Definition of Electronic Records in the Public Sector and Their Reliability and Authenticity

Today I am going to discuss the efforts made by the InterPARES Project to provide a definition of electronic record that is at the same time all encompassing and useful. For those who are not familiar with InterPARES, I am going to provide a brief summary of its goal and objectives.

InterPARES (International research on Permanent Authentic Records in Electronic Systems) is a research endeavour that aims at developing the theoretical and methodological knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form. This knowledge should provide the basis from which to formulate model policies, strategies and standards capable of ensuring the longevity of such material and the ability of its users to trust its authenticity. InterPARES has developed in two phases. It started out to deal with records mandated for accountability and administrative needs. In most countries, such records are the majority of those selected for permanent preservation, and constitute a high priority for the public sector. When in electronic form, they are usually created in databases and document management systems. The authenticity of these records on traditional media has been a concern of most governments, which have explicitly stated requirements for their authenticity that could be used as a starting point for developing new requirements for their electronic counterparts. The creation, maintenance and use of these records are highly controlled, thus the first phase of InterPARES was able to focus on the preservation of the authenticity of records that are no longer needed by the creating body to fulfill its own mission or purposes, and issued authenticity requirements, and methods

of appraisal and preservation. However, by the time this phase was concluded, the electronic records produced in the normal course of affairs had become much more complex. Thus, a second phase of research began, InterPARES 2, the goal of which is to ensure that the portion of society's recorded memory that is digitally produced in interactive, dynamic and experiential systems in the course, and as a byproduct of, artistic, scientific and electronic government activities can be created in accurate and reliable form, and maintained and preserved in authentic form, both in the short and the long term, for the use of those who created it and of society at large, regardless of digital technology obsolescence and media fragility.The research objectives of InterPARES 2 are:

- to develop an understanding of interactive, dynamic and experiential systems and of the records produced and maintained in them, of their process of creation, and of their present and potential use in the artistic, scientific and government sectors;
- to formulate methods for ensuring that these records are generated and maintained by the creator in such a way that they can be trusted as to their content (that is, are accurate and reliable) and as records (that is, are authentic);
- to formulate methods for selecting among them those that have to be kept after they are no longer needed by the creator in the ordinary course of activity because of their legal, administrative, social or cultural value;
- to develop methods and strategies for keeping the records selected for continuing preservation in authentic form over the long term;

- to develop processes for analyzing and criteria for evaluating advanced technologies for the implementation of the methods listed above in ways that respect cultural diversity and pluralism; and
- to identify and/or develop specifications for policy, metadata, and automated tools necessary for the creation of an electronic infrastructure capable of supporting the creation of accurate and reliable, and the preservation of authentic digital records

The InterPARES research team determined at the very beginning of the first phase of the project that, before plunging into the study of the material in question, it was necessary to agree on the definition of record and on how it differed from document, information and data. Thus, the group decided to define a record as any document created (i.e., made or received and set aside for further action or reference) by a physical or juridical person in the course of a practical activity as an instrument and by-product of it, thereby choosing the traditional archival concept. The group then proceeded to define document as recorded information, information as a message intended for communication across space or time, and data as the smallest meaningful piece of information. Finally, an electronic record was defined as a record created (i.e., made or received and set aside for action or reference) in electronic form, meaning that a message received in electronic form but set aside for action in paper form is a paper record, while a letter received on paper but scanned in the computer and only used as a digital file is an electronic record. However, the research focused on records born, maintained and used in electronic form.

Regardless of the choice of a traditional archival definition for an electronic record, it was essential to determine what the necessary characteristics of such record are. The following were identified: 1) a fixed form, meaning that the binary content must be

stored so that it remains complete and unaltered, and its message can be rendered with the same documentary form it had when first set aside; 2) an unchangeable content; 3) explicit linkages to other records within or outside the digital system, through a classification code or other unique identifier based on a taxonomy; 4) an identifiable administrative context; 5) an author, an addressee, and a writer; and 6) an action in which the record participates or which the record supports either procedurally or as part of the decision making process.

The other concept to clarify was that of authenticity, given that so often in common language it is confused with reliability and with authentication. Thus, authenticity was defined as the trustworthiness of the record as a record. In other words, the term refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted. In this sense, authenticity differs from reliability, which is the trustworthiness of the record as to content, that is, its ability to stand for the facts it is about. Reliability is an exclusive responsibility of the record creator and is assessed on the basis of the completeness of the record, the competence/trustworthiness of its author, and the amount of control exercised on the process of creation.

