As Strong as its Strongest Link: A Critique of the Policy Framework Governing Federal Agency Recordkeeping in Canada

Ian McAndrew

Paper submitted for InterPARES student essay competition
30 April 2001

As the conclusion of the InterPARES Project approaches, Project researchers are beginning to assess the results of their findings to date with reference to existing national and international standards on recordkeeping and records management. The purpose of this essay is to support the work involved in this final stage of the research by presenting a critical review of records management policies of the federal government of Canada. It begins by sketching a portrait of the overall regulatory framework currently governing agency recordkeeping. Proceeding from here, the analysis evaluates the instruments in the framework by comparing them with the latest version of the Authenticity Task Force's "Benchmark Requirements that Support the Presumption of Authenticity of Electronic Records." The overall argument holds that it will be necessary to introduce substantial revisions to the federal recordkeeping regime if the principles underlying the Draft Requirements are to be incorporated into it. Moreover, this essay concludes that regardless of whether policy-makers choose to bring regulations into line with InterPARES recommendations, comprehensive reform should be undertaken.[1]

Introduction to the Canadian Records Management Policy Framework

The primary statute dealing with government recordkeeping in Canada is the *National Archives of Canada Act* [*NAC Act*]. This law, in its pertinent sections, assigns to the National Archivist responsibility for "facilitat[ing]" records management, and "advis[ing] government institutions concerning standards and procedures pertaining to the management of records." Note that this facilitative and advisory role includes power to establish "guidelines" on best practices for recordkeeping, but that the Archivist does not posses authority to issue "regulations" in the official sense.[2]

Below the *NAC Act*, the most authoritative recordkeeping rules are those contained in the *Treasury Board Administrative Policy Manual*, and particularly those in the "Management of Government Information Holdings" chapter [MGIH]. However, while this document is reputed to be the main government recordkeeping policy, it is almost entirely silent on records management *per se*. As its title suggests, the MGIH is an information management policy statement, and in fact it contains no stipulations directly related to recordkeeping other than two brief clauses: one directing government institutions to "ensure that records of enduring value which document the evolution of government policies, programs and major decisions are maintained;" and another mandating that they "identify and document projects, programs and policies sufficiently to ensure continuity in the management of government institutions and the preservation of a historical record." Furthermore, since most other passages of the *Treasury Board Manual* are similarly vague, the only chapter that comes under consideration here is that containing the "Information Technology Security Standard" [ITSS].[3]

As a result of this high degree of abstraction in instruments at the top level of the regulatory hierarchy, this analysis focuses on policy documents at the level of the common service organizations [CSOs]. These include, for example, the RCMP *Technical Security Standard for Information Technology* [*TSSIT*], and various documents issued by the Information Management Forum [IMF] and the National Archives of Canada [NAC]. In one instance a departmental policy is introduced for assessment, although generally speaking instruments at this level are beyond the scope of this research.[4]

InterPARES Benchmark Requirements and the Canadian Federal Framework

The latest version of the InterPARES Draft Requirements, written in April 2001, is intended to provide organizations with a set of benchmarks against which recordkeeping systems may be evaluated. The methodology behind the analysis presented here also involves benchmarking, although in a somewhat different sense. The following passages examine each Draft Requirement in succession, and in comparison with the documents that comprise the regulatory framework. The main purpose is to locate the aspect or aspects of government policy that most closely relate to each individual requirement, and to determine the extent to which the policy plank in question could serve as a substitute for the requirement in question. At the end, a portrait of the overall recordkeeping regime will emerge; depending on how many close matches between policy and requirement can be located, it will be possible to determine whether the existing framework is either more or less compliant with the principles and practices the Authenticity Task Force [ATF] recommends to support a presumption of authenticity.[5]

Draft Requirement 1: Draft Requirement 1 establishes that the presumption of authenticity will be stronger if the creator has inextricably linked to the record the essential metadata elements that attest to its identity and integrity. There are two main Canadian government sources dealing with metadata capture. First, the IMF guideline entitled *Record Keeping Metadata Requirements for the Government of Canada* lists a set of elements that, to an extent, match those found in Draft Requirement 1. The list includes most of the sub-elements under the InterPARES "persons" category, as well as counterparts for "action or matter," "expression of archival bond," "annotations," "technical modifications," and some relevant "dates." However, the document fails to address certain important issues. Mainly, its drafters did not require that the elements be inextricably linked to the record, and they neglected to explain the intended purpose for metadata capture. [6]

1. the creator has ensured the following attributes are inextricably linked to every record. These attributes can be distinguished into categories, one concerning the identity of records, and one concerning integrity of records.

a) identity of the record:
- i) Persons (that is, author, writer, addressee, originator)
- ii) Action or Matter
- iii) Dates (that is, of the document, archival and transmission)
- iv) Expression of archival bond (for example, classification code, file identifier)
- v) Status of transmission (that is, draft, original, copy)
- vi) Attachments

b) integrity of the record:
- i) Handling office
- ii) Office of primary responsibility (if different from handling office)
- iii) Annotations
- iv) Technical modifications

