tools on email. However, it should ensure that this guidance both captures the new policy well, but also stays abreast of guidance elsewhere. This guidance from the State Archivist of Queensland, while it to some degree overlaps with GRS's guidance, is a good example of the plain language resources that are needed:

> Capturing emails is simple – save as you would any other record. So whatever recordkeeping application, shared drive, other business or collaborative application you're using, save your emails accordingly and apply any additional metadata as required. Remember, most email systems are not designed with recordkeeping functionality, so you will likely need to save your emails elsewhere if they are evidence of a business activity or decision. Remember, email archives and back-up tapes are not suitable methods of capture.
>
> In your agency's data entry standard, make suggestions on the creation and capture of emails:
>
> - include as much detail as possible in the subject field
> - suggest a standard for capturing emails e.g. Email from [name] to [name] regarding [subject].
>
> Think about business rules relating to emails:
>
> - if you are the sender – you are responsible for capture
> - if you have received an email from an external sender and you are the only recipient in your agency – you are responsible for capture

- if you have received an email from an external sender and you are one of many recipients in your agency – the person who is most directly involved in the issue or task is responsible for capture.

Remember to:

- capture emails at the end of a thread where possible (rather than every to-and-from)
- capture attachments to emails
- capture work related emails from your personal email accounts if they are used for business
- check the relevant Retention and Disposal Schedule to ensure you don't delete any business emails that are required to be kept for a certain period of time.[63]

A much broader issue, noted here only in passing, is the need for a comprehensive framework for the management and retention of emails within the government's electronic records management system. This is indirectly acknowledged by the government's recently-released request for information on enterprise information management, issued in light of government's strategy for managing digital information.[64]

OVERSIGHT OF RECORDS DESTRUCTION

Commissioner Denham's recommendation 8 is that government should introduce amendments to provide "independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met." This is the discussion in the investigation report itself:

> There also needs to be independent oversight of the destruction of government records. It is unacceptable that no independent body watches over this important step in the lifecycle of government records. Adding independent oversight would be a major step towards restoring public confidence that government properly destroys its documents and is accountable for its practices.[65]

[63] http://www.archives.qld.gov.au/Recordkeeping/Digital/Pages/Strategies-for-capture.aspx (accessed November 30, 2015).
[64] Both the strategy and request for information can be found here, on the BC Bid website, under the 'supplier attachments tab': http://www.bcbid.gov.bc.ca/open.dll/showDisplayDocument?sessionID=901205826&disID=30790958&docType=Tender&dis_version_nos=3&doc_search_by=Tend&docTypeQual=TN (accessed December 1, 2015).
[65] Report, p. 57.

In her submission to the Special Committee, Commissioner Denham made this recommendation:

> Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records.
>
> The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:
>
> • any enactment of British Columbia, or
> • set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.
>
> The oversight over unauthorized destruction should come with complementary offences and penalties under FIPPA.[66]

Commissioner Denham appears to have in mind through recommendation 8 legislative authority to investigate whether a record has been destroyed contrary to an enactment or records management rules.

As her submission to the Special Committee notes, Alberta's Information and Privacy Commissioner has the authority to "conduct investigations to ensure … compliance with rules relating to the destruction of records" where those rules are set out in an Alberta enactment or local public body legal instrument.[67] A survey of other Canadian jurisdictions discloses that, in addition, Ontario's *Freedom of Information and Protection of Privacy Act* and *Municipal Freedom of Information and Protection of Privacy Act* will, effective January 1, 2016, include the following obligation:

> 10.1 Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or

[66] Submission to the Special Committee, recommendation 12, https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/4th-session/foi/presentations/20151118/FIPPA_2015_11_18_OIPC_Submission.pdf.
[67] *Freedom of Information and Protection of Privacy Act* (Alberta), s. 53(1)(a).

> records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution.[68]

Manitoba's *Freedom of Information and Protection of Privacy Act* gives the Ombudsman, who is responsible for enforcing that Act, the following authority:

> 49 In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may … (a) conduct investigations and audits and make recommendations to monitor and ensure compliance … (ii) with requirements respecting the security and destruction of records set out in any other enactment or in a by-law or other legal instrument by which a local public body acts.

The Information and Privacy Commissioner of Alberta is in the midst of an investigation of the alleged improper destruction of records in the wake of the provincial election earlier this year. In 2013, the Ontario Information and Privacy Commissioner investigated alleged improper destruction of records by political staff.

In British Columbia, the *Information Management Act* will authorize the government's chief records officer to approve information schedules, the modern version of records schedules. These are required to provide, "with as much specificity as practicable, for the disposal of all information required to be disposed of by law and for the holding of all information required to be held by law."[69] Under s. 19(5) of the *Information Management Act* "the head of each government body must ensure that no government information held by the government body is disposed of, except in accordance with an information schedule or an approval by the chief records officer" where no information schedule exists.

This legal duty should give executives every incentive to recognize the importance of executive commitment to a culture of proper records management. While this legal duty to ensure proper records management is vitally important, a culture of proper records management is also vitally important. It has been said that culture eats policy for breakfast: in this area, as in others, senior leadership will be critically important in preventing that from happening, by fostering a culture that fully supports sound information management practices.

The *Information Management Act* does not expressly provide oversight for destruction of records. It could reasonably be said that public confidence in the integrity of government records management requires independent authority to investigate allegations of improper destruction.

