Produced for

CHECKLIST

Of Requirements

FOR ELECTRONIC RECORDS MANAGEMENT (ERM)

Over the Life Cycle of Patent and Trademark Records

February 26, 1999

Contract Number: 50-PAPT-700041

Task Number: 56-PAPT-8-05089

Deliverable: 98-03-6

Government Task Managers: Arthur F. Purcell, (703) 308-6868, FAX (703) 308-6916
Kathy Schultz (703) 308-7400, FAX (703)308-7407

Contractor: Cohasset Associates, Inc.
3806 Lake Point Tower
505 North Lake Shore Drive
Chicago, IL 60611
Tel. 312/527-1550

Contracting Task Manager: Richard D. Fisher
tel. 408-741-1287, FAX 408-867-1289,
e-mail: rd.fisher@worldnet.att.net

FINAL

TABLE OF CONTENTS

1 INTRODUCTION 1

2 PURPOSE AND SCOPE 4

2.1 SCOPE 4

3 LEGAL REQUIREMENTS 5

3.1 FEDERAL STATUTES AND REGULATIONS 5
3.2 ADMISSIBILITY 6
3.2.1 Authenticity 7

4 DEFINITIONS 8

4.1 FEDERAL RECORDS 8
4.1.1 PTO Record Copy 10
4.2 ELECTRONIC RECORD 11
4.3 VITAL RECORD 11
4.4 A COMPLETE RECORD 12
4.5 CASE FILE AND FILE WRAPPER 14
4.6 RECORD RETENTION 14
4.6.1 Case File Retention 14
4.6.2 Retain Only One Record Copy 15
4.7 USAGE PERIODS 15

5 REQUIREMENTS 17

5.1 RECORDS ACQUISITION 17
5.1.1 Capture of Complete Electronic Records 17
5.1.2 Capture Links to Notes and Annotations 18
5.1.3 Capture Hyperlinks 19
5.1.4 Working Files 19
5.1.5 Conversion of Paper Records to Electronic Form 19
5.1.6 Quality Control 20
5.1.7 Quality Assurance 20
5.1.8 Audits 21
5.2 METADATA 21

5.2.1 Legal Requirements *21*
5.2.2 Metadata Management *22*
5.2.3 Case File and Record Profile Metadata *24*
5.3 FILE MANAGEMENT 31
5.4 PRESERVE INTEGRITY 32
5.4.1 Protect Against Alteration *33*
5.4.2 Validating Integrity *34*
5.5 PROTECT CONFIDENTIALITY 34
5.6 ACCESS CONTROLS AND AUTHENTICATION 35
5.7 SEARCH, RETRIEVAL AND REPRODUCTION 36
5.7.1 Search and retrieval *36*
5.7.2 Store Search Results *36*
5.7.3 Display/Print the Record, the Index and Annotations *36*
5.7.4 Applicant Access *37*
5.8 AUDIT TRAIL 37
5.8.1 Use History Profile *38*
5.8.2 Use History Profile Creation and Update *39*
5.8.3 Link to Other AIS Tracking or Event Logging Systems *39*
5.9 VITAL RECORDS BACKUP AND RECOVERY 40
5.10 RECORDS RETENTION 41
5.10.1 Case File Retention *42*
5.10.2 PTO Retention Period *42*
5.10.3 PTO Case File Retention Schedules *43*
5.10.4 Determine Retention Period *45*
5.10.5 Records to be Retained *46*
5.10.6 Disposal *46*
5.11 MIGRATION 48
5.11.1 Copy, Reformat and Transfer *49*
5.11.2 Media Management *50*
5.12 TRANSFER TO NARA 50
5.12.1 Transfer *51*
5.12.2 Media and File Format Requirements *51*
5.13 RECORDS HOLD 51
APPENDIX A – METADATA GUIDELINES 53

1 INTRODUCTION

The electronic commerce initiatives directed by Secretary of Commerce Daley in a memorandum on December 17, 1997 defined specific organizational roles and responsibilities for achieving the initiatives and also acknowledging the leading role that the United States Patent and Trademark Office (PTO) had already taken in formulating intellectual property policy. These initiatives have been incorporated into the "Reinvention Goals for 2000" which establishes the PTO's vision for the 21st Century - - " to lead the world in providing customer-valued intellectual property rights that spark innovation, create consumer confidence and promote creativity."

To accomplish this vision, strategic and operational goals have been defined that are designed to establish a leadership role for the PTO in electronic commerce and achieve production electronic filing and processing of patent applications by the year 2003 and the filing of trademark applications starting in 1999.

There are legal, and technological forces which will require that the policies, principals, processes, requirements and solutions for managing electronic patent and trademark case files by the PTO be addressed prior to entering full production:

- Laws and regulations require the PTO to provide for adequate management of all records, including electronic records.
- Laws and regulations also stipulate that the integrity of all records be preserved over the full retention period, and that the confidentiality of patent records be protected, as required.
- Retention periods, where ready accessibility to and maintenance of electronic case files and records must be provided, can be permanent. Registered trademarks are retained until they expire or are canceled or abandoned, and the PTO has the

responsibility for retention of granted patent case files for 40 years and abandoned patent applications for 20 to 23 years.

- Technology is certain to change and advance with a frequency that will require multiple migrations of electronic patent and trademark records to new storage media and new hardware and software during these retention period.

OMB Circular A-130 and industry best practices define records management as encompassing the full life cycle of a record, from the time of receipt or creation until final disposition.

> The term "Records Management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to *records creation, records maintenance and use and records disposition* in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective, economical management of agency operations. (emphasis added) **OMB Circular A-130 Management of Federal Information Resources, Section 6. s.**

As such, records management entails much more than just the "retention" of PTO electronic records. Accurate and reliable capture and storage of electronic (and paper) records received or created by the PTO must be assured. The appropriate metadata and file formats must be applied to ensure accessibility to and migration of case files for the full retention period. Integrity must be preserved and confidentiality protected, as required, from the moment of receipt or creation for the full retention period. Maintaining the integrity and confidentiality, as required, of electronic patent and trademark records is also essential for protecting the intellectual property rights and the value of the inventor's business assets. This can be accomplished by ensuring that accurate, reliable electronic copies of the records are captured and then assuring that they are protected from any loss, alteration, removal, or premature destruction over the complete life cycle.

Management of electronic records information has many similarities with the traditional management of digital data in information systems, however, there are also certain unique requirements. The unique areas relate to: long-term accessibility (decades); long-term retention

of records (in many cases permanently); renewal of electronic records to new storage media; transfer to new hardware, software and application systems; and unique metadata requirements that enable the management of electronic records for long-term accessibility and retention.

Given the PTO's plans and programs to move to electronic filing, processing and management of patent and trademark applications, there is a clear need for developing requirements that define policies, practices, procedures and automated information system features and controls that will provide for the effective management of the electronic records that will be received, created, stored, accessed, retained, reproduced and disseminated by these new business processes.

The goal of this working paper, Checklist of Requirements for Electronic Records Management, is to identify and define mandatory operational requirements that need to be reflected as the PTO business and development teams define work processes, develop requirements and implement application information systems that support the management of electronic case files and records.

The Checklist is divided into five sections.

1. Introduction
2. Purpose and Scope
3. Legal Requirements
4. Definitions
5. Requirements

2 PURPOSE AND SCOPE

The purpose of Task Order 98-03, Life Cycle Management of Electronic Patent and Trademark Records is to provide the PTO with issue definition, research, and analysis in specifically designated areas, and to assist in the development of an overall plan for managing electronic patent and trademark records over the full life cycle.

The purpose of this Checklist document is to define electronic record management requirements that must be met by patent and trademark AISs, over the life cycle of electronic case files and associated records, in order to comply with statutory, regulatory and legal admissibility provisions, and to achieve best practice guidelines.

2.1 SCOPE

The scope of the Checklist covers the complete life cycle of electronic case files and associated records and metadata. The Checklist is limited to the management of electronic case files or file wrappers and associated records and metadata. While many of the requirements stated herein may be applicable to other records at the PTO, there is no intent for this version of the Checklist to be applied to records other than those contained in patent and trademark case files.

3 LEGAL REQUIREMENTS

The PTO is required by law to provide for the adequate management of all records, including electronic records, for the required retention period. Patent and trademark case files and records stored by the PTO are subject to legal discovery and must, therefore, also meet the tests of admissibility in Federal courts and in patent appeals and interferences, and in trademark appeals.