The second guideline relevant in this instance is the *Records/Document/Information Management (RDIM): Software Requirements*.[7] While certain InterPARES fields have no counterparts in the RDIMS policy statement, and while the document is particularly weak in the "persons" category, it does provide reasonable matches for "Originator," "Action or Matter," most “Dates,” “Expression of Archival Bond,” “Attachments,” and to an extent “Status of Transmission.” Furthermore, the *RDIMS Requirements* mandates use of record or document profiles, creates rules to deal with their disposition, and allows for profiling of non-electronic records. On the other hand, though, RDIMS officials did not require anything stronger than a “link” to bind record and profile, and, as with the IMF, they have not clearly articulated why agencies must retain the specified metadata fields.[8]

It is important to note that while neither of these guidelines clearly states the purpose for metadata capture, there is some evidence of what their authors had in mind. The RDIMS officials, first, indicated their views by stating that “the following list of profile fields are examples of fields that may be required to be able to identify/retrieve an object.” Drafters of the IMF policy made no statement as direct as this, but they did hint at a similar attitude by offering their product as an alternative to certain other metadata sets that have been designed overtly to serve retrieval purposes. At very least, then, it seems fair to say that neither of these instruments requires metadata capture primarily to protect authenticity, and it may also be warranted to conclude that both instruments treat metadata exclusively as a retrieval tool. Whichever is the case, policies in this instance only match the requirement incidentally because the former were designed for purposes significantly different from those on which the latter is based.[9]

2. the creator has defined and effectively implemented access controls over the creation, modification, annotation, relocation, and destruction of records.
3. the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records.

Draft Requirements 2 and 3: The intent behind Draft Requirements 2 and 3 is to make clear that a presumption of authenticity is strengthened when evidence can be found that the creator took steps to ensure security of its electronic system, and of the data and records in it. There are two documents particularly relevant to security. At the highest level, there is the Treasury Board Secretariat’s [TBS] “Information Technology Security Standard.” This instrument requires, among other things, use of access privileges, implementation of “environmental safeguards to protect IT systems from such threats as water, humidity, smoke and fire," and use of software with capacity for "management, audit controls, logging, labeling, isolation, system recovery, and integrity verification techniques." The ITSS, then, mandates several of the methods the ATF has identified for satisfying Draft Requirements 2 and 3. However, the policy does not specifically state that access controls serve the purpose of preventing unauthorized actions to records, nor that audit trails, system recovery, and other means must exist to guard against loss and corruption of records. Thereby, TBS officials appear to have overlooked the connection between security measures and the need to guard authenticity.[10]

The RCMP *TSSIT*, in the second place, was designed to supplement the ITSS by translating the principles it establishes into detailed specifications for system, data, and records security. This document requires agencies to implement particular system configurations and operating procedures to ensure that "access control systems [are designed] with an evaluated level of trust appropriate to the sensitivity of the data;" that audit trails that log all "security-relevant events" including events as specific as each "user sign-on and sign-off;" and that sufficient "Software Library Control" exists to allow system reconstruction in the event of disaster. In addition, the *TSSIT* issues directives relevant to several other matters in considerable detail, including, for instance, stipulations that "data [must] be recover[able] automatically or with the assistance of the data originator following computer crashes," and that system back-up must allow "full recover[y], taking into account the length of time an error may remain undetected." Note, finally, that the RCMP security policy resembles that of the TBS in that it also neglects to make a connection between the methods it prescribes—access privileges, back-up and recovery specifications, and so on—and authenticity.[11]

Taken together, the ITSS and the *TSSIT* comprise a fairly stringent standard for system and data security. On the other hand, though, it seems that both TBS and RCMP officials have a restrictive understanding of the purposes served by security policies—concentrating almost exclusively on confidentiality of sensitive information. The statement of purpose that introduces the *TSSIT*, for example, explains that the document is "intended to assist departments in achieving a minimum level of security for classified and designated information and assets." Once again in this instance, then, the resemblance between policy and requirements is incidental. The documents prescribe several of the methods for satisfying Draft Requirements 2 and 3. However, there is no indication that their authors were aware that security also supports a presumption of authenticity.[12]

Draft Requirement 4: The fourth Draft Requirement stipulates that the presumption of authenticity will be stronger if the creator has implemented procedures to minimize or prevent loss of record identity and integrity when record components are introduced to new hardware or software environments. To fulfill this requirement the ATF reccommends, among other means, advance planning for system upgrade, procedures determining when records must be migrated, and procedures requiring full documentation of elements lost in the migration process.

4. the creator has established and implemented procedures to guarantee the continuing identity and integrity of records across technological change.

It appears that the only location where the terms of Draft Requirement 4 are addressed is in the *RDIMS Requirements* document, which dictates that systems must

> permit conversion of objects to newer versions of the native software (preferably automatically converted upon upgrading) as well as to different software (preferably automatically converted upon opening). The software may retain the objects in their native format and software version, with an option to convert, as long as they maintain readability and editability. … The preferred approach is to automatically convert the objects, as required, when the native software is upgraded.