Authenticity also differs from authentication, which is defined as a declaration of authenticity, resulting either by the insertion or the addition of an element or a statement to a record. In fact, the distinction between authenticity and authentication is even more important at a time when governments are legislating about the use of digital signatures and other similar devises. In the InterPARES analysis, digital signatures are identified as examples of electronic seals, being functionally equivalent to the ancient seals, which were not only a means of verifying the origin of the record and the fact that it was intact,

but also made the record indisputable and incontestable, that is, had a non-repudiation function. The analogy is not perfect, because those seals were associated exclusively with a person, while the digital signature is associated with a given person and a specific record, and because the former is an expression of authority, while the latter is only a mathematical expression. However, it is essential to remember that authenticity is a property of the record that accompanies it for as long as it exists, while authentication is a means of proving that a record is what it purports to be at a given moment in time.

In order to understand further what the idea of authenticity implied when it came to ensure its existence in the first place, and preservation later, we divided the concept into two components: identity and integrity. Identity refers to the attributes of a record that uniquely characterize it and distinguish it from other records. These attributes include: the names of the persons concurring in its formation (i.e., author, addressee, writer and originator); its date(s) of creation and transmission; an indication of the matter or action in which it participates; the expression of its relationship to other records; and an indication of any attachment(s). These attributes may be explicitly expressed in an element of the record (like a signature for the author) or in metadata related to the record, or may be implicit in its various contexts (documentary, procedural, technological, provenancial, or juridical-administrative). Integrity is the wholeness and soundness of a record. A record has integrity if it is intact and uncorrupted, that is, if the message that it is meant to communicate in order to achieve its purpose is unaltered. This means that a record's physical integrity, such as the proper number of bit strings, may be compromised, provided that the articulation of the content and its required elements of

form remain the same. Integrity may be demonstrated by evidence found on the face of the record, in metadata related to the record, or in one or more of its contexts.

One of InterPARES 1 primary objectives was to establish conceptual requirements for assessing the authenticity of electronic records. The rationale for this objective was that, while in archival theory and jurisprudence, records that are relied upon by their creator in the usual and ordinary course of business are presumed authentic, with records in electronic systems, the presumption of authenticity must be supported by evidence that a record has not been substituted, modified or corrupted in essential respects when transmitted across space (i.e. between persons, systems or applications) or time (i.e., when stored off line, or when the hardware or software used to process, communicate or maintain it is upgraded or replaced). To assess the authenticity of a record, one must be able to establish its identity and demonstrate its integrity by observing the existence of certain conditions, which are made of key importance by the fact that the records of each creator can be distinguished in two categories: 1) the records that exist as created, and 2) the records that have undergone some change and therefore cannot be said to exist as first created.

In order to define the requirements for authenticity, the research team made the fundamental assumption that, regardless of differences in nature, provenance or date, all records are similar enough to make it possible to conceive of one typical, ideal documentary form containing all possible elements of a record. On the basis of this assumption, we hypothesized that, while they may manifest themselves in different ways, the same elements that are present in traditional records exist either explicitly or implicitly in electronic records, and that all electronic records share the same elements.

Thus, we created a template that would allow for a systematic analysis of the electronic records contained in several different systems. "The template is a decomposition of an electronic record into its constituent elements, which defines each element, explain its purpose, and indicates whether, and to what extent, that element is instrumental in verifying the record's authenticity."[i] The template was used to study a significant number of cases in order to assess whether the elements identified in the template were present in the records contained in the systems in question and, if so, to what extent and where, and to identify elements present in the records contained in the systems but not in the template. As the case studies proceeded, the template was refined in light of the results.

The template is composed of four sections: documentary form, annotations, context, and medium. The documentary form includes, among the internal elements, the names of the persons concurring to the creation of the document, the chronological date, the indication and description of the action or matter, the attestation, and a statement of validation, and, among the external elements, overall presentation feature (e.g. text, image, sound, graphic), specific presentation features (e.g. layouts, hyperlinks, colors, sample rate of sound files, resolution of image files, scales of maps), electronic signatures and seals (e.g. digital signature), digital time stamps, and special signs (e.g. digital watermarks, organization crest, personal logo).