3.1 FEDERAL STATUTES AND REGULATIONS

The 1997 PTO Comprehensive Records Schedule states that records created and maintained in every office are critically important to document the evidence of the functions, policies, decisions, procedures and operations of the PTO. The disposition (retention, destruction, or permanent maintenance) of these materials is governed by 44 USC 33 and 36 and CFR 12. In part, the law states, ". . . records may not be removed from Federal custody or destroyed without regard to the provisions of the agency records schedule (SF 115) approved by the National Archives and Records Administration (NARA) or the General Records Schedule (GRS) issue by NARA."

36 CFR § 1220.34 requires each Federal agency to institute adequate management controls for its records:

> 36 CFR § 1220.34 **Creation of records.** Adequate records management controls over the creation of Federal agency records shall be instituted to ensure that the agency functions are adequately and properly documented.

Other Federal regulations relating to specific aspects of records management and electronic records are cited in other sections of this Checklist.

3.2 ADMISSIBILITY

In addition to meeting the requirements of these patent-specific laws and regulations, it is of utmost importance that, when offered as evidence in Federal courts and before the Board of Patent Appeals and Interferences and the Trademark Board of Appeals, electronic records produced in the normal course of business meet the tests of admissibility.

The Federal Business Records Act (FBRA), the Federal Rules of Evidence (FRE), and the Federal Uniform Photographic Copies of Business and Public Records as Evidence Act (Federal UPA) and related case law generally provide for: (a) overcoming objections to the Hearsay and Best Evidence rules, and (b) provide for the admissibility in evidence of copies or duplicates of records (data compilations) that were created or received by a computer system in the normal course of business. Admissibility of records in matters before the Board of Patent Appeals and Interferences is generally governed by the FRE.

The overwhelming prevalence of electronically created, stored and reproduced (copies or duplicates of) records has also been recognized by the judicial system:

> ... [N]o court could fail to notice the extent to which business today depends on computers for a myriad of functions. Perhaps the greatest utility of a computer … is its ability to store large quantities of information, which may be quickly retrieved on a selective basis. Assuming the properly functioning computer equipment is used, once the reliability and trustworthiness of the information put into the computer has been established, the computer printouts should be received as evidence of the transactions covered by the input.[1]

Being able to demonstrate that the records being offered into evidence are authentic and that they were accurately and reliably produced in the ordinary course of business are critical to admissibility:

> [T]he foundation for admission of computerized records consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business

[1] United States vs. Russo, 480 F.2d 1228, 1239 (6th Cir. 1973).

> relies on the computerized records in the ordinary course of carrying on its activities. The … opposing party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information … [T]he court must "be satisfied with all reasonable certainty that both the machine and those who supply the information have performed their functions with utmost accuracy." … [The] trustworthiness of the particular records should be ascertained before they are admitted and the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction.[2]

3.2.1 Authenticity

The test of authenticity is one of the more critical and potentially difficult tests of admissibility since it is somewhat broadly defined and typically relies more on the testimony of a knowledgeable witness to establish.

> [T]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.[3]

This rule suggests that, in addition to the record having been accurately and reliably created, received, inputted and stored, it was:

- created, transacted and/or communicated by an identifiable and verifiable party,
- received or created and stored at a specified point in time, and
- maintained in its originally inputted or transacted form; protected from any alteration or unauthorized destruction; and, as such, the integrity of the record is preserved.

---

[2] United States vs. Russo, 480 F.2d 1228, 1239 (6th Cir. 1973) (quoting United States v. De Georgia, 420 F.2d 889, 895 (9th Cir. 1969)).

[3] Federal Rules of Evidence (FRE) Rule 901 (a).

4 DEFINITIONS

First, it is important to understand what is considered to be a "record" within the laws and regulations of the Federal Government and to define what is the "legal" or "official" PTO record that will be committed to the electronic case file and managed for the full retention life. In this overall context it is also relevant to understand how Federal regulations define "working files", "non-records" and "vital records."

The following are definitions provided by Federal statutes and regulations governing the management of Federal records and from guidelines relating to best practice in records management.

4.1 FEDERAL RECORDS

Documentary materials is a collective term for records and non-record materials that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording. (36 CFR § 1220.14 General Definitions)

The point in time when documentary materials become a record is defined in 36 CFR § 1222.34 **Identifying Federal Records**:

> (b) Record status. Documentary materials are records when they meet both of the following conditions:
>
> (1) They are made or received by an agency of the United States Government under Federal law or in connection with the transaction of agency business; and
>
> (2) They are preserved or are appropriate for preservation as evidence of agency organization and activities or because of the value of the information they contain.

A Federal Record is defined in 44 USC § 3301:

> Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, *made or received* by an agency of the United States Government under Federal law or *in connection with the transaction of public business* and *preserved or appropriate for preservation by that agency* or its legitimate successor *as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government* or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, *extra copies of documents preserved only for convenience of reference*, and stocks of publications and of processed documents *are not included*. (italicized emphasis added)

Working files are also documentary materials that can be deemed "appropriate for preservation" when their status meets the criteria set forth in 36 CFR § 1222.34:

> (c) Working files and similar materials. Working files, such as preliminary drafts and rough notes, and other similar materials shall be maintained for purposes of adequate and proper documentation if:
>
> (1) They were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action recommendation, follow-up, or to communicate with agency staff about agency business; and
>
> (2) They contain unique information, such as substantive annotations or comments included therein, that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions or responsibilities.

36 CFR § 1222.34 defines the standards for agency recordkeeping requirements. It states the importance of properly distinguishing between records and non-record materials:

> (a) *General.* To ensure that complete and accurate records are made and retained in the Federal Government, it is essential that agencies distinguish between records and nonrecord materials by the appropriate application of the definition of records (see 44 U.S.C. § 3301 and 36 CFR § 1229.14) to agency documentary materials. Applying the definition of records to most documentary materials created or received by agencies presents few problems when agencies have established and periodically updated recordkeeping requirements covering all media and all agency activities at all levels and locations.

Certain types of documents and materials are not considered to meet the definition of a record copy and, therefore, are considered a non-record. As generally defined in 36 CFR § 1222.34 (f):

> Nonrecord materials are those Government-owned documentary materials that do not meet the conditions of record status (per 36 CFR 1222.34 (b)) or that are specifically excluded from status as records by statute (44 U.S.C. 3301) statutory definition of records (Section 3301 of reference (d)) or that have been excluded from coverage by the definition. Excluded materials are *extra copies of documents kept only for reference,* stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit. (italicized emphasis added)

4.1.1 PTO Record Copy

In this Checklist, any record that is stored and managed as evidence of activities or events related to a patent or trademark case file, whether paper or electronic, is referred to as the "record copy". In selected regulations (e.g. 36 CFR § 1234.22 (a)) there is also reference made to an equivalent term, the "official file copy."

From the perspective of 44 U.S.C. § 3301, as detailed above, a record must meet the following tests:

- Made or received in connection with the transaction of public business, and
- Preserved or appropriate for preservation by that agency as
- Evidence of the organization, functions, policies, decisions, procedures, operations or other activities, or because of the informational value of the date in them.

44 USC § 3301 also defines *record copy* by defining what is to be considered a *non-record*: "extra copies of documents preserved only for convenience of reference . . are not included".

Also, working files are not considered a record copy unless they fall within the criteria spelled out in 36 CFR § 1222.34 (c).

Essentially, any incoming documents from an applicant to the PTO, whether paper or electronic, that are materially related to a patent or trademark case file is a "record copy" because the record is evidence of transacted business by the PTO, and also because the record represented what an applicant would have considered to be their record copy at the time of submission to the PTO.

Any document created by the PTO when finalized and communicated to an applicant and/or otherwise stored to a patent or trademark case file is a record.

Also, any working file that falls within the criteria spelled out in 36 CFR § 1222.34 (c), i.e., "were circulated or made available to employees other than the creator for official purposes, and" "contain unique information . . that adds to understanding of . . basic policies, decisions, actions or responsibilities" (emphasis added), are to be considered record copy and must be stored in the electronic case file. This definition also implies that all working files created and kept solely by an examiner, for instance, and not circulated to other employees for any official purpose would not be considered a record copy.