This passage, while requiring that certain plans be put in place to safeguard "objects" across technological change, is notably lacking in that it concentrates on readability and editability. Nothing, by contrast, requires that attention be paid to ensuring continuing identity and integrity. The focus, in other words, is not on guaranteeing authenticity of records and documents, but on providing that they will still be serviceable, or usable, after migration.[13]

Aside from this document, federal policies overlook not only the authenticity questions involved with technological change, but in fact they avoid addressing technological change in general. The MGIH, for instance, makes no statement on the need to plan for system upgrade at all, and the "Management of Information Technology" policy requires only that agencies "use government standards … for new applications involving the exchange of information with outside organizations." This represents a considerable problem, and not only in that it is another case in which authenticity concerns are marginalized. More basically, it also demonstrates that policy-makers are reluctant to face the fact that implementing an "information revolution" will require continuous funding, not merely start-up costs. The unrealistic view of budgetary issues suggested by oversights in this area indicates that government planners may have overly optimistic ideas about the feasibility of their plans for "renewing government" through use of technology.[14]

Draft Requirement 5: According to Draft Requirement 5, a presumption of record authenticity can be strengthened if the creator has established specific documentary forms for records associated with various procedures undertaken in the course of its business. The criteria determining conditions under which form is prescribed may be imposed from external sources, or they may result from the creator's own definition of its needs. In either event, however, the presumption is strengthened because evidence that the creator has undertaken the activity of forms management in this respect suggests that business and documentary procedures are, to a greater or lesser extent, controlled and integrated.

5. the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical

Counterparts to Draft Requirement 5 are absent from the Canadian government recordkeeping regime. Until the 1980s, a *Treasury Board Manual* chapter devoted entirely to "Forms Management" existed. This was repealed, however, when several disparate and relatively unrelated TBS regulations were amalgamated into the MGIH in 1989. This new *Information*

Holdings policy does treat the topic in some measure, although its scope is restricted to matters such as bilingualism in forms management and “standardiz[ation] and reduc[tion] of the response burden” for citizens. At its most specific, the MGIH explains that

> institutions must control their creation and use of forms, regardless of the media in which they appear, and review such forms for conformity with all statutory and government policy requirements prior to the implementation of any information collection. … Institutions should try to eliminate duplication, improve consistency in data collected and reduce costs by consolidation.[15]

This is yet another instance in which policy could and should take authenticity into account, but instead devotes exclusive attention to issues that are tangentially related to records management at best. There is nothing wrong with addressing response burden, cost reduction, and the like, of course. In this case, however, these topics are treated to the exclusion of other important interests.

6. if authentication is required by the juridical system or the needs of the organization, the creator must have specific rules regarding which records must be authenticated, by whom, and the means of authentication.

Draft Requirement 6: The sixth Draft Requirement, and those that follow, state conditions that must be met by the creator only if certain contingencies exist. In this case, applicable to situations in which the creator must authenticate records, the appraiser’s presumption of authenticity is strengthened if rules determine the circumstances in which the process is required, and if procedures govern its execution. In this context it is important to note that InterPARES defines the term “authentication” as “a declaration of authenticity that occurs by inserting or adding an element that allows one to verify that the record is what it purports to be at that point in time.”[16]

As with Draft Requirement 5, no regulatory instruments adequately deal with this issue. The MGIH and its related policies do not touch on authentication, nor do *Treasury Board Manual* chapters dealing with “Access to Information.” The silence of these latter regulations is particularly surprising since it is entirely foreseeable that some citizens making requests under the *Access to Information Act* would have a need for copies certified to be authentic. Admittedly, some documents associated with the Canadian Public Key Infrastructure [PKI] initiative appear to be relevant to Draft Requirement 6. However, the PKI definition of authentication focuses on verification of the authority of a digital signature, and does not touch on authenticity of records.[17]

Draft Requirement 7: Draft Requirement 7 stipulates that when multiple copies of a record exist, the creator should have procedures to determine which copy is authoritative: that is to say, which is to be treated as the "record copy." The idea behind this requirement is that the presumption of authenticity will be strengthened by the existence of such procedures because all copies will be identified to be what they are—for instance, record copy, convenience copy, source record, and so on. This, in turn, will make affirmation of whether the record is what it purports to be more reliable.[18]

7. if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative, and when reproducing it, must identify the form of the authoritative copy (that is, imitative copy, copy in the form of the original, simple copy, insert).

No high level instruments or CSO guidelines deal with this issue. On the other hand, however, it may be that designation of the record copy is a matter generally treated in policies at the departmental level. Whether this is so is difficult to say, but the one sample of a departmental policy that is publicly available does establish certain measures to satisfy the first aspect of the requirement. This instrument, Natural Resources Canada's *Guidelines on Managing Electronic Mail Messages*, sets out, first, that officers must distinguish record from non-record e-mails according to particular criteria. This passage is noteworthy in that it illustrates specifically how line officers can use the legal definition of records contained in the *NAC Act* to determine if the documents they create in the course of their business are records. Following this, the policy sets out similar criteria for determining the circumstances under which e-mail drafts and copies are considered to be records, how to identify transitory records, and procedures for disposition of e-mail source records when local office systems dictate a print-out-and-file procedure for recordkeeping.[19]

Within these passages, implicitly, the *Guidelines* establish regulations determining which shall be considered the record copy. Consider, for example, the following extracts dealing with duplicates and source records:

> E-mail messages sent internally through postmaster or other departmental distribution lists, for administrative or organizational requirements, are considered duplicate copies. You may delete these messages once this information is no longer of use to you. The onus is on the originator to ensure that the original messages are retained as departmental records. This would also apply to copies of e-mail messages sent internally between work groups/units, solely for reference or information. If you reply to any of these e-mail, you are adding to the copy and, therefore, creating a new original. As the originator you must determine if this new message is a departmental record and needs to be retained. … It is unnecessary to keep more than one format of your e-mail record. If you have printed and filed your e-mail record in hard copy … you can delete the electronic copy. If you have copied and filed your e-mail record in a shared directory … you can delete the copy in Microsoft Exchange.[20]

Certainly, the policy could be more stringent in its terms. For one matter, the passage dealing with printing messages makes no provision for capture and preservation of metadata. Overall, though, the document certainly provides important guidance by suggesting that the record copy will be, depending on the circumstances, the version remaining with the "originator," that which is stored in a shared directory, or that which is printed and filed.