---

[68] Section 10.1, to be in force as part of the *Freedom of Information and Protection of Privacy Act* (Ontario). The same provision will come into force in the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario).
[69] Section 4 provides that an "information schedule is not an enactment."

The government should therefore give the most serious consideration to Commissioner Denham's recommendation, with legislation along the lines of Alberta's s. 53 being a good model to consider. This would be focussed on improper destruction of records, not oversight of information management generally.

When viewed through the lens of Commissioner Denham's submission to the Special Committee, recommendation 8 has another aspect. In her submission, she refers to the fact that it is an offence under Alberta's law to destroy records in an attempt to evade a request for access. Section 92(1)(g) of that province's *Freedom of Information and Protection of Privacy Act* provides as follows:

> 92(1) A person must not wilfully
>
> (e) alter, falsify or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record, …
>
> (g) destroy any records subject to this Act, or direct another person to do so, with the intent to evade a request for access to the records.

Similar offences exist in other Canadian freedom of information laws.[70] For example, Ontario will also, as of January 1, 2016, have a very similar provision.[71] Such a provision actually exists already in British Columbia. The *Personal Information Protection Act*, British Columbia's private sector privacy law, provides as follows:

> 56 (1) … an organization or person commits an offence if the organization or person …
>
> (b) disposes of personal information with an intent to evade a request for access to the personal information.

There are two possible approaches here; these are not mutually exclusive. First, at the very least government should promptly make such policy and practice changes as are necessary to ensure that any employee appointed under the *Public Service Act* who destroys a record, or directs or assists anyone else in doing so, with the intent to evade a request for access to the record is subject to employment discipline up to and including dismissal for cause.

[70] The freedom of information laws in the following jurisdictions make it an offence to, in essence, destroy records in an attempt to evade or frustrate an access request for those records: Alberta, Manitoba, Ontario (as of January 1, 2016), Quebec, New Brunswick, Nova Scotia, Prince Edward Island, Newfoundland and Labrador and Yukon.
[71] Section 61(1)(c.1) of the *Freedom of Information and Protection of Privacy Act*.

The second approach is to legislate along the lines of s. 92 of Alberta's *Freedom of Information and Protection of Privacy Act*. It must be acknowledged that there might be a concern that the mere possibility of such a penalty for wilful destruction could persuade employees to retain records that are transitory and thus need not be retained.

It has to be remembered that the offence is to destroy with an intent to "evade" a request for access. The offence would be very specific, focussing on the kind of wilful misconduct that Commissioner Denham has found had more likely than not occurred in the MOTI case. It has nothing to do with ordinary-course records management compliance. Rather, the offence contemplates specific intent to "evade" an access request. This would require knowledge on the part of the individual that the request has been made and that it attaches to the records in question. Ordinary-course disposal of a record, whether as transitory or in accordance with other records schedules, would not be an attempt to "evade … a" request for access to "the" record that is disposed of with knowledge of the request.

On the basis that the above elements can be clarified in statute, to underscore how focussed the scope is, government should give serious consideration to amending FIPPA to create such an offence. Both aspects of the Alberta provision cited above.

In summary, government should make such policy and practice changes as are necessary to ensure that any employee appointed under the *Public Service Act* who destroys a record, or directs or assists anyone else in doing so, with the intent to evade a request for access to the record is subject to discipline up to and including dismissal for cause. Second, government should also give serious consideration to introducing legislation, consistent with s. 92(1) of the Alberta *Freedom of Information and Protection of Privacy Act*, that would make it an offence to destroy a record, or direct or assist anyone else in doing so, with the intent to evade a request for access to the records.

Government will, of course, wish to consider how best to proceed with the two above recommendations for legislative reform. If Minister Virk's referral to the Special Committee on these matters remains active, and government decides to support these recommendations, one option might be to make a submission to the Special Committee indicating government's support and indicating what government's intentions are should the Special Committee recommend these amendments.

DUTY TO DOCUMENT

Commissioner Denham's eleventh recommendation is that a duty to document should be enacted. As discussed below, the option that merits serious study by government is to legislate, as Commissioner Denham has recommended, a general duty to document, with supporting policies being devised ministry by ministry in a manner comparable to how information schedules will be created under the *Information Management Act*.[72] If government did decide, after study, to introduce legislation of this kind it would be the first government in Canada to do so in such direct terms.[73]

In Investigation Report F13-01, and in her testimony last month to the Special Committee, Commissioner Denham recommended enactment of a legislated duty "to document key decisions", referring to this as demonstrative of a government commitment to accountability "by creating an accurate record of its actions." This passage from the preface to Investigation Report F13-01 succinctly states her position:

> In the course of this investigation, we have seen evidence of the practice of "oral government", where business is undertaken verbally and in a records-free way. There is no requirement in FIPPA to document these activities. Without a duty to document, government can effectively avoid disclosure and public scrutiny as to the basis and reasons for its actions. The lack of documentation undermines the ability of citizens, journalists and the public to understand the basis for government's actions on any particular matter.[74]

The report went on to say this:

> I would reiterate that this requirement need not be an onerous one. The duty to record actions, decisions and reasons are not [*sic*] merely a question of creating records for the purposes of openness and accountability, but also go to good governance, the state of information management and information holdings of government.