4.2 ELECTRONIC RECORD

An electronic record is defined within the context of a general record, but with the added characteristic of being represented in a digital form that only a computer can process.

As defined in 36 CFR § 1234.2:

> Electronic record means any information that is recorded in a form that only a computer can process and that satisfies the definition of Federal record in 44 USC § 3301.

36 CFR § 1234.1 provides a definition regarding the scope of an electronic record:

> This part establishes the basic requirements related to the creation, maintenance, use and disposition of electronic records. Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks; and optical disks. Unless otherwise noted, these requirements apply to all electronic records systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of storage media, in network or stand-alone configurations. **. . .**

4.3 VITAL RECORD

Essentially, all patent and trademark case files, including any related annotations, links and metadata are considered vital records. As such, a backup copy of all electronic patent and

trademark case files and records, including associated metadata, must be made and managed for the full PTO retention period as a means of providing for business recovery from a disaster.

36 CFR 1236.4 defines a vital record as follows:

> **§ 1236.4 Categories of vital records.**
>
> The following definitions are pertinent to the development of a vital records program:
> . . .
>
> (b) *Rights and interests records* are records essential to the preservation of the legal rights and interests of individual citizens and their Government. These records include such groups as social security records, retirement records, payroll records, insurance records, and valuable research records. These records require protection, but storage points do not have to be at or in the vicinity of emergency operating centers.

4.4 A COMPLETE RECORD

A complete record as defined in archival science, and being more broadly accepted as a best practice guideline in electronic records management, has three primary elements:
(1) content, (2) structure, and (3) context.

- **Content**

- *Content* is the actual data resulting from a transaction conducted in the normal course of business, such as from a receipt of a patent or trademark application or the creation and communication **of** an Office action. For example, the content of a patent or trademark application transmittal record includes various data fields related to specific components of the form plus a signature.

- **Structure**

  Structure is generally defined in two parts: logical structure and physical structure. The logical structure of a record includes the identifiable parts of the record, such as the title, applicant address, date and "signature" on a patent or trademark application form. These parts may be both computer identifiable, as in metadata, and/or human identifiable (graphical) when rendered on a viewing screen or printer.

  The physical structure relates to the format of the record, such as the type font, spacing, page margins, logo, and the "encoding" or format of the file, which provide information for processing (rendering) or transferring of the record over the retention period.

- **Context**

  Context is the meaning of the record, or the "what" and "why" of the business transaction from which the record was created or received. The context may be implicit in the content and structure of the record, such as a patent or trademark application form which contains a form number, or phrase and a signature block which states the *intent* of the signer. The context may also include the general environment within which the records are stored and managed, e.g., records managed within a patent or trademark case file, or case files that are managed as part of a larger PTO case file repository.

One of the key requirements for admissibility as evidence in a Federal court is that the system receiving or creating the record store an "accurate" representation of the record. A record is more likely to be perceived as accurate and reliable and, therefore, trustworthy when as many elements of the record as possible are documented. The more "complete" a record can be shown to be, the more likely it would be considered "authentic" (that it is what it purports to be) for purposes of admissibility as evidence, and the more weight it would likely carry as evidence.

A record may consist of one or more files (such as in the case of a compound record consisting of a text file and a graphics file) with the content, structure and context of each being separately identified, either as part of the record or as metadata about the record and files. The electronic

case file or electronic file wrapper will consist of one or more records with the content, structure and context of each record being separately identifiable.

4.5 CASE FILE AND FILE WRAPPER

For purposes of this Checklist, the terms “case file” and “file wrapper” are used synonymously. The records for patent and trademark applications are and will continue to be managed in case files or file wrappers, whether paper or electronic.

4.6 RECORD RETENTION

The 1997 PTO Comprehensive Records Schedule provides the guidelines for the retention of patent and trademark case files. The specific retention schedules are covered in Section 5.10 Records Retention. Retention periods vary based on the status of the case file, i.e., whether the patent is issued or abandoned, or whether a trademark is registered or abandoned, and also based on the period of time during which the application was filed.

The retention period for which the PTO has responsibility may, in some cases, be shorter than the full retention period for the record as determined in conjunction with NARA. For instance, in the case of selected, granted patent case files, the full retention period is “permanent”, however, the PTO’s period of responsibility is for 40 years from the date of issuance, after which the records and the responsibility for disposition are transferred to NARA.

4.6.1 Case File Retention

For the scheduling of records retention, the complete electronic patent or trademark case file or file wrapper is assigned a single retention period. Accordingly, all of the electronic records in the case file can be managed and retained as a single entity.

4.6.2 Retain Only One Record Copy

For operational and for legal purposes only one "record copy", plus a vital records disaster backup copy, of an electronic record and electronic case file should be retained.

From an operational perspective, having a single record copy of the electronic case file avoids any confusion as to what the "official file copy" is and also may avoid someone retaining and accessing a copy that is not up-to-date. This means that copies retained purely for reference should be deleted at the earliest practical point in time. Also, working files should either be committed to the electronic case file if they meet the criteria as defined in 36 CFR 1222.34 (c), or they should be deleted at the earliest practical point in time.

From a legal discovery perspective, *all* records pertaining to a subpoenaed subject matter, such as one or more specific patent or trademark applications, are discoverable and must be produced if requested. As such, any reference copies or working files that have not been deleted are subject to discovery and must be searched, retrieved and produced if requested.

4.7 USAGE PERIODS

When viewed from the perspective of records management, there are two logical, progressive periods of time in the life of an electronic patent or trademark case file.

1) **In-Process and Use**: This period defines the "pending" period for a patent or trademark application. During this period, the electronic file wrapper and all electronic records are being managed by the AISs and the associated work flows that control the filing, reviewing, examination, and the issuance, registration or abandonment processes.

2) **Maintenance and Use**: This period defines the management of electronic patent and trademark case files subsequent to the issuance of a patent, the registration of a trademark or the abandonment of either. In the current paper process, this is the point when the case file is transferred to a PTO repository and enters a "maintenance" period for the remainder of the authorized retention period prior to being transferred to NARA. It is also at this point, that the case file where a retention period for the case file is established.

During the maintenance and use period, electronic records and associated metadata may be added to the case file, such as assignments, or certain metadata may be added or updated, such as the address of the applicant or inventor. It is also during this period when the migration and retention management events would are most likely to occur, such as media renewal and transfer to another hardware, software or application system, or to NARA or the disposal of records at the end of the retention period. On an exception basis, the electronic case file may be subjected to a more active process, such as a reexamination, or a appeal or interference proceeding.

5 REQUIREMENTS

This section defines and describes the requirements for electronic records management over the complete life cycle of patent and trademark case files. The following requirements areas are addressed:

- Records Acquisition
- Metadata
- File Management
- Preserve Integrity
- Protect Confidentiality
- Access Controls and Authentication
- Search, Retrieval and Reproduction
- Audit Trail
- Vital Record Backup and Recovery
- Records Retention
- Migration
- Transfer to NARA
- Records Hold

5.1 RECORDS ACQUISITION

The capture of electronic records by PTO application information systems (AIS) applies to all documentary materials that meet the tests for a record copy, including records received or created electronically and those received and converted from paper or microfilm to electronic form. The preciseness and reliability of the acquisition process is critical to obtaining an accurate and complete electronic record . . a record that preserves the content, structure and context of the information.

5.1.1 Capture of Complete Electronic Records

It is important to acquire a complete electronic record: a) to ensure that an accurate copy of all elements of the record are captured and b) to ensure long-term processibility and transferability.

There are also legal precedents that establish the need to capture a complete electronic record. An example is the *Armstrong v. Executive Office of the President*, wherein the court concluded that the paper e-mail printouts did not contain some information that was a part of the electronic record, such as the date and time the message was delivered, the list of recipients, etc. Thus, the court concluded that the paper printout did not satisfy the requirements of a complete record for retention as evidence purposes because it excluded certain critical content and contextual information.