The annotations fall into three fundamental groups: 1) additions made to the record after its creation as part of its transmission (e.g. priority of transmission, date and date of transmission in an e-mail record, the indication of attachments), 2) additions made to the record in the course of handling the business matter in which the record participates (e.g. date and time of receipt, action taken, name of handling office), and 3)

additions made to the record in the course of managing it as a record (e.g. filing date, class code, registration number). The categorization of the contexts of the record and the list of what would reveal them correspond to an hierarchy of frameworks that goes from the general to the specific: 1) juridical-administrative context (e.g. laws and regulations), 2) provenancial context (e.g. organizational charts, annual reports, tables of users in a database), 3) procedural context (e.g. workflow rules, codes of administrative procedure), 4) documentary context (e.g. classification schemes, records inventories, indexes, registers), and 5) technological context (e.g. hardware, software, data, system models, system administration).

The medium was difficult to place within the template, because, although it is still necessary for an electronic record to exist, it is no longer inextricably linked with the message, does not store the record as such, but a bit-stream—as the record, to exist, needs the software that reads it—and its choice by the record-maker or keeper can be completely arbitrary or based on reasons related to preservation rather than to the function of the record. In addition, the medium is not a relevant factor in assessing a record's authenticity, at least from the perspectives of the creator and of the record preserver. This was confirmed by the case studies, by the end of which the research team was convinced that, with electronic records, the medium should be considered part of the technological context.

As a consequence of the use of the template to identify electronic records and determine on what their authenticity is based, InterPARES was able to develop two sets of authenticity requirements: the first set, called "benchmark requirements", is meant to give the person who assesses the authenticity of the electronic records of a creator before

they are transferred to the custody of the preserver a reasonable belief that they are authentic; the second set, called "baseline requirements", is meant to support the production of authentic copies of electronic records that have been transferred to the custody of the preserver. The two sets of requirements are based respectively on the notions of trusted record-keeping and trusted custodianship.[ii]

The Benchmark Requirements are eight. While the first identifies the fundamental information about an electronic record that establishes its identity and allows for the demonstration of its integrity, the other seven identify the types of procedural controls over the record's creation, handling and maintenance that support a presumption of integrity.

The first requirement prescribes that the value of the following attributes[iii] are explicitly expressed and inextricably linked to every record. These attributes can be distinguished into categories, the first concerning the identity of records, and the second concerning the integrity of records:

•A.1.a

Identity of the record:

•A.1.a.i

Names of the persons participating into the formation of the record, that is: name of author, writer, originator, and addressee

•A.1.a.ii

Name of action or matter

•A.1.a.iii

Date(s) of creation and transmission: chronological date, received date, archival date, transmission date(s)

•A.1.a.iv

Classification code

•A.1.a.v

Indication of attachments

•A.1.b

Integrity of the record:

•A.1.b.i

Name of handling office

•A.1.b.ii

Name of office of primary responsibility

•A.1.b.iii

Indication of types of annotations added to the record

•A.1.b.iv

Indication of technical modifications

The attributes listed above may appear on the face of the record (e.g. the date, the name of the handling office), but they are more likely to be metadata linked to the record. It is essential that these attributes be inextricably linked to the record and become therefore part of the record itself, and this means that their presence in separate parts of the system, such as the audit trail, is not helpful to guarantee their permanent accessibility in connection with the record and their ongoing existence, in addition to being unpractical, because the preserver would have to maintain a very large amount of

unneeded information in order to keep the specific data related to a record. The two primary means of linking these attributes to a record are the record profile and the topic map. A record profile is a form inextricably linked to a record, which includes specific fields for the automatic or manual inclusion of data related to the record, and it is very common in electronic records management systems. A topic map visually expresses the characteristics of a record and the relationships among them. When a record is either removed from the system for external storage, migrated on the occasion of a system upgrade, or transferred to the preserver, the attributes must go with it, remain inextricably linked to it and be accessible to the user.

The second benchmark requirement regards access privileges. It prescribes that a presumption of authenticity be supported by the fact that the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records. The assignment of the authority and capacity to carry out administrative action on the records must therefore be accompanied by the exclusive technical capability to exercise such responsibility. This is usually done by creating inside the system tables of users' profiles that provide differentiated kinds of access depending on the users' administrative competence. However, access control can also be exercised by means of external security systems, such as the exclusive assignment of a key to a location. The effective implementation of access privileges consists in monitoring access through the use of audit trails that record each interaction of a user with a record.