[72] And as is now done with records schedules under the *Document Disposal Act*.
[73] Section 6 (1) of the Newfoundland and Labrador *Management of Information Act*, it should be noted, requires the head of every public body to develop, implement and maintain a "record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records." This speaks to a records management system for creation of records. It does not directly and unequivocally impose a positive duty to create records.
[74] Investigation Report F13-01, p. 3

> I believe a legislated duty to document is a critical element of the Government of British Columbia's open government movement, which promotes public oversight of its actions.[75]

In a March 18, 2013 letter to the Minister of Citizens' Services and Open Government, the Commissioner spoke in broader terms about the nature and scope of the duty.[76] She elaborated that government should legislatively require "public bodies" to "document the decisions, actions, advice, recommendations and deliberations of their officials." Moreover, she said that there should be a new duty to secure and preserve records in the custody of public bodies.[77] The Commissioner's letter stated that there are "many precedents for a statutory duty to document", citing examples from jurisdictions outside Canada.

In 2013, Canadian information and privacy commissioners jointly called for "the creation of a legislated duty on public bodies to document (that is, create records relating to) any non-trivial decision relating to the functions, policies, decisions, procedures and transactions relating to the public body."[78] In addition, in Newfoundland and Labrador a legislative review committee last year made the following recommendations to the provincial government there:

> The Committee recommends that
>
> 79. The Government take the necessary steps to impose a duty to document, and that the proper legislation to express that duty would be the *Management of Information Act,* not the *ATIPPA.*
>
> 80. Implementation and operation of this new section of the *Management of Information Act* be subject to such monitoring or audit and report to the House of Assembly by the OIPC as the Commissioner considers appropriate.
>
> 81. Adequate resources be provided to public bodies served by the Office of the Chief Information Officer, so that there is consistency in the performance of information management systems.[79]

---

[75] *Ibid.*, p. 21.
[76] https://www.oipc.bc.ca/public-comments/1514 (accessed December 3, 2015).
[77] In Investigation Report F13-01, the Commissioner recommended a legislated duty to document in a way that appears more oriented to the provincial government. Her March 18, 2013 letter to the Minister, however, speaks in terms of public bodies, of which there are more than 2,000. As noted below, a broader duty in this sense would, clearly, have much greater fiscal implications.
[78] https://www.priv.gc.ca/media/nr-c/2013/res_131009_e.asp (accessed December 4, 2015).
[79] Hon. C. Wells, D. Letto and J. Stoddart, *Report of the 2014 Statutory Review of the Access to Information and Protection of Privacy Act*, p. 315. http://www.ope.gov.nl.ca/publications/pdf/ATIPPA_Report_Vol2.pdf (accessed December 4, 2015).

As already noted, no Canadian jurisdiction has enacted a statutory duty to document that is as direct as that recommended by Commissioner Denham. For the reasons given below, Commissioner Denham's recommendation merits every serious consideration.

In terms of the archival, records and information management context, there is undoubtedly a clear link between records and information management and a duty to document. A duty to document will necessarily involve archivists, or records and information managers, becoming involved to some degree in deciding what kinds of records should be created, by whom and how. The duty to document may also involve them in overseeing what is done on the ground, perhaps through audit and review.

In the past, it was thought that archivists and records managers should remain separate from the institutions whose records they were to review and preserve. They should not, it was believed, intervene in the decision-making and operations of agencies in relation to records creation. Some archivists have in the past argued there is danger in having archivists, who are interested in historical research, harming their impartiality as evidence if archivists' opinions about what should be created, and what should be kept for posterity, influence the record–creator in deciding what to create and keep, and what to destroy. These observers have been concerned that an archivist or records manager might say to an official, 'You should have documented this activity or transaction this way, and said these things, and not those things.'

By contrast, others have concluded that electronic record-keeping has eroded the practicality of maintaining any strict boundary between an organization creating records for its own purposes and archivists waiting for the organization to finish with the records before they can appraise and preserve them. Indeed, in Australia and New Zealand, it can be argued, the distinctions between archives and records managers, and between archives, records managers, and the records-creating agencies, are diminishing. Moreover, it is surely possible to manage any risk by implementing a duty to document through policies that are developed and implemented by organizations themselves, in light of their organizational purposes and activities. To sum up, these considerations should not be seen as a barrier to creation of a duty to document, since they can be managed.

Further, it is undoubtedly true that significant risks are raised by a failure to keep adequate records:

1. Diminishment or elimination of accountability of elected or appointed officials for their actions and decisions

2. Reduced openness and transparency of government activities, notably through freedom of information requests
3. Harm to sound management and administration of government due to failure to document processes, deliberations and actions (the risk of unrecorded or lost corporate knowledge, experience and learning from mistakes and successes)
4. Litigation risk flowing from government not being able to rely on proper documentation to demonstrate lawful actions and decisions, unnecessarily exposing it to damages and judicial censure
5. Government not being able to rely on proper documentation in response to internal or external audits, exposing government to censure by auditors
6. Loss to the historical record because documents do not exist that have archival and historical importance (with links to the immediately preceding risk)
7. Loss of public confidence in government over time due to the perception that the absence of documentation reflects a deliberate tactic to hide, among other things, wrongdoing (including corruption or favouritism).