The requirements for capturing a complete record are:

- ❑ Provide for the capture of all received and created electronic records that meet the tests of a record copy and commit the records to an electronic patent or trademark case file or file wrapper. Such records might include:
  - ❑ Records received from an applicant.
  - ❑ Office actions created by an examiner.
  - ❑ Communications between the examiner and the applicant, including e-mail.
  - ❑ Working files that meet the tests of 36 CFR § 1222.34 (c).
  - ❑ Other documentary materials that are *appropriate for preservation*.
- ❑ The act of "committing" documentary patent or trademark material as a record copy to a case file should be a distinct, conscious and auditable event.
- ❑ Capture the content, structure and context of each record.
- ❑ Capture attachments and addenda as separate records such that they do not alter the record to which it is linked.
  - ❑ Logically link the attachment or addenda to the associated record copy.
- ❑ Capture metadata associated with the electronic case file and records that allows for search, retrieval, routing, confidentiality status, migration and retention management. (see Section 5.2, Metadata)
- ❑ Establish file format standards for receiving, creating and storing records that are processible and transferable for the full retention life of the record.
- ❑ If multiple renditions (same content but different file format, such as a MS Word and an XML rendition of the same document) of the same record are captured, each should have the same content, structure and context.

5.1.2 Capture Links to Notes and Annotations

- ❑ Capture notes and annotations as "logical" additions to the record and ensure that they do not alter the content or structure of the record.
- ❑ Allow users to position notes and annotations on the document in a meaningful location. Retain the location of the annotation, like a bookmark.

- ❑ The electronic record should be viewable and reproducible at any time without the notes or annotations.

5.1.3 Capture Hyperlinks

- ❑ Capture hyperlinks within an electronic record that refer to another part of the same record.
- ❑ Capture hyperlinks within an electronic record that refer to other electronic records within the same case file.
- ❑ Hyperlinks to electronic records outside of the electronic case file should not be allowed, unless a method is provided to update the hyperlinks whenever the record location or the record or hyperlink changes.

5.1.4 Working Files

Capture working files when they meet the requirements for preservation as a record copy as stipulated in 36 CFR § 1222.34:

> (c) *Working files and similar materials.* Working files, such as preliminary drafts and rough notes, and other similar materials shall be maintained for purposes of adequate and proper documentation if:
>
> (1) They were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action recommendation, follow-up, or to communicate with agency staff about agency business; and
>
> (2) They contain unique information, such as substantive annotations or comments included therein, that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions or responsibilities.

Electronic working files are managed outside of the case file until it is determined that they are to become a record copy, then they are committed to and managed as part of the case file.

- ❑ Establish a process for committing a working file as a record copy, per the definition in 36 CFR § 1222.34, above.
- ❑ Utilize version control to capture and track the creation history of working files and link successor records to the predecessor records.

5.1.5 Conversion of Paper Records to Electronic Form

When it is required that documentary materials in paper form be converted to electronic form, specific guidelines should be followed in order to ensure that accurate and complete records are captured and that the process is consistent and reliable.

- ❑ Ensure that the scanning resolution for image capture is sufficiently high to capture a readable, usable and reproducible copy of the original.
- ❑ Perform a high level of quality control to ensure that accurate and complete records have been captured.
- ❑ Periodically test the scanners to ensure that they are operating according to manufacturers specifications and are producing the desired quality level for the documents being scanned.
- ❑ Provide a means to rescan documents that quality control has shown to be of insufficient quality, or mark the documents prior to scanning as “best copy”.
- ❑ Track the batch number for both the imaged and paper documents as a means of accessing any documents determined to be of insufficient quality.

5.1.6 Quality Control

A quality control step should be an integral part of the record capture process, independent of whether the documentary materials are being scanned from paper or are being automatically acquired from electronically received or created sources.

- ❑ As an integral part of the capture process, conduct quality control on a sample of the captured records, whether scanned from paper or acquired from electronically received or created sources.
- ❑ The sampling level required will depend on the quality level of: a) the source materials, higher for image-scanned paper and lower for documents acquired from electronic sources, and b) the error levels encountered during the quality process. Sampling rates should be adjusted to reflect the level of errors per sample determined during the quality control process.
- ❑ For records captured from paper, a thorough quality control should be conducted to ensure accurate, complete and readable information is acquired from the original paper document.
- ❑ If OCR is used to convert scanned image documents to computer readable format, the converted text should undergo a thorough of quality control.
- ❑ For records captured from an electronic source, the sampling level would normally be lower, depending the accuracy and completeness of prior samples.

5.1.7 Quality Assurance

In addition to the quality control process, a quality assurance sampling process should be conducted by the PTO to ensure that all records were accurately and reliably captured. The sampling level can generally be lower than that used for quality assurance, unless the observed quality level of the captured records warrants an increased sample size.

- ❏ Regularly conduct a final quality assurance process as the means of being certain that all records and associated metadata are being accurately and reliably captured.
- ❏ It is preferable that the PTO conduct the final quality assurance, particularly if a third party contractor is performing the record capture and/or quality control.

5.1.8 Audits

PTO personnel should periodically conduct audits of the document capture process to ensure that all procedures and guidelines are being followed and that accurate and reliable records and associated metadata are being acquired.

- ❏ Conduct period audits of all elements of the document capture process and adjust scanning, quality control and assurance procedures and levels accordingly.

5.2 METADATA

Metadata can be defined as “data describing stored data”, that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records. Traditionally, the term "metadata" has been widely used to characterize the descriptive information that supports search and retrieval of both hardcopy (paper and microfilm) and electronic material. Over the last three or four years the use of the term metadata has expanded to include additional information, such as file formats and creation sources, that must be acquired and retained in order to effectively manage electronic records over long periods of time, including permanent retention.

5.2.1 Legal Requirements

Provisions for locating and retrieving electronic case files and the individual records contained therein are required by law. Minimum guidelines for metadata are specified in the Department of Defense (DOD) directive DOD 5015.2. - Design Criteria for Electronic Records Management Software.

36 CFR § 1220.36 states that Federal agencies must adequately control and maintain its records:

> 36 CFR § 1220.36. **Maintenance and use of records.** Adequate records management controls over the maintenance and use of records shall be instituted to ensure that permanent records can be

> located when needed and that they are preserved for eventual transfer to the National Archives of the United States.

36 CFR § 1234.22 specifies that electronic text documents must be indexed or searchable by text:

> 36 CFR § 1234.22. **Creation and use of text documents.**
>
> (a) Electronic records systems that maintain the official file copy of text documents on electronic media shall meet the following minimum requirements:
>
> > (1) Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system . . .

5.2.2 Metadata Management

The records for patent and trademark applications are managed in case files or file wrappers, whether paper or electronic. The metadata required to provide accessibility, auditability and transferability of the electronic records must also be managed in conjunction with the case file. It is recommended that the metadata be integrated or encapsulated in the electronic case file.

5.2.2.1 Metadata Retention

The retention management requirements for the electronic case file and records must also be applied to the related metadata.

- One of the fundamental requirements for long-term access and retention of metadata is that it must be retained for the same period of time as the electronic case files and records. This includes maintaining the accuracy and completeness of all case file and record-related metadata through media renewals and through transfers to new hardware or software or new application information systems, and transfers to NARA.

5.2.2.2 Metadata Profiles

It is recommended that the following metadata record profiles be implemented and that metadata elements be defined, acquired and retained for the following areas:

Case File and Case File Records profiles: These profiles contain metadata for storage, search and retrieval, confidentiality and tracking accesses.

Use History (see Section 5.8 Audit Trail): This profile documents an audit trail of events and actions (such as accesses to and migrations of electronic patent case files) in order to provide a basis for: a) establishing the reliability and general trustworthiness of electronic patent and trademark case files and records, b) use in meeting the test of authenticity in admissibility, and c) for tracking or researching events related to proving that integrity has been preserved or that confidentiality has been protected.

Copy, Reformat and Transfer profiles (see Section 6.3 Migration): These profiles document the copy or reformat of electronic case files in the event of media renewal; the transfer to a new hardware and software system or AIS; or the transfer to NARA. These three metadata profiles are based on the analysis and definitions documented in the report produced for Task Order 98-03, Deliverable 98-03-10 *Long-term Access and Migration Strategy*, December 24, 1998.

The Metadata Profiles do not identify *how* each metadata element should be captured. Nonetheless, it assumes that many metadata elements, such as those for the Case File Profile and Case File Record Profile could be automatically acquired from the PALM and TRAM replacement databases. Many of the other metadata elements, such as access dates, may be supplied automatically by the AIS or, as a last resort, via manual data entry.