The third requirement prescribes that the creator has established and implemented procedures to prevent, discover, and correct loss or corruption of records. Examples of

these procedures are making of regular back-ups of records and their attributes, as well as of the entire system; and ensuring that the backup and recovery procedures will guarantee that, in case of system failure, all complete updates are reflected in the rebuilt files and so is any incomplete operation.

The fourth requirement prescribes that the creator has established and implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across technological change. In order to counteract media fragility and technological obsolescence, the creator must plan upgrades to the technological infrastructure of its organization, making sure that the ability to retrieve, access and use records when the upgrades occur is maintained. In addition, the creator must plan procedures of refreshment of the records, moving them from a storage medium to another, and of migration of the records from obsolescent to new technologies.

The fifth requirement prescribes that the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator. This requirement derives from the fact that the authors of electronic records feel much freer in compiling the record than the authors of paper records, and tend to let technology, rather than administrative procedure, determine the form of the record. An acceptable compromise is to let the form of a record be determined by workflow control technology, where one can connect each step of a procedure to a documentary form. Also, the creator can customize specific applications for the whole organization, so that all e-mails or all spreadsheets of a certain kind, for example, will present the same form. The control on documentary form must go down to

the level of records elements, because this is the level at which the authenticity of the record is maintained and can be verified.

The sixth requirement prescribes that, if authentication is required by the juridical system or the needs of the organization, the creator has established specific rules regarding which records must be authenticated, by whom, and what are the means of authentication. This requirement may be met by linking the authentication of specific types of records to the various steps of the administrative procedure, assign responsibility to a given officer or an office for authenticating either individual or all records, and determining either a method of authentication valid for the entire organization or specific authenticating instruments for specific types of records.

The seventh requirement prescribes that, if multiple copies of the same record exist, the creator has established procedures that identify which is the official record. One of the greatest problems presented by electronic records is the easiness of reproduction. Innumerable copies of each record may exist everywhere in the organization, each slightly different from the other, as it resides in a different hard drive of a different computer or because of modifications voluntarily applied to the record by the one or the other person in the organization. It is vital for each organization to know what is its official record, especially because the original record ceases to exist after being stored for the first time. When recalled, the stored entity is a copy. Thus, the official copy of each record will have to be subject to strict procedural controls that will serve as a form of authentication, considering that technologically based forms of authentication (i.e., digital signatures) only serve when records are transmitted across space, as they usually constitute an obstacle to the maintenance of the record to which they are linked. Of

course, when the official record is identified, so is the office of primary responsibility for that record, that is, the office having the formal competence for maintaining the official records that share the same classification and retention period. This will help also reducing duplication in the organization and designating accountability for the records.

The eight and last requirement prescribes that, if records are to be removed from the electronic system in which they were created and/or used, the creator has established and implemented procedures determining what documentation has to be removed and transferred to preservation along with the records. This documentation includes all the information necessary to access the records, to establish their identity and to demonstrate their integrity. If the system generates records profiles, it will be sufficient to ensure that all records are accompanied by their profile. Otherwise, it may be necessary to transfer with the records audit trails, indexes, data directories and data dictionaries, etc.

The requirements listed above are thus intended to allow the archivist to assess, in the course of the process of appraisal, the authenticity of the electronic records of a creator before they are transferred to archival custody. They are cumulative, in the sense that the strength of the assessment of authenticity is based on the number of satisfied requirements and on the degree to which each individual requirement is satisfied.

After the records have been assessed as authentic and transferred to the custody of the archivist, their authenticity must be maintained by the preserver. To do so, the archivist must produce authentic copies of the records in question, because the production of authentic copies is the only way of ensuring their preservation. This fact derives from the nature of electronic records.