Building on this, many authoritative sources have commented on the benefits of good record-keeping. For example, the Office of the Chief Information Officer for Queensland observes that record keeping "should be a systematic part of the essential business activities of all public authorities." [80] The perspective of the United States National Archives and Records Administration is that "the practice of ensuring 'adequate and proper documentation' contributes to efficient and economical agency operations by guaranteeing that information is documented in official files, including electronic recordkeeping systems, where it will be accessible to all authorized staff who may need it."[81] In Canada, federal Treasury Board policy speaks to creation of records and the reasons for doing so. The Treasury Board Directive on Recordkeeping requires each department to:

[80] Chief Information Office, Queensland Government: http://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2357-recordkeeping-is40 (accessed December 4, 2015).

[81] 'Agency Recordkeeping Requirements: A Management Guide' (National Archives and Records Administration Management Guide Series 1995). http://www.archives.gov/records-mgmt/policy/agency-recordkeeping-requirements.html (accessed December 4, 2015). This guidance assists federal agencies with creating record-keeping policies and practices suited to their agency. They have a legal duty to create records by virtue of 44 U.S.C. §3101: "The head of each federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities."

> 5.1.1 Ensure effective recordkeeping practices that enable departments to create, acquire, capture, manage and protect the integrity of information resources of business value in the delivery of Government of Canada programs and services. [82]

The following excerpts from the Directive on Recordkeeping elaborate on the policy objectives of documentation:

> 3.1 Recordkeeping is a resource management function through which information resources of business value are created, acquired, captured, managed in departmental repositories and used as a strategic asset to support effective decision making and facilitate ongoing operations and the delivery of programs and services.
>
> 3.2 As a core resource management function within the Government of Canada, effective recordkeeping enables departments to manage their ongoing operations, deliver programs and services, and ensure key departmental capacities for accountability, stewardship, evaluation, audit, access to information, privacy, security and policy compliance.
>
> 3.3 Information resources of business value include published and unpublished materials, regardless of medium or form, that are created or acquired because they enable decision making and the delivery of programs, services and ongoing operations, and support departmental reporting, performance and accountability requirements. An information resource identified as having business value and placed into a repository enables effective decision making and provides reliable evidence of business decisions, activities and transactions, for program managers, deputy heads, ministers, and Canadian citizens.

The Treasury Board's Policy on Information Management further underpins the federal policy, by making the deputy minister of each department responsible for "ensuring that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of the evolution of policies and programs, and allow for independent evaluation, audit, and review."[83]

Somewhat similar principles are already enshrined in the government's own Core Policy and Procedures Manual, which states the following over-arching principles:

> 12.2.1 Information management is a core component of government infrastructure; it is the intellectual capital of responsible governance. Best practice policies and standards

[82] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16552 (accessed December 4, 2015).
[83] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742&section=text#cha5 (accessed December 4, 2015).

> result in efficient, accountable and cost-effective use of resources. Information technology constitutes the full spectrum of technologies and services that support information management.[84]

In a similar vein, existing government policy recognizes the importance of managing, preserving, providing access to and disposing of those records that do exist in order to:

- ensure government accountability;
- provide evidence of its activities and organizational structure;
- document its responsibilities, rights and entitlements; and
- preserve records of enduring value.[85]

It is also now British Columbia government policy to "[c]reate and retain a full and accurate record documenting decisions and actions".[86] What does not exist is a duty—whether created by policy or law—to create records.

Implementation of a duty to document will have some resource and operational implications for government and these should be assessed. The following are some considerations government should consider:

1. Implementation would involve major policy work across government. Significant consultation and preparation would be needed with ministries to identify, plan and implement changes in policy and practice. There would be significant planning and change-management costs.
2. To give one example, such a direction could require possibly significant changes to the existing government records classifications systems, ARCS and ORCS, as well as the Core Policy and Procedure Manual.
3. Longer-term, the necessary policy changes would drive operational changes and resource needs. The need to record whatever matters law and policy stipulate—*i.e.*, the specified 'deliberations', 'meetings', 'actions', 'decisions', and so on, however defined—is likely to have implications for staffing numbers. The scale of this would, naturally, depend on what law and policy demand.
4. There would be implications for information management. There would be no point creating new kinds of records if they are not managed properly. This is also likely to have staffing

[84] BC Government 'Core Policy & Procedures Manual'. http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#
[85] *Ibid*, section 12.3.3, Part III.
[86] *Ibid*, section 12.3.3, Part III. http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm# (accessed December 5, 2015).

implications because more information managers might be needed to manage the increased volumes and kinds of records.

5. The costs of storing and retrieving records could possible increase as a result of new kinds and larger volumes of documentation (or they might not, since the rules that are adopted will determine whether this is the case, noting that the rules could in fact rationalize and reduce the volume of records created).[87]

Yet the fact remains that, if key actions and decisions are not documented, risks arise and these can have significant consequences in a given case, or create risks to the public interest overall.

Nor is it the case that a duty to document would necessarily require a sea change in practice. Government is likely, when it assesses the matter, to discover that existing legislation or policy either expressly or implicitly require or provide incentives for creation of an array of records. To give only one example, the *Financial Administration Act*, the *Budget Transparency and Accountability Act*, and government's adherence to GAAP, either expressly or in practice lead to creation of a wide range of financial and fiscal records already. Good administrative practice, and protection from legal liability, also undoubtedly result in creation of many kinds of records. A duty to document, therefore, may to some extent overlap with what is already being done. Creating a duty to document would provide a foundation, and guidance, for existing practices, while ensuring that appropriate records are created where that is not the case under current law, policy or practice.