On the other hand, of course, this sample document is not necessarily representative of departmental e-mail policies, not to mention records management policies, across the many agencies of the federal government. Moreover, the fact that the Natural Resources *Guidelines* only treats the question obliquely—*in effect* providing a regulation to determine the authoritative copy, but not stating as much—tends to suggest that the drafters of the document were not attempting to implement rules that would guard the authenticity of their records. More likely, they devoted this attention to distinguishing records, copies, drafts, and source records in order to protect the department against the kinds of legal difficulties raised in the prominent U.S. court case of *Armstrong v. Executive Office of the President*. Finally, it is worth considering whether the questions addressed by Draft Requirement 7 should be left for departments to regulate at the lowest level of the policy hierarchy. In consideration of the fact that record authenticity should be a concern for all government agencies, it seems that requirements to identify the authoritative record copy should be written into one of the standards applicable government-wide.[21]

Draft Requirement 8: The idea standing behind Draft Requirement 8 is that the appraiser will have a greater presumption of authenticity if the creator has provided evidence of a recognition that preserving authenticity can, in some circumstances, require bringing forward supporting documentation pertinent to the records or the system. Evidence of this recognition can be located if procedures are in place to specify what supporting material will be required under which circumstances.

8. if there is a transition of records from active to semi-active status and semi-active to inactive status, the creator has established and implemented procedures determining what has to be removed along with the records (for example, indexes, data directories, data dictionaries, profiles).

Requirement 8 has a rough equivalent in a document entitled *Guidelines for the Transfer of Textual Archival Records to the National Archives of Canada*. This document is designed to state principles by which terms-and-conditions agreements for transfer of records should be drafted. For the most part it deals with paper records. However, one section addressing electronic records stipulates that

> when electronic records are transferred to the National Archives, the institution must transfer the archival component of the specific system including such descriptive elements as data, tables, modules or electronic textual records. The institution must also include supporting metadata for the system which include printed or electronic versions of data elements, data definitions, code values, naming protocols, user or system manuals.[22]

These rules only meet the terms of Draft Requirement 8 in part. They do establish that when transfer of supporting documentation is necessary, such transfer will take place. While it is no doubt beneficial that this guarantee exists, unfortunately the guideline is silent on several matters. First, the document does not, *per se*, create policy, but instead provides advice on what should be included in agreements for transfer of records from agencies to the NAC. This accounts for the fact that the *Guidelines* do not create specifications to determine the circumstances under which supporting documentation must be brought forward, nor which kinds of documentation will be required in which situations. In addition, and vitally important, the policy does not require that the creator have procedures in place to deal with transfer of supporting information. Instead, it only dictates that agency personnel "must transfer" the pertinent material. With this failure to require that agencies establish procedures, the policy fails to create a mechanism forcing the creator to recognize the need to plan for protection of record authenticity. Finally, as with several other policies, it is necessary to point out once again that nothing in the *Transfer* regulation states that the issue of supporting documentation is related to authenticity.

Evaluation and Conclusion

It should be clear from this analysis that federal policies do not match-up well against the product of the ATF's work. To an extent, it is possible to locate a counterpart for each Draft Requirement—to identify where regulatory instruments come closest to addressing the eight principles that determine what actions on the part of the creator are necessary to support the presumption of authenticity. However, in no case is the association between policy and Draft Requirement more than incidental: at best, the government dictates implementation of certain of the methods by which requirements may be satisfied, but never are these mandated for the purpose of guarding authenticity. The implication is that government personnel have neglected to consider authenticity of records as a matter that should be addressed in records or information management policies. The Canadian government should take steps to rectify this oversight. The first step toward ensuring that records will be created and maintained authentic is to educate creators to the importance of record authenticity, and the necessary precondition for achieving this is to institute policies that explain the meaning and importance of authenticity through specifying practices that are required to protect it.

Although it has not been emphasized thus far, another weakness of federal regulations may have become evident by this point as well: that the policy framework has manifest flaws even if examined in isolation. The remainder of these conclusions place the foregoing discussion in a wider perspective, and argue that the need for comprehensive reform can be recognized even without an analysis based on a comparison with the InterPARES Draft Requirements.