5.2.2.3 Case File Encapsulation

It is recommended, primarily for ease of migration and for auditability purposes, that all metadata information be integrated or encapsulated within the electronic patent or trademark case file or file wrapper. Encapsulation of all metadata as part of the case file provides a "single digital object" that contains the elements necessary for accessing and for tracking activity related to the case file. Encapsulation also makes it easier to identify all information that needs to be migrated in the event of media renewal or the transfer of case files. Encapsulation can be done using either a logical or physical approach.

Logical encapsulation: "Links" all of the records, annotations and notes, and metadata profiles that comprise a case file as a "logical" single digital object. However, the records and metadata related to a case file may reside on different storage servers and different media volumes. While

logical encapsulation may represent the most flexible method for storage, it creates a potentially complex management environment and, as such, a higher risk of loss or corruption when performing media renewal or transfer of case files.

Physical encapsulation: Means that all of the information associated with a specific electronic patent case file, such as the records, related annotations and notes, metadata, and intra-or inter case file or record linkages, exists as a single physical object or entity residing on the same volume of media. Physical encapsulation may provide the most straightforward environment for media renewal and transfers of case files, however, it could pose issues related to the resources and time required to keep the case file physically encapsulated.

For a more detailed analysis of logical vs. physical encapsulation of electronic case files, see the report entitled, *Metadata Requirements for Long-term Access and Retention of Electronic Patent and Trademark Case Files*, Task Order Deliverable 98-03-10 dated December 30, 1998.)

5.2.3 Case File and Record Profile Metadata

One of the primary purposes of metadata is to provide an easy and efficient means for retrieval of the electronic records by authorized personnel. One type of metadata is defined as "profile data."[4] The Case File and Case File Record profiles are designed to include information such as: a unique identifier for the case file and each record in the case file, the subject or title of the case file or record, the creator or origin of the record; why, when, and how the record came into existence; accuracy of the source data; source granularity; processing status; use history; and the quality and extent or scope of the resource.

The following guidelines are provided for capturing and managing metadata for purposes of retrieving electronic records.

- ❑ Each electronic case file and each record in an electronic case file should have at least one unique metadata identifier that differentiates them from other electronic case files and records.

[4] Department of Defense Directive 5015.2 Design Criteria Standard for Electronic Records Management Software Applications (hereafter DOD 5015.2).

- ❑ Encapsulate Case File and Case File Record profile metadata in the related electronic case file for effective retention and migration management. (See electronic Case File and Case File Record metadata requirements below).
- ❑ Utilize the PALM and TRAM replacements to provide the primary source of metadata for the Case File and Case File Record profiles.
- ❑ Utilize the PALM and TRAM replacements as the primary database for search and retrieval of electronic case files and records.
- ❑ Provide a link from the PALM and TRAM databases to the electronic case files.
- ❑ Define specific document-type designations that allow for retrieval of only specific records within an electronic case file.
- ❑ Provide for the identification of hard copy records and other non-electronic materials, where relevant, as Case File Record Profiles so that retrievals are kept simple, e.g., one search to identify all records available, regardless of media type or physical location.
- ❑ Provide for electronic case file and record profile information that such that retrievals can comply with the Freedom of Information Act, Privacy Act and Paperwork Reduction Act.
- ❑ Use the Case File Metadata profile to indicate the status of confidential records, e.g., identify confidential, privileged and private records so they can be secured from unauthorized users.
- ❑ Where possible, automatically index all records received or created in accordance with the PTO-wide filing scheme for electronic case files that is to be developed using the metadata profiles defined for Case Files and Case File Records. Specific requirements may include:
  - ❑ Capture record profile metadata by extracting selected fields directly from PALM or TRAM and/or the electronic record. For example, determine the application number and applicant for a patent or trademark application or an office action interpreting and extracting from the metadata defined for a particular record type.
  - ❑ Capture index data from e-mail or other internal and applicant/PTO communication system, e.g., capture the author or originator, addressee, other recipient names, date created, date received, subject, etc.
  - ❑ Automatically capture document type designation codes from electronic records, using the metadata fields or possibly by bar-coding or scanning and OCRing hard-copy forms.
  - ❑ Capture index data by converting an paper form to image, then OCRing and extracting the appropriate metadata fields.
- ❑ For ease of mass retrievals, allow for designation of common predetermined metadata fields, e.g., application number, subject, date, originator, record type or form number, disposition code, etc.
- ❑ No alteration of metadata associated with (or encapsulated with) an electronic case file should be allowed, unless it is determined that the metadata contains errors that must be corrected.
- ❑ Should corrections to metadata be required (such as due to errors induced during automatic or manual data capture), access to and use of modification programs or tools for correcting metadata should be limited and controlled for use only by authorized

personnel. Audit trail information about any changes should be added to the Use History metadata profile.

5.2.3.1 Case File Profile

The recommendations for metadata in the Case Files and Case File Record profiles are based on the needs for filing, retrieval and disposition of electronic patent and trademark records . They take into consideration the requirements delineated in the Code of Federal Regulations (CFR) and synthesize those identified in DOD 5015.2 (see Section 5.2.3.3 below), the University of Pittsburgh "Requirements for Business Acceptable Communications," and the SMPTE Task Force on Harmonized Standards.

The data elements comprising the Case File Metadata Profile capture core information about the case file as a logical entity that supports long-term access and retention management. All of these data elements are considered non-revisable from the moment that they are registered as part of the case file. The only instances where an authorized modification is allowed in the metadata of the case file profile is when there are updates to the case file for error correction, or after issuance, registration or abandonment, such as assignment of rights or reexamination, or if the storage location status changes, or when access dates are transferred from the individual record profile.

CASE FILE METADATA PROFILE

- ❑ Unique Identifier
- ❑ File Type
  - Patent
  - Trademark
- ❑ File Subject
- ❑ Applicant* (may be changed if attorney or agent changes)
- ❑ Inventor(s)* (may be changed via an assignment)
- ❑ Filing Date
- ❑ Closure Date (defines the beginning of the authorized retention period)

- ❏ Process Status Code (pending, issued, registered, abandoned)
- ❏ Representation
  - Binary
  - ASCII
  - EBCIDIC
  - UNICODE
- ❏ Encryption of Case File (optional, if required)
  - Name of Algorithm Used
  - Name of Software and Version Used
- ❏ Formats Used
  - Text
  - Image
  - Vector
  - Compound (e.g. text, vector and/or image combined)
  - Database
  - Audio
  - Moving Image
- ❏ File Formats Used
  - TIFF
  - XML
  - SVG
  - JPEG
  - CNG
  - MPEG
  - Other (e.g., complex work units)
- ❏ Case File Size
  - Logical Record Length
  - Logical Record Count*
  - Physical Record Count*
  - Byte Count*
  - Total Number of Records*

- ❑ Case File Authentication (If Used)
  - Cyclical Redundancy Check (CRC)
  - Hash Digest
- ❑ Updates After the Pending Period*
  - Assignment
  - Reexamination
  - Change of Address
  - Etc.
- ❑ Access/Event Dates List*
  - Date of Access/Event
  - Type of Access/Event
  - I.D. of Access/Event User
- ❑ Location of Case File*
  - In Process and Use
  - Maintenance and Use
  - NARA
- ❑ Location of Paper or Microfilm Records Related to Case File
- ❑ Disposition*
  - Instruction Code
  - Action Date

*Indicates update to the profile is permitted

5.2.3.2 Case File Record Profile

The data elements comprising the case file record profile capture core information about each record as a logical entity that can be used individually or collectively to provide control of the records. For example, the Unique Record Identifier provides for direct access to the record, and the Access/Event Date element contains all instances of access to or other actions related to the record. A specific date can be linked to the Use History Profile, for example, that would disclose if the access was linked to an update, reformat, copy, or transfer activity. Each of these data

elements is considered non-revisable from the moment the record becomes part of a case file. The only instance of a change that could occur in the case file record profile is when access dates are added. An asterisk ("*") identifies these instances.