In considering legislating a duty to document, government should keep in mind that its policy objectives indisputably invoke many important public interests. These include, of course, government openness and accountability, with freedom of information being vital to those things. A key consideration, in the context of this report, is that the duty to document would enhance openness through access to information, in turn enhancing citizens' ability to hold government to account. Government should also account for the other important public interests mentioned earlier, which could be advanced by an appropriately fashioned duty to document.

In this light, government should give the most serious consideration to Commissioner Denham's recommendation that a duty to document be created. Specifically, it should seriously consider introducing legislation[88] creating such a duty (with the details being worked out in policy at a

[87] Moreover, even if there is an increase in the costs of storing and retrieving records, the public interest benefits of improved documentation weigh significantly in the balance.

[88] It is recognized that government could achieve the policy objectives of such a duty through policy, not legislation. Government policy already requires the creation and retention of a full and accurate record documenting decisions and actions. Further policy could be developed ministry by ministry.

ministry, even program, level). Government should consider adopting a risk-based approach, with the nature and significance of decisions, actions and transactions being used to determine which records have to be created and in what manner.

The guiding principles issued by the State Archivist of Queensland to assist state institutions in complying with their legislated duty to document can be of assistance in fashioning legislation and agency-by-agency policy:

1. Public authority recordkeeping must be compliant and accountable
2. Recordkeeping must be monitored and audited for compliance
3. Recordkeeping activity must be assigned and implemented
4. Recordkeeping must be managed
5. Recordkeeping systems must be reliable and secure
6. Recordkeeping must be systematic and comprehensive
7. Full and accurate records must be made and kept for as long as they are required for business, legislative, accountability and cultural purposes.[89]

Last, government should, in any event, as soon as practicable remind public servants that it is existing government policy to create and retain full and accurate records documenting decisions and actions. This should be done at the same time as the interim guidance mentioned elsewhere in this report.

PRACTICE REVIEW FOR RECORDS MANAGEMENT PROCESSES

Under the *Information Management Act*, the head of each government body will have a variety of duties, including the already-noted duty to ensure government information is disposed of only in accordance with information schedules. Each head will also be "responsible for ensuring that an appropriate system is in place" in that body "for managing and securing government information." The head will also be required to "take reasonable steps" to ensure compliance with information schedules.[90]

This de-centralized approach to information management compliance is realistic. It reflects the fact that each government body has different information holdings, statutory mandates and operational context. Each is therefore best placed to implement appropriate systems for

[89] In this respect, the guiding principles issued by the State Archivist of Queensland for fashioning, agency by agency, appropriate policies to implement the duty to document are worth serious study.
[90] Section 19, *Information Management Act*.

managing information and to decide what reasonable steps are needed to ensure compliance with central direction through information schedules.

There is, however, undoubtedly a need for compliance oversight, quality control and continuous improvement processes. The *Information Management Act* can enable this. The government's chief records officer will be responsible for promoting the "preservation of valuable government information for current and future use" and promoting "effective information management by government bodies."[91] The minister responsible will be authorized to establish an information management advisory committee to advise the chief records officer in relation to approval of information schedules.[92]

Government should ensure that the information management advisory committee has a broader role than this. It should have an advisory mandate to ensure that government information management policies and practices continue to meet accepted good practice, and improve over time, as technologies and government programs evolve. To help ensure public confidence in the committee's work, government should ensure that it includes experts from outside government who have expertise in records management, archives and government administration.

Government also should ensure that the chief records officer establishes guidance on information management systems in order to assist ministries in achieving early compliance with their *Information Management Act* duties. Guidance should also be established on the steps heads should take to ensure compliance with information schedules.

Further, government should ensure that GRS establishes a program of regular (and spot) review of information management practices in individual ministries. GRS staff would examine the practices of a ministry and make any necessary recommendations for improvement.[93] Each report should be provided to the information management advisory committee for review and any recommendations. The committee should also be mandated to ensure that these practice reviews inform ongoing practice improvement.

It is also recommended that the committee have a web presence through GRS. Practice review reports, and committee input, should be published. The committee should be required to report

[91] *Information Management Act*, ss. 3(a) and (d).
[92] *Information Management Act*, s. 4(4).
[93] Under s. 7 of the *Information Management Act*, the chief records officer will have the power to require the head of a government body to provide information about its information management. This authority should be used for the practice review program recommended here.

annually to the minister, who should make each report publicly available, such as by tabling it in the Legislative Assembly.

TRAINING AND GUIDANCE

A number of areas have been identified where government should enhance training and guidance for public servants. These are consolidated in this section. It should be underscored that it is out of scope to actually craft training and guidance materials. In any case, it is not possible to do this if government accepts the above recommendation to consolidate and update its transitory records policy.

As a first step, there is a clear need for interim guidance to all public servants on records management and freedom of information issues addressed in the investigation report. These are questions of compliance with the law. The duty to assist is, after all, a legal duty, not mere policy. The existing transitory records rules are policy, not law, but those rules are, as the investigation report illustrates, intimately linked with the legal duty to assist and FIPPA compliance.