The idea standing behind the federal recordkeeping framework is that top-level documents establish principles for records and information management, while lower-level instruments provide specifications that translate principle into practice. In other words statutes and TBS policies are intentionally written to be general in character, while CSO guidelines and department policies, purportedly, will supply the necessary details. However, a dilemma arises in that instruments at all levels are far too vague to perform their intended function. At the top level, the failings of the MGIH have already been introduced. To reiterate, however, this policy only refers to recordkeeping in the clause dictating that institutions must "maintain" their "records of enduring value." This hardly constitutes a set of records management principles.[23]

As for regulations at lower levels, the preceding discussion should have provided some sense of the vague character of most CSO guidelines. The *TSSIT* can be identified as an exception to the rule, but recall, for example, how both IMF and RDIMS officials avoided stating a purpose for metadata capture, how the NAC *Transfer* guidelines allowed full discretion to those writing terms and conditions agreements, and how the issues of planning for upgrade, forms management, and authentication of records were not addressed anywhere in government regulations. To take another, more specific example, consider the "recordkeeping requirements" listed in the NAC guideline entitled *Record Keeping in the Electronic Work Environment*:

- Appropriate records are kept as evidence of business activities.
- Records must have sufficient content, context and structure to provide evidence of the activities they document.
- Records remain available, understandable and useable for as long as they are needed for business and accountability purposes.
- Records are preserved and protected from accidental or intended damage, destruction and unauthorized access.[24]

The problem here is that while these “recordkeeping requirements” are supposed to describe specific practices, they are, at best, principles in themselves: they are more detailed than the recordkeeping passages in the MGIH, but they do little to define which records are “appropriate” to retain as evidence of business transactions, how to ensure that records have “sufficient content, context and structure,” and so on. Thus, they will not be of great assistance to line officers in creating and handling their records, nor to agency technical staff attempting to establish system configurations that will facilitate proper records management. As we have seen, some of these issues are addressed in the Natural Resources Canada *Electronic Mail* policy. The point, though, is that such specifications should be contained in instruments above departmental policies. If failings like these are not addressed, the government’s proclaimed goal of “provid[ing] an environment where information is *managed in a consistent fashion*” will be defeated. The same can be said of the need to revise higher level policies as well.[25]

Reform to the federal regime directed at improving records management policies is not difficult to envision. All that would be required is the strengthening of the framework at one level. This kind of reform holds potential to be effective because in policy, unlike in physics, a chain can be as strong as its *strongest* link; if a single instrument specifies detailed methods and practices, and binds agencies to comply with them, reform of the framework as a whole will be unnecessary. Moreover, the basic structure of the regulatory hierarchy can be retained in this manner, and agencies can be left with the appropriate amount of discretion to create their own policies within those effective government-wide. One proviso needs to be added, however: this new, enhanced plank in the framework must be written by staff at the National Archives, and personnel delegated for the task must be allowed to base their work on a foundation of archival and records management theory. To do otherwise, to allow the TBS or the IMF to act as lead agency, would risk defeating the purpose of the reform effort. Under such a scheme future policy would be set, as it has been since passage of the MGIH in 1989, by personnel preoccupied with information management concerns—security classification, data retrieval, cost reduction, and so on. As a result, questions vital to the proper management of records, such as the implementation of procedures to support authenticity, would continue to be neglected.[26]

How would a framework revised along these lines look? Some comparison with other countries participating in InterPARES may be helpful for clarification. In the United States, to take just one example, the National Archivist is empowered by statute to "promulgate standards, procedures, and guidelines with respect to records management." These standards are published in the *Code of Federal Regulations* [*CFR*], and thereby they dictate minimum requirements that must be satisfied by all agencies. They are also highly specific, stipulating, for instance, that

> disposition instructions … shall be incorporated into the [electronic] system's design, [that] electronic recordkeeping systems [shall] provide a standard interchange format [and] provide for the grouping of related records into classifications, [and that] agencies shall maintain the storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the following temperatures and relative humidities:
>
> Constant temperature -- 62 to 68°F.
> Constant relative humidity -- 35% to 45%[27]

The point here is not necessarily to advocate replicating the American model, but instead to point out that national archival institutions are expected to play a policy-making role in other countries. In the case of the United States, furthermore, we can see that at least one country allows the Archivist not only to create binding rules, but also makes room at the level of secondary legislation for highly detailed requirements, including matters as technical as temperature and humidity specifications. In Canada, no instruments containing this degree of detail exist above the level of CSO guidelines, and the closest instrument we have to secondary legislation is a chapter in the *Treasury Board Manual* nearly silent on recordkeeping, the MGIH.

It is worthwhile to acknowledge that the impending finalization of the International Standards Organization's records management standard, and the Canadian government's commitment to adopting it, will address many of the issues raised here. Nevertheless, it is still crucial that reform be initiated. The first step is to mount a concerted effort to educate senior government officials to the fact that records management regulations will continue to be ineffective unless they are made more precise, brought into line with archival theory, and, ideally, revised in accordance with the InterPARES Draft Requirements. Achieving these educational goals is indispensable because it is these senior officials who have power to decide whether responsibility for writing policies will be transferred to experts at the NAC, or if it will remain with those who created the regulations currently in place.[28]