CASE FILE RECORD METADATA PROFILE

- ❑ Case File Unique Identifier
- ❑ Unique Record Identifier (e.g., serial number)
- ❑ Record Descriptor (form number, alpha code)
- ❑ Date Received/Created
- ❑ Name of Record Recipient/Addressee
- ❑ Subject
- ❑ Originating Organization
- ❑ Author
- ❑ Security Level (Pending, Issued, etc.)
- ❑ Representation
  - Binary
  - ASCII
  - EBCIDIC
  - UNICODE
- ❑ Encryption of Record (optional, if required)
  - Name of Algorithm Used
  - Name of Software and Version Used
- ❑ Formats Used
  - Text
  - Image
  - Vector
  - Compound (e.g., text and vector)
  - Database

- Audio
- Moving Image

❏ File Formats Used
- TIFF
- XML
- SVG
- JPEG
- CNG
- MPEG
- Other (e.g., complex work units)

❏ Record Size in Bytes

❏ Record Authentication (If Used)
- CRC
- Hash Digest

❏ Access/Event Dates*
- Date of Access/Event
- Type of Access/Event
- I.D. of Access/Event User

*Denotes that updates are permitted

5.2.3.3 DOD 5015.2 Record Profile Metadata

A general reference point for the minimum metadata elements that should be used for electronic records management in a government agency is the DOD 5015.2. This directive is gaining wide visibility and increasing acceptance as a base set of guidelines for the management of electronic records in Federal agencies as well as in academic and commercial organizations. The metadata defined in this directive has been used as one baseline for determining the recommended Case File and Case File Record metadata profiles defined above. The recommended set of metadata fields for identifying and filing records set forth in this directive are:

- Subject

- Date Filed
- Addressee(s)
- Media Types
- Format
- Location of Record
- Document Creation Date
- Author or Originator
- Originating Organization
- Other Recipients (e-mail)
- File Code (from PTO Retention Schedule)
- Vital Record Indicator
- Disposition Instruction Name
- Disposition Instruction Code
- Disposition Instruction Type (Time, Event, Time-Event)
- Disposition Cutoff Date
- Disposition Action Date
- Disposition Action Code (Transfer, destroy or freeze)
- Record Identifier
- User definable fields

Also consider the following metadata for indexing and retrieval:

- Keywords or phrases
- Description or abstract of record
- Access security level for the record

5.3 FILE MANAGEMENT

The file management system must protect the physical and referential integrity of electronic case file and records and associated metadata over the full life cycle. The file management system must protect an electronic record and associated metadata from being overwritten or inadvertently deleted. It should also provide the means to enable access to electronic case files,

records and metadata for the full retention period, independent of the storage media - - digital, paper or microfilm.

- ❑ The file management system must not allow electronic case files and records or related metadata to be overwritten or inadvertently deleted.
- ❑ Using access controls, the disposal of electronic records and associated metadata should be restricted to specific personnel who are authorized by the PTO Records Officer to destroy or transfer case files and metadata.
- ❑ For accessibility purposes, a unique link or pointer should be created and maintained between the retrieval and tracking database (such as PALM or TRAM), the file management directory and/or the metadata, and the physical location of the electronic case file and records.
- ❑ For the vital records backup of electronic case files and records and related metadata, provide a link or pointer between the retrieval and tracking database (such as PALM or TRAM), the file management directory and/or the metadata profiles, and the physical location of.
- ❑ Capture metadata to locate any records related to a case file that are maintained only in physical form (such as sequence listing or other attachments, sometimes referred to as "bulkies" or "jumbos"), or on physical media (such as diskettes or CD-ROM), or odd-sized specimens for showing current or intended use of a trademark.

For management of physical storage media, see Section 5.11.2 Media Management.

5.4 PRESERVE INTEGRITY

Integrity means ensuring consistency of data, in particular, preventing (including detecting) unauthorized alteration or destruction of data.

Maintaining the integrity of patent and trademark records is required by law (18 U.S.C. § 2071. Concealment, removal, or mutilation generally). There are regulations that also require preservation of records integrity.

36 CFR § 1234.22 specifies that the integrity of electronic records must be protected:

> 36 CFR § 1234.22. **Creation and use of text documents.**
>
> (a) Electronic records systems that maintain the official file copy of text documents on electronic media shall meet the following minimum requirements:

> . . .
>
> (2) Provide an appropriate level of security to ensure integrity of the documents;
>
> . . .

Further, maintaining the integrity of patent and trademark records is essential for ensuring the protection of the intellectual property rights and the value of the inventor's business assets. For these reasons, checks and balances must be in place to assure the preservation of the integrity, authenticity and trustworthiness of the PTO's records over time. This may be accomplished by managing and protecting the electronic records from any loss, alteration, removal, or premature destruction. Since evidence of record tampering may not be as readily identifiable with electronic records, as it might be with paper records, it is even more important that the controls are in place to adequately protect and preserve the electronic record.

5.4.1 Protect Against Alteration

- ❑ Access controls to electronic case files and records should be applied on a "least privilege" basis with access limited based on the role or function of an individual.
- ❑ No alteration of the content, structure and context of a record committed to an electronic case file will be allowed. The integrity of each record must be preserved for the full retention period of the case file.
- ❑ Any annotations and addenda related to an electronic case file or record should also be protected from alteration or loss and should be maintained as data that is separate from, but logically linked to the record - - so that an electronic record can be viewed or reproduced in the original manner it was stored.
- ❑ No alteration of metadata associated with (or encapsulated with) an electronic case file or record should be allowed, unless it is determined that the metadata contains errors that must be corrected.
- ❑ Should corrections to metadata be required (such as due to errors induced during automatic or manual data acquisition), access to and use of modification programs or tools for correcting metadata should be limited and controlled for use only by specifically authorized personnel, and an audit trail of any modification activity should be tracked in the Use History metadata profile.
- ❑ If new electronic records are to be created using an existing electronic record as the basis, the new electronic version must be committed to the electronic case file as a new record with new case file record profile metadata. Version controls (such as check-out/check-in procedures) must be used to ensure that the original electronic record remains unaltered.
- ❑ Access to programs or functions used for destroying electronic case files and records at the end of the authorized retention period (including associated attachments and

annotations, and the metadata) should be limited to persons or system functions specifically authorized by the Records Officer.

5.4.2 Validating Integrity

- ❑ An electronic record should contain some feature, such as a cyclical redundancy check (CRC) or a digital signature hash, that allows the integrity of the record to be validated at the time of each receipt/creation and for each access, and allows for detection of any attempt at or alteration of the record to be detected.
- ❑ Each validation of integrity should be recorded in the Use History metadata profile.

5.5 PROTECT CONFIDENTIALITY

Confidentiality is defined as ensuring that information is not disclosed or revealed to unauthorized persons.

Confidentiality applies only to pending and abandoned electronic patent records and associated metadata, except when the abandoned patent is reference by an issued patent. Confidentiality is not a requirement for trademark records.

Maintaining the confidentiality of pending and abandoned patent records, where required, is mandated by law (35 § U.S.C. 122. Confidential status of applications, and 37 § CFR 1.14. Patent application preserved in secrecy).

Maintaining the confidentiality of pending or abandoned patent case file and record content is crucial because the information is the confidential, and highly valuable intellectual property of the inventor.

The following requirements apply only to protecting the confidentiality of pending and abandoned patent case files:

- ❑ Protect confidential electronic records and associated metadata from unauthorized viewing during transmission, such as using encryption, especially when using a public or open communication network.
- ❑ Protect confidential electronic records during the review, pre-examination, examination, publication steps, and during maintenance of abandoned patents, and ensure that they are not disclosed or revealed to unauthorized persons.
- ❑ Provide a metadata field that indicates when the status of an electronic case file is confidential.

- ❑ Access controls to confidential records should include the ability to restrict access on a "least privilege" basis within one or more specified functions or roles for an individual.
- ❑ Physically secure off-line media that contain confidential records from unauthorized access.

5.6 ACCESS CONTROLS AND AUTHENTICATION

Providing access controls (identification) and authentication (validation of identity) is critical for protecting the confidentiality and preserving the integrity of electronic case files and records. It is required to prevent unauthorized viewing, modification, destruction and, generally, the unauthorized issuing of commands. Access controls should be based on "least privilege" such that it grants users access only to those electronic case files and records, and to associated annotations and metadata, that are minimally required to perform their roles or functions. Controls may selectively limit access to electronic case files and electronic records, to any action or event related to electronic case files, and to specific computing resources related to migration or purging.