As soon as practicable, therefore, all public servants should be reminded of, and given specific guidance on, the duty to assist in searching for records and in interpreting access requests. The same recommendation applies for transitory records policy. It would be desirable for the head of the public service to deliver this guidance, although the Deputy Attorney General, as the deputy of the chief law officer to the Crown, could do this. Whoever does this, government should at the earliest opportunity broadcast to all public servants a written reminder, and supportive guidance, on these two issues.

Regarding ongoing training, government acknowledged during preparation of this report that it does not have an integrated approach to training on freedom of information and records management. Training in each area is done separately. So is privacy training. As this report shows, there is a close link between records management and freedom of information compliance duties in the areas of duty to assist and transitory records. Integration of training in these two key areas is therefore recommended.

Existing records management training

GRS delivers records management training across government. It has three full-time positions for this, with staff from the branch or clients sometimes assisting. Training materials are developed by GRS. Training is presented in-person in Victoria in a dedicated classroom, and in ministry facilities around the province. Training is also done using video and conference calls.

GRS advised that it has on average delivered 151 sessions each year over the last five years. Ministry records officers, who are GRS staff, also provide training on request by client ministries. They also act as expert resources for client ministries and can answer staff questions.

Two basic modules are treated as prerequisites to a number of other courses. These are Managing Our Information Assets (IM110) and Managing Government Records (IM112). As government acknowledged during preparation of this report, these modules require updating to anticipate the *Information Management Act*, but also to better address issues associated with management of digital information.

While privacy training is mandatory for all government employees, it is not mandatory for records management. Not all employees need to be records managers, of course, but some level of records management training should be mandatory. A key focus should be on transitory records policy, with practical guidance on the topic. Essential areas for training are management of email and draft records. GRS already has a number of useful guides on email management and draft records on its website. These could be incorporated into the training materials. This is an opportune time for GRS to revamp existing materials in light of the *Information Management Act* in any case. This training should be an online orientation module for new employees. Existing employees should also be required to complete the module.

Freedom of information training

A variety of programs are delivered to educate public servants about freedom of information. As noted earlier, these materials include brief mention of the duty to assist, and at least one module includes a slide on transitory records. It is recommended that a single set of materials be prepared for freedom of information training courses, and the duty to assist and transitory records portions should be substantially enhanced. The duty to assist portion should relate to searches for records and also interpretation of requests.

Training for ministerial staff and Premier's office staff

As indicated earlier, all ministerial staff have received access and privacy training since 2013. This should, however, be made mandatory. The training should use the integrated records management and freedom of information module recommended above. The Premier's office should be responsible for ensuring that all staff complete the training in a timely way. Staff should be required to repeat the training at least every two years.

SUMMARY OF RECOMMENDATIONS

This section summarizes the recommendations earlier in this report. Reference should be had to the discussion of each recommendation in order to best understand what is intended. As will be noted, a number of recommendations below respond to more than one of Commissioner Denham's recommendations.

It has not been necessary to make recommendations in response to Commissioner Denham's recommendation 1 (MOTI should respond to the access request in question) or recommendation 3 (AVED should respond to the access request in question). Government has advised that it has responded to both of these requests, thus fulfilling both of these recommendations.

The following summarizes the recommendations made earlier in this report, mapped against Commissioner Denham's recommendations. The blue text in italics and square brackets indicates which of Commissioner Denham's recommendations are addressed by each of the following recommendations.

1. Government should devise, and implement, a plan to ensure that during any future data migrations, email accounts are backed up as recommended by Commissioner Denham. *[Commissioner Denham's recommendation 2 (data migration plan and execution).]*

2. It is recommended in the strongest possible terms that government resist any notion that all emails should be kept, or that they should all be kept in order to be vetted by archivists or records managers, who would decide which to keep. The prudent approach is to ensure that government's transitory records policy is appropriate, understood by all, and implemented by all. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

3. Government needs to ensure that all ministries have the expert resources in-house necessary to ensure every reasonable effort is made to locate records in response to access requests. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records).]*

4. Government should improve its training materials, and guidance resources, to provide better education and support for front-line staff searching for records. The materials and guidance should inform all staff about the policy objectives of the duty to assist, the test for search efforts expected of public bodies, and practical steps they can take to help meet the duty.

Employees should be given guidance on typical steps for finding records, such as tips on how to search their email accounts. These materials should also underscore the importance of documenting all steps taken to search for records, with specific guidance on what is expected in terms of documentation. *[Commissioner Denham's recommendations 5 (clarify access requests), 6 (guidance on searching for records).]*

5. IAO should ensure it continues to watch for cases where it has reason to believe records should exist, yet none are produced to it. In such instances, IAO should rapidly escalate the matter to obtain appropriate direction. This should ideally come from the deputy minister for the ministry involved (or her or his immediate delegate). Government should create policy to govern such cases. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

6. Where an executive branch office does not have responsive records due to ordinary-course records management, IAO should explain why that is so. It should confirm that the ministry's records were searched and any responsive records are included in the release package. Government also should enhance public understanding by publishing information about how records management is handled as between ministries, ministers' offices and the Premier's office. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

7. Government should issue a rule prohibiting anyone from triple deleting emails. It should also configure its email system so that the contents of the recover deleted items folders in all mailboxes are, as recommended by Commissioner Denham, retained for 31 days, not 14 days. Government also should dedicate effort and resources to the other associated policy and practice changes recommended elsewhere in this report. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records), recommendation 10 (retaining recover deleted items folder contents for just over one month).]*

8. Government should work with Commissioner Denham and with Microsoft to ensure that all mailbox content, including deleted emails, is preserved for 13 months for legal purposes. Solutions to this might, subject to technical confirmation, include configuring government's Microsoft Exchange servers to implement a time-based in-place hold on all email mailboxes. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's*

office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records), recommendation 9 (configuring Microsoft Outlook to prevent triple deletion of emails).]