Although it might be a controversial proposal to make, the most effective way to work toward reform may be for members of the InterPARES Canadian Team to direct a greater proportion of the dissemination effort toward federal government officials. Doing so would entail expanding and enhancing the analysis presented here, drafting a comprehensive business case detailing the flaws of the framework in place and the reasons why reform is necessary, and attempting to arrange a series of seminars, lectures, or other means of communicating the message to powerful audiences: Treasury Board personnel, relevant parliamentary committees, and perhaps even Cabinet members. There is no question that InterPARES researchers would be hard-pressed to take on additional responsibilities such as these with the completion of the project drawing near. Moreover, it may not be appropriate for archivists to engage in lobbying activities of this sort. On the other hand, though, the Social Sciences and Humanities Research Council recently recommended that InterPARES begin to disseminate its results further afield, to audiences beyond the archival community, and it may be that members of the Review Committee had undertakings like this in mind. In addition, it may be that InterPARES has an obligation to do more than simply make its results available to the Canadian government. Due to the significant amount of federal funding received by the Project, and as consequence of the truly anemic state of the current recordkeeping regime, perhaps this is a case where it would be justifiable for archivists to act as lobbyists. The stakes are high, and, if the experts in the field do not force senior Canadian officials to realize the magnitude of the problems that exist, it is unlikely that anyone else will.[29]

Endnotes

[1] InterPARES Project, Authenticity Task Force, “April 2001 Meeting: Minutes and Documents” (Vancouver: InterPARES Project, 2001), 26-7. For the sake of simplicity, “Draft Requirements” is used hereafter to refer to those requirements that support the appraiser’s presumption of authenticity. The other requirements, those enabling the preserver to attest to the authenticity of copies of electronic records, are not considered in this analysis. The reason for this selectivity in coverage has to do with the need to reduce the scope of the essay to manageable proportions. Note also that, notwithstanding the differences between their formal definitions, the terms “recordkeeping” and “records management” are used synonymously throughout this essay. Such usage is intended solely to relieve repetitiveness in the prose.

[2] *National Archives of Canada Act.* R.S., 1985, c. C-1. The Governor in Council has authority under the Act to create regulations *per se*. The difference is that formal regulations—or, secondary legislation in the strict sense—are contained in the *Consolidated Regulations of Canada*, while the standards approved by the National Archivist are lower in the hierarchy of instruments. Policies in the *Treasury Board Administrative Policy Manual* occupy a position between these levels; they are not approved by Cabinet, as are entries in the *Consolidated Regulations*, but they are binding rules rather than advisory standards like most of the NAC guidelines.

[3] Treasury Board Secretariat, Chief Information Officer Branch, “Policy on the Management of Government Information Holdings,” *Treasury Board Manual – Information Management,* Chapter 3-1, last revision 31 July 1994, “Section 6: Preservation, Retention and Disposal,” <http://www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_GIH/CHAP3_1_e.html> (25 April 2001).

[4] Unfortunately, no departmental policies seem to be publicly available other than the *Guidelines on Managing Electronic Mail Messages* issued by Natural Resources Canada. This is treated below, in connection with Draft Requirement 7. On CSO’s and their powers and responsibilities in the regulatory process, see Treasury Board Secretariat, *Strategic Direction for Government: Information Management*, 10. <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/im-gi/sdg-osg_e.html> (25 April 2001).

[5] The use of the Draft Requirements as ‘benchmarks’ in the sense described here is not intended to suggest any position on their need for future revision, or lack thereof. Instead, simply, the timing of the writing of this essay has made it necessary to refer to a product, the Draft Requirements, that is not quite finalized yet.

[6] Information Management Forum, *Record Keeping Metadata Requirements For the Government of Canada,* September 2000, <http://www.imforumgi.gc.ca/new_docs/metadata1_e.html> (25 April 2001). See the following chart for a comparison between InterPARES fields and IMF fields. In some cases the matches are quite close. For example, see InterPARES fields "Writer" and "Addressee," and corresponding IMF fields. In most cases, though, IMF elements listed as counterparts only bear a distant resemblance. Consider, for example, IMF fields "Department Identifier," "Organization," and "Signed by." These are listed here as counterparts to InterPARES element "Author" because they treat the matter of responsibility and accountability for the record. However, a very good case could be made for their being closer counterparts to InterPARES field "Writer" because they refer to responsibility and accountability for content of the record, not for issuing it. Or, to take a second example, IMF "Management History" is listed here because it could include data relevant to InterPARES fields "Annotations" and "Technical Modifications." But, due to the discretion left by the IMF definition, this will not necessarily be the case. At any rate, the chart serves to give a feel for the juxtaposition between the two metadata sets even though it does not provide a detailed comparison of concepts upon which the InterPARES and IMF mandated elements are based.

InterPARES field	**IMF Field**
Author	**Department identifier**: Department responsible / accountable for content. **Organization**: Organization responsible/accountable for content. There may be several organizational levels depending upon departmental requirements. **Signed by**: Person who signed the record and is accountable for its content. **Trustee**: Person responsible for the record. Could be the same as author, used when the author has moved on, or used when responsibility for the record does not rest with the author.
Writer	**Author**: Person primarily responsible for creation of the intellectual content.
Addressee	**Designated recipient**: The target name or position title, audience or destination for outgoing correspondence.
Originator	———
Action or Matter	**Title**: Name, caption or subject line. **Description**: Summary, synopsis, key words.
Dates (that is, of the document, archival and transmission)	**Date**: Date created, date of the record, date of last administrative use, edit date, approval date, etc., depending on departmental requirements.