- ❑ Provide access controls and authentication, such as a valid user ID/password or PIN combination, public/private key pair or other method, to authenticate the identity of the sender, creator, and user of the record.
- ❑ Identify and authenticate each user at the time of log-on to all patent and trademark AIS systems that receive, create, process, maintain or otherwise manage electronic case files and records.
- ❑ Access controls and profiles should include the ability to restrict access by an individual on a "least privilege" basis to one or more specific functions or roles as well as to selected computing resources based on the process status of the case file.
- ❑ Access should be strictly limited to any AIS or other computing functions or resources that provide for the modification of metadata, creating new versions of documents, and the scheduled purging (deleting) of electronic case files and associated metadata.
- ❑ Utilize an audit trail to track all events related to access of the record, including the detection of unauthorized access attempts.

5.7 SEARCH, RETRIEVAL AND REPRODUCTION

5.7.1 Search and retrieval

- ❑ Search for all case files or records relevant to an authorized request, whether they are stored on on-line, near-line, or off-line media.
- ❑ Search options should include:
  - ❑ Searching the metadata for a specific "case file".
  - ❑ Searching a case file for a specific record.
- ❑ Allow for a variety of types of searches:
  - ❑ Linguistic-based word matching, e.g., knife or knives; record keeping, recordkeeping, or record-keeping.
  - ❑ Boolean searches, e.g., water AND H_2O.
  - ❑ SQL expressions, e.g., like, contains, etc.
- ❑ Incorporate features to ease screening for Freedom of Information Act, Privacy Act and Paperwork Reduction Act requirements.

5.7.2 Store Search Results

- ❑ Allow users to store the search results as a record, e.g., a list of all patents that were reviewed during a search process of a patent application examination.
- ❑ Allow users to temporarily store and then retrieve from search results until a business task or event is complete.

5.7.3 Display/Print the Record, the Index and Annotations

- ❑ Ensure that a human–readable copy (screen display and hard-copy) of the complete record can be generated over the life of the record.
- ❑ Display/print options should include any combination of the following:
  - ❑ Display/print of the record.
  - ❑ Display/print of the annotations.
  - ❑ Display/print of Case File and Case File Record metadata.
- ❑ Notes and annotations should be distinguishable from the record.
- ❑ The record should be able to be printed or displayed with annotations on the record, annotations following the print of the record, or no annotations.
- ❑ Provide for zooming in and out to easily distinguish hard-to-read text and graphics.

5.7.4 Applicant Access

Where access to electronic case file, records and/or metadata information is provided, such as through the Trademark Application and Registration Retrieval (TARR) or the Patent Application Retrieval and Review (PARR), measures must be taken to restrict access only to the records and metadata that an applicant is authorized to view. The integrity of the electronic case file records and metadata must be preserved, and the confidentiality of pending patent application information must be assured.

- ❏ Provide a means of identifying and authenticating the applicant.
- ❏ Provide a means of restricting access to only those case files, records and/or metadata that the applicant is authorized to access and view.
- ❏ Log all accesses by applicants in the Use History Metadata Profile as an audit trail of these events.

5.8 AUDIT TRAIL

An audit trail, also know as an event log, is the "chain of custody" that records the "who, what, and when" for each action or event, including creation or receipt, processing, access, distribution, dissemination, migration, transfer and disposal of an electronic patent or trademark case file. As such, an audit trail essentially captures specific metadata that documents the intent and result of activities related to electronic case files and records.

The audit trail can provide an independent (computer-controlled, not human-controlled) element of proof that policies and procedures were followed and that the integrity and confidentiality of the information was not compromised. An audit trail of all incoming and outgoing electronic record communications compiled by the Electronic Mail Room would be a good example.

From a legal perspective, an audit trail can be used as "management data" to help prove the authenticity of a record for admissibility in evidence in an interference or appeal proceeding.

It is recommended that audit trail information for accesses and events related to electronic patent and trademark case files be documented using the metadata in the Use History Profile.

5.8.1 Use History Profile

As set forth in Section 5.2.2.2 Metadata Profiles, it is recommended that a Use History metadata profile be created for each case file, and encapsulated in the electronic case file, as the audit trail of accesses and events related to the case file. The Use History metadata profile logs accesses and events (such as migrations of electronic case files) that provide a basis for: a) establishing the reliability and general trustworthiness of electronic patent and trademark case files and records, b) meeting the test of authenticity in admissibility, including patent and trademark appeals, and c) tracking or researching events related to proving that integrity has been preserved, that confidentiality has been protected, that system procedures have been followed and that the management of electronic records has been conducted in a trustworthy manner. The following metadata are recommended for inclusion in the Use History profile:

USE HISTORY METADATA PROFILE

- ❑ Case File Unique Identifier
- ❑ Event/Activity Date (Repeatable)
- ❑ Access Dates (Repeatable)
- ❑ Reformat (Repeatable)
  - Date
  - Reformat Iteration Number
  - Logical Record Size
  - Logical Record Count
  - Byte Count
  - CRC (If Used)
  - Hash Digest (If Used)
- ❑ Copy (Repeatable)
  - Date
  - Copy Iteration Number
  - Logical Record Count

- Byte Count
- CRC (If Used)
- Hash Digest (If Used)

❏ Transfer (Repeatable)

- Date
- Transfer Iteration Number
- Logical Record Count
- Byte Count
- CRC (If Used)
- Hash Digest (If Used)

❏ Purge/Delete (Optional)

- Date
- Authorization

5.8.2 Use History Profile Creation and Update

❏ Create a Use History Profile at the time the patent or trademark application is filed and log the "filing" event metadata in the Use History Profile.

❏ Each access to an electronic case file should be logged in the Use History profile.

❏ Each event that receives, creates, updates, disposes of or is otherwise material to the prosecution and maintenance of a patent and trademark case file should be logged to the Use History Profile.

❏ Log each copy, reformat and transfer event in the Use History Profile

❏ When retention schedules are applied and case files are disposed of, log the disposition action and date to the Use History File

❏ When case files are transferred to the NARA, log the types of case files transferred, the case file count transferred and the date transferred.

5.8.3 Link to Other AIS Tracking or Event Logging Systems

❏ Link to PALM as the source for the patent access and event information.

❏ Link to TRAM as the source for the trademark access and event information.

- ❏ Link to other work flow or process tracking systems to extract or capture information related to maintenance events, such as reassignments of a patent from one party to another.

5.9 VITAL RECORDS BACKUP AND RECOVERY

Patent and trademark case files are considered vital records, that is, they must be available for purposes of reconstructing the business of the PTO should a disaster occur that damages the primary electronic case files.

To ensure that this vital information is backed up and available, specific policies must be defined and specific procedures implemented and practiced.

A vital records backup copy of all electronic case files and associated metadata must be made and be available for disaster recovery purposes. A backup copy of all AISs and operating software used to manage the electronic case files should also be available for disaster recovery.

- ❏ Develop automated backup policies and procedures for electronic case files, metadata and associated AISs and operating software.
- ❏ Create a vital records backup copy of all electronic case files and records, and related metadata.
- ❏ Create a backup copy of all operating software and AISs that process and maintain electronic case files, records and related metadata software
- ❏ Store all vital records backup copies in a geographically separate location from the primary media.
- ❏ Provide electronic and physical (where appropriate) labeling that allow ready identification of the location of and access means to the backup media.
- ❏ Develop procedures and implement automated and manual capabilities, as required, that allow for full recovery of electronic case files and records and related metadata in the event of a disaster.
- ❏ Maintain metadata and/or file directory that allow access to both the primary and backup media for each electronic case file and records, as well as for any associated hard copy records.
- ❏ Retention management, including disposal of electronic case files and records and related metadata, should be applied consistently for the backup media and the primary media.
- ❏ Secure the vital records backup media and protect it from environmental and other potential harms, including: (a) Ordinary hazards, such as fire, water, mildew, rodents, and insects; (b) Man-made hazards, such as theft, accidental loss, sabotage, and

> commercial espionage; (c) Disasters, such as fire, flood, earthquake, wind, and explosion; and (d) Unauthorized use, disclosure, and destruction.

5.10 RECORDS RETENTION

The PTO is required by law to ensure that electronic case files and records are retained as long as defined, and as approved by NARA.

> 36 CFR § 1234.30. **Retention of electronic records.**
>
> Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government. These retention procedures shall include provisions for:
>
> (a) Scheduling the disposition of all electronic records, as well as related documentation and indexes, . . . The information in electronic records systems, including those operated for the Government by a contractor, shall be scheduled as soon as possible but no later than one year after implementation of the system.
>
> (b) Transferring a copy of the electronic records and any related documentation and indexes to the National Archives at the time specified in the records disposition schedule in accordance with instructions found in § 1228.188 of this chapter. Transfer may take place at an earlier date if convenient for both the agency and the National Archives and Records Administration.
>
> (c) Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle (see § 1234.28).