9. Government should change the process for handling access requests in ministers' offices by adopting the following procedures: *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

   (a) Each minister's office should be required to designate a career public servant as the person in charge of request processing within the office. The position of senior executive assistant is an example. The goal is to ensure that political staff involved in the day-to-day hurly-burly of political work are not in charge of searches for records.

   (b) Whenever IAO receives a request that requires the records of a ministerial office to be searched, the designated staff person in the minister's office should be responsible for contacting all staff directly, in writing (for example, by email), setting out the wording of the request and directing that staff search for responsive records and respond in a set time.

   (c) These emails should include clear direction on searching for records (and should underscore the duty to provide a complete and accurate response).

   (d) Each member of the minister's staff should be required to respond directly to the assigned staff member, reporting in writing on the search and sending responsive records directly to the assigned staff member, who will then send them to IAO.

   (e) If any member of a minister's staff has questions about the scope of a request, or about whether a record is responsive, those questions should be directed in writing to IAO. IAO should have the final say on how the request is to be interpreted.

   (f) IAO should be required to report any failure by a ministerial staff member to respond or any failure to co-operate with IAO. This report should be made to the Premier's chief of staff and to the deputy minister for the ministry.

   (g) Each minister's office should be required to ensure that IAO at all times has a current list, with contact particulars, for all staff in the office.

(h) IAO should be authorized to, where it considers it necessary in a given case or on an *ad hoc* basis, have access without notice to ministerial office files for the purpose of ensuring that all responsive records have been identified and produced to IAO. This includes the government email accounts, but not personal emails in them, of ministerial staff.

(i) Rules will be needed to ensure there is no collection of constituency records of a minister (as opposed to ministerial records, *i.e.*, records of the ministry as a public body).

10. Government should take the following measures to enhance training for political staff in ministers' offices: *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

(a) Training should be mandatory for all new ministerial staff. Each time someone is hired, that individual should be required, during orientation, to take access and privacy training.

(b) The training should be done by IAO on an in-person basis, in groups if necessary.

(c) Existing training materials should be significantly enhanced in the areas of the duty to assist and records management (notably regarding transitory records, discussed below).

(d) As further described below, the materials should be designed to help ensure that staff understand and comply with the duty to assist. Another goal is to ensure appropriate practices in relation to transitory records. A third goal is to ensure a sufficient understanding of records management rules and practices. This is also important for the proper management of records other than emails.

(e) Reference materials, or guidance, on all of these matters should be provided to ministerial staff for their reference.

(f) Staff should be made aware of IAO's contact centre number, so they can reach out with any compliance questions.

(g) The director of executive operations in the Premier's office should be responsible for ensuring that training is performed and for keeping records of this.

(h) Ministerial staff should be required to take refresher training periodically, at least every two years.

11. Regarding the guidance materials for ministerial staff on interpreting requests and searching for records, new materials should be created to ensure that existing (and new) ministerial staff have a proper understanding of what is expected of them. This guidance material can align with the guidance material recommended below for public servants. The material should also, however, make it clear to ministerial staff that the minister's office is part of the ministry as a public body and is not exempt from FIPPA. The guidance should also address constituency records of the minister in her or his role as a member of the Legislative Assembly, since these are not generally considered to be ministry records for FIPPA purposes. This will help staff understand where the lines are drawn. Last, the guidance should help staff understand that personal email accounts are not to be used for government business and, if they nonetheless are, that these records are not excluded from FIPPA and must be produced for request-processing purposes. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

12. The recommendations for training for ministerial staff should also apply to staff in the Premier's office. On this point, as noted at the outset of this report, the terms of reference contemplate providing training to staff in both ministers' offices and the Premier's office as early as practicable in 2016. This should be done *after* the enhanced training materials are prepared, which should be done as soon as practicable. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

13. Political staff who are employed in ministers' offices are appointed under the *Public Service Act*. This means they are subject to government policies on acceptable use of technology and on records management. They are also subject to a code of conduct for political staff. They should be required to certify in writing that they are aware of their responsibilities under FIPPA, including the duty to assist, and are aware of applicable records management policies and rules, particularly those relating to transitory records. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

14. Regarding searches for records within the Premier's office, the above recommendations about IAO authority and access to records in a minister's office should be implemented in relation to the Premier's office. So should the recommendations about FIPPA and records management training for political staff in the Premier's office, and their agreement to be

bound by records management rules. *[Commissioner Denham's recommendations 4 (improve request processing in the Premier's office), 5 (clarify access requests), 6 (guidance on searching for records), 7 (records management training on transitory records).]*