Expression of archival bond (for example, classification code, file identifier)	**Document number**: Unique, system-generated, unalterable number. **Subject code**: Controlled identifier, number or code indicating related program activity/sub-activity, function, responsibility centre and/or subject. used to group related records.
Status of transmission (that is, draft, original, copy)	**Final**: Check box to indicate the final iteration, and to trigger locking to prevent further alteration.
Attachments	———
Handling office	———
Office of primary responsibility (if different from handling office)	———
Annotations	**Management history**: Audit trail of actions captured by the system, including access, edits, deletions, etc.
Technical modifications	**Management history**: Audit trail of actions captured by the system, including access, edits, deletions, etc.

[7] Treasury Board Secretariat, Shared Systems Program, Interdepartmental RDIMS RFP Sub-Committee, and National Archives of Canada, Information Management Standards and Practices Division, R*ecords/Document/Information Management (RDIM): Integrated Document Management System for the Government of Canada Request for Proposal (RFP) Software Requirements,* May 1996, <http://www.archives.ca/06/0603_e.html> (25 April 2001).

[8] Treasury Board Secretariat and National Archives of Canada, *RDIMS Requirements,* 7-9. See chart below for comparison between InterPARES and RDIMS fields. The same provisos expressed above, in relation to the IMF metadata set, apply here as well.

InterPARES field	**RDIMS field**
Author	**From** [no definition] **Created By** [no definition]
Writer	**From** [no definition] **Created By** [no definition]
Addressee	**To** [no definition]
Originator	**Department Identifier**: code assigned to every department in the government of Canada.
Action or matter	**Object Title**: formal title. **Object Description**: further description of the subject of the object, if necessary.
Dates (that is, of the document, archival and transmission)	**Version Number/Date**: version information, and/or links to original and other versions. **Date of Object**: date appearing on object. **Date Created** [no definition] **Date Sent** [no definition] **Date Received** [no definition]

Expression of archival bond (for example, classification code, file identifier)	**Department Identifier**: code assigned to every department in the government of Canada. **Program/Activity/Sub-Activity/RC Title**: titles as set forth in the departmental OPF or main estimates. **Program/Activity/Sub-Activity/RC Identifier**: codes as part of the financial codes linking to the OPF or equivalent.
Status of transmission (that is, draft, original, copy)	**Version Number/Date**: version information, and/or links to original and other versions.
Attachments	**Links to Other Objects/Attachments**: links between electronic and non-electronic objects, links between objects and attachments, etc.
Handling office	———
Office of primary responsibility (if different from handling office)	———
Annotations	———
Technical modifications	———

[9] Treasury Board Secretariat and National Archives of Canada, *RDIMS Requirements*, 7. The metadata sets against which the IMF compares its products are those produced by the Dublin Core project, the Canadian Government Information Locator Service, and the Canadian Common Look and Feel for internet design. On the matter of these being designed for the purpose of retrieval, see Dublin Core Metadata Initiative, "Overview," <http://dublincore.org/about/> (25 April 2001); Treasury Board Secretariat, Chief Information Officer Branch, "CLF - Navigation and Format Section," 19 April 2001 <http://www.cio-dpi.gc.ca/clf-upe/6/6_e.asp> (25 April 2001); Canada, "Government of Canada Internet Guide, Third Edition," Chapter 3.2, Introduction to GILS and Precision Searching, July 1998, <http://canada.gc.ca/programs/guide/3_2_2e.html> (25 April 2001). Note also that use of the term "identify" in the statement of purpose of the RDIMS document may refer to establishment of identity in the sense used in the InterPARES Project. However, from the context of this passage, and especially the "identify/retrieve" construction of the sentence, it appears the authors of this policy were using the term in a different sense; that is, in the sense that it is necessary to "identify" an object by establishing whether or not it is relevant to a particular search query before retrieval is possible.

[10] Treasury Board Secretariat, Financial and Information Management Branch, "Information Technology Security Standard," *Treasury Board Manual - Security*, Chapter 2-3, last revision 1 June 1995, "Section 4: Information Technology Security and Physical Security," and "Section 5.2: Software Security," <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.html> (25 April 2001). Regarding

means, or methods, recommended by the ATF, see InterPARES Project, *April 2001 Meeting: Minutes and Documents,* 29-32.

[11] Royal Canadian Mounted Police, *Technical Security Standard for Information Technology* (*TSSIT*), August 1997, 49-56, <http://www.rcmp-grc.gc.ca/tsb/pubs/standards/index_e.htm> (25 April 2001).

[12] Royal Canadian Mounted Police, *TSSIT*, 1.

[13] Treasury Board Secretariat and National Archives of Canada, *RDIMS Requirements*, 4.

[14] Treasury Board Secretariat, "MGIH;" Treasury Board Secretariat, Financial and Information Management Branch, "Management of Information Technology," *Treasury Board Manual – Information Management*, Chapter 2-1, last revision 17 January 1994, "Electronic Service," <http://www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_IT/CHAP2_1_e.html> (25 April 2001).; Prime Minister's Response to the Speech from the Throne, October 13, 1999, quoted in Canada, *Government On-Line: Serving Canadians in a Digital World*, 10, n. 1, <http://www.gol-ged.gc.ca/pub/serv-can/serv-canpr_e.asp> (25 April 2001).; [Canada], *Blueprint for Renewing Government Services Using Information Technology*, Discussion Draft 1994, <http://www.intergov.gc.ca/docs/fed/blueprint/index.html> (25 April 2001).