In electronic records, the physical and intellectual components do not necessarily coincide, and the concept of digital component (physical part) accompanies that of element of form (intellectual part). A digital component is a digital object that may contain all or part of a record, and/or the related metadata, or more than one record, and that requires specific methods for preservation.[iv] In other words, it is a unit of storage. In addition, the relation between a record and a computer file can be one-to-one, one-to-many, many-to-one, or many to many; the same presentation of a record can be created by a variety of digital presentations and, vice-versa, from one digital presentation a variety of record presentations can derive; and it is possible to change the way in which a record is contained in a computer file without changing the record. Thus, the risks of corruption and loss are very high, and become very complex when records pass across technological boundaries. To minimize these risks, controls of two types are implemented: those inside the digital system, which ensure that the records remain unaltered within it, and dynamic ones, which ensure that the records remain unaltered when they cross technological boundaries. These controls are technological in nature but are determined on the basis of our archival understanding of the structure of the record, because it is impossible to maintain literally unaltered an electronic record. What is possible to do is to protect those components of the record that include the elements of form conveying its meaning, and the archivist must prove to have done so when producing autentic copies of the records. In other words, the archivist must attest that he has satisfied all the baseline requirements for the production of authentic copies. Only by virtue of this attestation, the copy is deemed to conform to the record it reproduces until proof to the contrary is shown. For this reason, the second set of requirements, the

Baseline Requirements, directed exclusively to the archivist, must all be implemented at the highest degree.

The Baseline Requirements are as follows. The first requirement prescribes that the procedures and system(s) used to transfer records to the archival institution or program, maintain them, and reproduce them embody adequate and effective controls to guarantee the records' identity and integrity, and specifically that:

- unbroken custody of the records is maintained;
- security and control procedures are implemented and monitored; and
- the content of the record remains unchanged after reproduction

As part of the transfer process, the assessment of the authenticity of the records, which had occurred during the appraisal process, should be verified by ensuring that the attributes relating to the records' identity and integrity have been carried forward with the records themselves (Benchmark Requirement 1), along with any relevant documentation (Benchmark Requirement 8). Once the records have been transferred to archival custody, the preserver must establish many of the controls that were described in the Benchmark Requirements, that is, must establish access privileges concerning the access, use and reproduction of the records within the archives, implement and monitor them; must establish procedures to prevent, discover, and correct loss or corruption of records, as well as procedures to guarantee the continuing identity and integrity of the records against media deterioration and across technological changes; and, if authentication is required, must establish rules determining responsibility for and means of authentication.

The second requirement prescribes that the activity of reproduction be documented, and this documentation includes:

•the date of the records' reproduction and the name of the responsible person;

•the relationship between the records acquired from the creator and the copies produced by the archivist;

•the impact of the reproduction process on their form, content, accessibility and use; and

•in those cases where a copy of a record is known not to fully and faithfully reproduce the elements expressing its identity and integrity, the details of this information made readily accessible to the user.

The documentation of the reproduction process is essential for the archivist to fulfil the role of trusted custodian of the record, for the user to have access to the history of reproduction, which becomes an integral part of the history of the record, and for future generations to be able to verify the authenticity of the records.

The third requirement prescribes that the archival description of the fonds containing the electronic records includes–in addition to information about the records' juridical-administrative, provenancial, procedural, and documentary contexts– information about changes the electronic records of the creator have undergone since they were first created. It has always been the function, either explicit or implicit, of archival description to authenticate the records and perpetuate their administrative and documentary relationships, but with electronic records, this function has become indispensable. In fact, as original electronic records disappear and an interminable chain of non-identical reproductions follows them, the researchers looking at the last of those reproductions cannot find in it any information regarding provenance, authority, context, or authenticity. The authentication function of archival description is different from that

of a certificate of authenticity, because it is a collective attestation of the authenticity of the records in an archival group and of all their interrelationships as made explicit in the description, rather than being simply an attestation of the authenticity of individual records. One could say that, given the mandatory documentation of each reproduction process carried out by the archivist, for the purposes of demonstrating the authenticity of the records copies themselves archival description is superfluous. However, if archival description summarizes the history of all reproductions, it obviates the need to preserve all the documentation of each reproduction and acts as a certificate of authenticity for the fonds.

The definitions of electronic records, reliability and authenticity, and the requirements for authenticity discussed above seem to work quite well with databases and document management systems. However, they are problematic when applied to the records examined by InterPARES 2, the most salient characteristic of which is the lack of a stable form and content (that is, of fixity). They are experiential, interactive and dynamic records.

Experiential records are electronic objects the essence of which goes beyond the bits that constitute the object to incorporate the behavior of the rendering system, or at least the interaction between the object and the rendering system. Defining the authenticity of such objects is much more complex than with raw data or more traditional electronic records, because it is dependent not on the ability to reproduce a copy of the object's original bit-stream, but on the ability to recreate the environment in which that object was experienced. Examples of experiential digital objects range from audio and moving images embedded in a web page to virtual reality systems.