15. Government should significantly update and enhance its transitory records policy, notably in relation to emails, in light of the detailed recommendations made above in this respect. This should include a purpose statement recognizing the need for government to create records of key activities and decisions and retain them in accordance with its records management system. *[Commissioner Denham's recommendation 7 (records management training on transitory records), 8 (oversight above of records management).]*

16. Guidance on transitory records policy will have to be updated to support the new transitory records policy. The Government Records Service should also regularly review and update guidance to keep abreast of new issues, new types of information and new information systems in government. Updates should be informed by users' experience, through an effective feedback loop to inform guidance on transitory records. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

17. Government should give serious consideration to introducing legislation, consistent with s. 53 of the Alberta *Freedom of Information and Protection of Privacy Act*, that would give the Information and Privacy Commissioner authority to investigate alleged unauthorized destruction of records. *[Commissioner Denham's recommendation 8 (oversight above of records management).]*

18. Government should make such policy and practice changes as are necessary to ensure that any employee appointed under the *Public Service Act* who destroys a record, or directs or assists anyone else in doing so, with the intent to evade a request for access to the record is subject to discipline up to and including dismissal for cause. Second, government should also give serious consideration to introducing legislation, consistent with s. 92(1) of the Alberta *Freedom of Information and Protection of Privacy Act*, that would make it an offence to wilfully destroy a record, or direct or assist anyone else in doing so, with the intent to evade a request for access to the record. *[Commissioner Denham's recommendation 8 (oversight of records management).]*

19. Government should give the most serious consideration to Commissioner Denham's recommendation that a duty to document be created, specifically, it should seriously consider

introducing legislation[94] creating such a duty (with the details being worked out in policy at a ministry, even program, level). Government should consider adopting a risk-based approach, with the nature and significance of decisions, actions and transactions being used to determine which records have to be documented and in what manner. *[Commissioner Denham's recommendation 11 (create a duty to document).]*

20. As regards respondent practice review and improvement, government should ensure that the information management advisory committee established under the *Information Management Act* has an advisory mandate to ensure that government information management policies and practices continue to meet accepted good practice, and improve over time, as technologies and government programs evolve. To help ensure public confidence in the committee's work, government should ensure that it includes experts from outside government who have expertise in records management, archives and government administration. *[Commissioner Denham's recommendation 7 (records management training on transitory records), 8 (oversight above of records management).]*

21. Government also should ensure that the chief records officer under the *Information Management Act* establishes guidance on information management systems in order to assist ministries in achieving early compliance with their *Information Management Act* duties. Guidance should also be established on the steps heads should take to ensure compliance with information schedules. *[Commissioner Denham's recommendation 7 (records management training on transitory records), 8 (oversight above of records management).]*

22. Further, government should ensure that GRS establishes a program of regular (and spot) review of information management practices in individual ministries. GRS staff would examine the practices of a ministry and make any necessary recommendations for improvement. Each report should be provided to the information management advisory committee for review and any recommendations. The committee should also be mandated to ensure that these practice reviews inform ongoing practice improvement. *[Commissioner Denham's recommendation 7 (records management training on transitory records), 8 (oversight above of records management).]*

23. It is also recommended that the committee have a web presence through GRS. Practice review reports, and committee input, should be published. The committee should be required to report annually to the minister, who should make each report publicly available,

[94] It is recognized that government could achieve the policy objectives of such a duty through policy, not legislation. Government policy already requires the creation and retention of a full and accurate record documenting decisions and actions. Further policy could be developed ministry by ministry.

such as by tabling it in the Legislative Assembly. *[Commissioner Denham's recommendation 7 (records management training on transitory records), 8 (oversight above of records management).]*

24. There is a clear need for interim guidance to all public servants on records management and freedom of information issues addressed in the investigation report. As soon as practicable, therefore, all public servants should be reminded of, and given specific guidance on, the duty to assist in searching for records and in interpreting access requests. The same recommendation applies for transitory records policy. It would be desirable for the head of the public service to deliver this guidance, although the Deputy Attorney General, as the deputy of the chief law officer to the Crown, could do this. Whoever does this, government should at the earliest opportunity broadcast to all public servants a written reminder, and supportive guidance, on these two issues. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

25. Not all employees need to be records managers, but some level of records management training should be mandatory. A key focus should be on transitory records policy, with practical guidance on the topic. Essential areas for training are management of email and draft records. The Government Records Service has a number of useful guides on email management and draft records on its website and these could be incorporated into the training materials. This is also, nonetheless, an opportune time for the Government Records Service to revamp existing materials in light of the *Information Management Act*. This training should be an online orientation module for new employees. Existing employees should also be required to complete the module. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

26. It is recommended that a single set of materials be prepared for freedom of information training courses and the duty to assist and transitory records portions should be substantially improved. The duty to assist portion should relate to searches for records and also interpretation of requests. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

27. All ministerial staff should be required to have access and privacy training, along with a records management aspect. The training should use the integrated records management and freedom of information module recommended above. The Premier's office should be responsible for ensuring that all staff complete the training in a timely way. Staff should be required to repeat the training at least every two years. *[Commissioner Denham's recommendation 7 (records management training on transitory records).]*

CONCLUSION

The goal of this report is to advise government on how best to implement recommendations made by Commissioner Denham in her investigation report. Government has the opportunity to seize the initiative and demonstrate, through specific actions recommended here, commitment to openness and accountability.

***