[15] Treasury Board Secretariat, "MGIH," "Section 2: Assessing and Defining Information Needs." Whether or not the former "Forms Management" policy addressed establishment of documentary forms associated with each procedure is open to question since this document does not appear to be available at present. The other policies amalgamated into the MGIH were those dealing with "Records Management," "Government Information Collection and Public Opinion Research," "Micrographics," and "EDP Records Management;" see Interdepartmental Work Group on the Evaluation of Information Management Policies, *Guide to the Review of Management of Government Information Holdings*, November 1995, "Background," <http://www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_GIH/GUIDE_e.html> (25 April 2001).

[16] InterPARES Project, *Minutes and Documents*, 27, n2.

[17] Treasury Board Secretariat, "MGIH;" Treasury Board Secretariat, Financial and Information Management Branch, *Treasury Board Manual – Access to Information Volume*, last revision 19 August 1994, <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_121/siglist_e.html> (25 April 2001). Treasury Board Secretariat, Financial and Information Management Branch, "Policy on Electronic Authorization and Authentication," *Treasury Board Manual – Comptrollership*, Chapter 2-2, last revision 15 July 1996,

"Section 3: Definitions," <http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_142/2-2_e.html> (25 April 2001). See also Treasury Board Secretariat*,* "Management of Information Technology;" Treasury Board Secretariat*,* "Information Technology Security Standard;" Treasury Board Secretariat, Financial and Information Management Branch, "Guidelines," *Treasury Board Manual - Information Management*, Chapter 2-2, last revision 17 January 1994, <http://www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_IT/ABD2_2_e.html> (25 April 2001).; Treasury Board Secretariat, Financial and Information Management Branch, "Security Policy," *Treasury Board Manual*, Chapter 1-1, <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT1-1_e.html> (25 April 2001). Regarding authentication in PKI policy, the TBS *Manual* defines it as "the process by which an electronic authorization is verified to ensure, before further processing, that the authorizer can be positively identified, that the integrity of the authorized data was preserved and that the data are original." In turn, data integrity is defined as "the quality or condition of being accurate and complete and not altered or destroyed in an unauthorized manner," and authorization is "the process by which a digital signature is linked to an electronic business transactions to signify that a person with delegated authority has effectively authorized the further processing of that data and cannot credibly deny that s/he has done so." While verification of "data integrity" is involved, there are significant discrepancies between these concepts and InterPARES authentication. First, the object of authentication in the Canadian government scheme is not the record, but the "authorization," the affixing of a digital signature. Second, this policy only treats data integrity, not record integrity. Finally, the policy places priority on authorization, and only treats authentication in passing. The focus of the regulation is to prove authorization and ensure that the authorizer can be identified. See Treasury Board Secretariat, "Policy on Electronic Authorization and Authentication," "Section 2: Preface."

[18] The term "authoritative" was chosen to avoid confusion that would result if the term "original" was used. For the sake of convenience, "record copy" is used here as a synonym for "authoritative" copy.

[19] Natural Resources Canada, *Guidelines on Managing Electronic Mail Messages*, 7 January 2000, 3-5, 6-8 <http://www.imforumgi.gc.ca/products_e.html> (25 April 2001). Note that the second aspect of Draft Requirement 7, the identification of the form of the authoritative copy, is not addressed in federal policies. This, however, is not entirely surprising; with policy-makers lacking awareness of basic archival theory, we

should not expect that they would be aware of diplomatic concepts, such as the differences between imitative copies, copies in the form of the original, simple copies, and inserts.

[20] Natural Resources Canada, *Guidelines*, 5, 7.

[21] The suggestion that Natural Resources Canada was motivated by fears of the post-*Armstrong* era is merely inference, but it does seem quite plausible given the degree of attention paid to distinguishing record and non-record e-mail in this guideline.

[22] National Archives Of Canada, Government Archives and Records Disposition Division, *Guidelines for the Transfer of Textual Archival Records to the National Archives of Canada*, 3, <http://www.archives.ca/06/0611_e.html> (25 April 2001).

[23] Treasury Board Secretariat, "MGIH."

[24] National Archives of Canada, Information Management Standards and Practices Division, *Record Keeping in the Electronic Work Environment – Vision*, May 1996, 5, <http://www.archives.ca/06/0603_e.html> (25 April 2001).

[25] National Archives of Canada, *Electronic Work Environment (EWE) – Vision*, 1996, 9 <http://www.archives.ca/06/0603_e.html> (25 April 2001). Emphasis added.

[26] The suggestion here that reform would not be difficult to envision should not be taken to mean that it would be a straightforward matter for implementation. This, in fact, would likely present considerable difficulties given government inertia, the political value public figures evidently identify in the rhetoric of "the information age" and related ideas, the fact that the IMF and other bodies would likely dispute any redistribution of power, and so on.

[27] 44 USC 2903; 36 CFR 1234.

[28] Information Management Forum, Archives/Records Management Sub-Committee, "Records Management Standard: Background and Update on the Progress of ISO/TC46/SC11," June 2000, <http://www.imforumgi.gc.ca/new_docs/rms2000_e.html> (25 April 2001). The Draft Standard is available at <http://www.nara.gov/records/nwm17-00.html>

[29] Major Collaborative Research Initiatives, Site Visit Peer Review Committee, *Site Visit Report: The Long Term Preservation of Authentic Records; InterPARES* (February, 2001), 9-10.