Interactive records are records made and maintained in interactive systems, where each user's entry causes a response from or an action by the system. To determine means to keep records in such systems authentic, one needs to ascertain a) how user input affects the creation and form of each record (as is the case with much on-line commerce); and b) if and when the interactive system and its inherent functionality need to be maintained intact. Examples of interactive systems range from web pages delivering government services online to musical performances based on human-computer interaction to commercial video games.

Dynamic records are documents whose content is dependent upon data that vary continuously and are held in several databases and spreadsheets. Examples range from simple web pages with embedded links to complex systems where information is stored and updated to be shared via wireless transmission by multiple mobile users in diverse ways. The increasing reliance on such documents by individuals and institutions will necessitate understanding how the information they contain is captured and set aside.

Whether experiential, interactive, and dynamic digital objects are indeed records should depend on their relationship to the activity of their creator. Ironically, the ease with which their form and content can be manipulated has given those who generate them a new reason for keeping them: 'repurposing'. Records creators often obscure the meaning and cultural value of their records by treating their content merely as digital data to be manipulated to generate new records, decontextualizing them from the activity by which they were produced. The potentially wide dissemination of repurposed documents threatens the authenticity if not the continuing existence of the materials subject to this treatment and it is another issue to wrestle with.

In light of these new types of records, it is probably necessary to revisit the concept of record itself, so that both the identification and the protection of experiential, interactive and dynamic documentary information will be possible. We have to consider the possibility of substituting the characteristics of completeness, stability and fixity with the capacity of the system where the document resides to trace and preserve each change that it has undergone. And perhaps we may look at the record as existing in one of two modes, as an entity in becoming, when its process of creation is in course (even if such creation is ongoing), and as a fixed entity at any given time the record is used. There is no doubt that knowledge and strategies must be developed that are beneficial for both the creators and preservers of these complex new records. One way of doing so is to keep in mind that many of the issues surrounding the management of electronic records in the arts and sciences are becoming relevant to government archives, because administrative bodies are increasingly employing complex multimedia systems in the creation of their records. In Canada, for example, the Government On-line initiative has mandated that most transactions between the government and its citizens be possible on the Internet in an interactive mode by 2006. This raises considerable questions for the creation and management of the electronic records generated by such interaction, in part because the making of the record will no longer be the sole responsibility of the body having control of the electronic system (in this case, the government), but also of the user. Additional questions are raised by the double public and private nature of these records that would be shared by private and public persons on-line, rather than existing as distinct entities in the archives of each person participating in the transaction. Further, when the terms and conditions that govern the recorded transactions between government and citizens are

articulated on web pages, those pages may need to be preserved together with their functionality for purposes of accountability.

To meet these challenges requires several more years of research capable of providing an understanding of the nature of the new electronic records and record-creating processes. It is our hope that InterPARES 2 will be able to provide the answers we need.

---

[i] Heather MacNeil, Providing grounds for trust: developing conceptual requirements for the long-term preservation of authentic electronic records, in Archivaria 50, 2000, p. 52-78, at p. 56. This article describes in detail all the elements included in the template and the way it was used in the case studies. The template itself can be found on the InterPARES website at www.interpares.org <resources> <reports> "The Template for Analysis."

[ii] A trusted record-keeping system is one that controls what records are included in the system, who can include, retrieve, modify, delete or remove them from the system, and how the records are included, maintained, retrieved, deleted or removed from the system. A trusted custodian is a person entrusted with the responsibility of preserving the records, having demonstrated that it has no reason to alter the records entrusted to its care or to allow others to do so, and is capable of implementing the necessary measures for the physical and intellectual protection of the records.

[iii] A record attribute is a defining characteristic of the record or of a record element. A record element is a constituent part of the record's documentary form. An attribute may manifest itself in one or more elements of a record's documentary form (e.g. the name of the author as a signature) or in an annotation to the record (e.g. the classification code as a record identifier) or in metadata in the audit trail, etc.

[iv] For example, a report containing graphics may consist of three or more digital components: the text of the report, the profile, and the graphic(s). In contrast, a message with textual attachments may consist of only one digital component.