Further, maintaining the integrity of patent and trademark records is essential for ensuring the protection of the intellectual property rights and the value of the inventor's business assets. For these reasons, checks and balances must be in place to assure the preservation of the integrity, authenticity and trustworthiness of the PTO's records over time. This may be accomplished by managing and protecting the electronic records from any loss, alteration, removal, or premature destruction. Since evidence of record tampering may not be as readily identifiable with electronic records, as it might be with paper records, it is even more important that the controls are in place to adequately protect and preserve the record.

5.10.1 Case File Retention

For the scheduling of case file retention, the complete electronic patent or trademark case file or file wrapper is considered to be a single entity, and, as such, the complete case file can be managed and preserved using a single retention period.

5.10.2 PTO Retention Period

The retention period for which the PTO has responsibility may, in some cases, be shorter than the full retention period for the record. For example the retention period for granted patent applications is permanent, however, the PTO's period of responsibility is for 40 years from the date the patent is granted, after which the case file and the responsibility for its disposition are transferred to NARA.

The PTO retention schedules for records (hard-copy and electronic) are developed in conjunction with and are approved by NARA. A number of Federal regulations developed and issued under the auspices of NARA provide guidance for the preservation and disposal of Federal records.

36 CFR § 1228.10 requires Federal agencies to maintain a records disposition program.

> 36 CFR § 1228.10. **Authority.** The head of each agency (in accordance with 44 U.S.C. 2904, 3102, and 3301) is required to establish and maintain a records disposition program to ensure efficient, prompt, and orderly reduction in the quantity of records and to provide for the proper maintenance of records designated as permanent by NARA.

36 CFR § 1228.50 states that it is mandatory for Federal agencies to apply approved retention schedules.

> 36 CFR § 1228.50. **Application of schedules.** The application of approved schedules is mandatory (44 U.S.C. 3303a). The Archivist of the United States will determine whether or not records may be destroyed or transferred to the National Archives. **. . .**

36 CFR **§** 1234.20 requires that disposition instructions be incorporated into the design of every automated information system:

> 36 CFR § 1234.20. **Creation and use of data files.**
>
> (a) For electronic records systems that produce, use, or store data files, disposition instructions for the data shall be incorporated into the system's design . . .

5.10.3 PTO Case File Retention Schedules

Retention periods for patent and trademark case files and records, whether electronic or paper-based, can be described as "event driven".

For example, a retention period does not start until the prosecution of a pending patent or trademark application is completed - - that a patent has been granted, a trademark has been registered or that a patent or trademark application has been abandoned. Also, the duration of the retention period is dependent on whether the patent was granted or abandoned, and whether the trademark was registered or abandoned, or has expired or been cancelled.

Retention periods as taken from the PTO Comprehensive Records Schedule, 1997 are:

For Patent Case Files:

14.00 Patent Case Files

Case files showing the prosecution of applications for, and the granting of, a patent. Files include the original application, the patent drawing, and all materials relating to the prosecution of the application and subsequent actions by the PTO. Includes patent files for reissues.	
a. Closed (granted) patent case files selected by the Commissioner of Patents and Trademarks and the Archivist of the United States.*	a. Permanent Transfer to NARA after 40 years
b. All other closed (granted) patent case files.	b. Destroy 40 years after closure.

1.00 Abandoned Applications

Applications that do not result in the grant of a patent. Abandonment occurs when the applicant ; fails to pay fees or submit documentation requested by the examiner within the allowed time; when claims made for the invention are not patentable or were previously patented; or when another applicant has filed an application for the same invention and can demonstrate an earlier date for the conception of the invention.	
a. Applications retained because they are referred to in another application that may have become registered.	a. Dispose of with Patent Case file in which cited. *
b. (1) Abandoned Applications dated before June 8, 1995. (2) Abandoned Applications dated on or after June 8, 1995.	b. (1) Destroy 20 years after closure. (2) Destroy 23 years after closure.

* Ed. Note: Currently, all patent case files are “selected” and retained permanently.

For Trademark Case Files:

It should be noted that when a trademark application is registered, the case file is maintained by the PTO until the trademark is cancelled or expires, which could result in permanent retention.

18.00 Trademark Case Files

Case files showing the prosecution of applications for, and the registration of, a trademark. Includes the original application, copy of drawing, and all materials relating to the prosecution of the application and subsequent actions by the PTO. Maintained in Publication and issue until all office action is complete and printed registration is received. Used to record cancellation and expiration of trademark. Also used to record disallowance or non-prosecution by applicant.	
a. Cancelled or expired registrations	
(1) Selected Files.	(1) Permanent Transfer to NARA after 6 years.
(2) Non-selected Trademark Files.	(2) Destroy 2 years after cancellation or expiration.
b. Abandoned applications.	
(1) Selected Files.**	(1) Permanent Transfer to NARA after 6 years.
(2) Non-selected Trademark Files.	(2) Destroy 2 years after cancellation or expiration.

** Ed. Note: For Trademarks, only the case files for specifically selected marks will be transferred to NARA.

5.10.4 Determine Retention Period

As can be noted from the retention schedules above, the business rules for determining the retention periods for Patent and Trademark case files, records and associated metadata are relatively straight forward. The AIS responsible for the event that triggers the start of a retention period, such as the granting of a patent or the registration of a trademark, should populate the appropriate Disposition metadata fields in the Case File Profile.

- ❏ The AIS responsible for an event that triggers the beginning of a retention period should automatically determine the values for and populate the Disposition attributes "Instruction Code" and "Action Date" in the Case File Profile with the appropriate retention information.
  - - Instruction Code relates to an action, such as "disposal", "transfer" or "hold".
  - - Action Date is the date that the "instruction" is to occur.

- ❏ Any modifications to disposition attributes should be restricted to personnel that are authorized by the PTO Records Officer, and should be tracked as part of the Use History Profile metadata for each case file.

- ❏ Under authorization by the PTO Records Officer, provide for the capability to perform selective, mass updates to the Disposition attributes, such as when retention schedules are modified in conjunction with NARA. For example, if the transfer period to NARA for granted patents was changed from 40 years to 30 years, allow for the mass change of the transfer "Action Date" to NARA for all affected case files.

5.10.5 Records to be Retained

- ❏ All documentary materials received or created by the PTO that meet the criteria of 44 USC § 3301, and working files that require preservation based on the guidelines in 36 CFR § 1222.34 should be stored and the integrity preserved for the full retention period.

- ❏ Only one legal record copy, plus a vital records disaster backup copy, of each electronic case file and record, including related metadata, should be retained.

  This eliminates the risk and burden of responding to legal discovery actions by needing to retrieve and provide "all copies of the requested information". It also prevents any confusion and risk regarding whether the most recent or "record copy" version of the record is being accessed.

- ❏ Ensure that the content and structure of the record in preserved such that a human readable display or print of the data can be reconstructed over the life of the record.

- ❏ Preserve the context (the circumstances under which the record was generated and stored) over the full retention period.

- ❏ Ensure that the chosen record format(s) will provide for record availability for the full retention life of the record, such as an industry standard or widely supported defacto standard file format.

5.10.6 Disposal

36 CFR § 1220.38 requires Federal agencies to preserve permanent records and to promptly dispose of or retire temporary (non-permanent) records.

> 36 CFR § 1220.38. **Disposition of records.** Provision shall be made to ensure that permanent records are preserved but that records no longer of current use to an agency are promptly disposed of or retired. Effective techniques for the accomplishment of these ends are the development of records disposition schedules; the transfer of records to records centers and the National Archives of the Unties States; the conversion of the information to

other media; and the disposal of valueless records. Disposition of any records requires the approval of the Archivist of the United States (see Part 1228 of this chapter).

The requirements for disposal of electronic case files and records, and associated metadata and backup copies are:

- ❑ Provide for access to and screening of the disposition action for case files by authorized personnel using the Disposition – Action metadata in the Case File Profile.
- ❑ Periodically produce electronic or hard copy lists for approval of case files whose action codes and dates indicate a pending disposal - - produced either automatically based on predetermined criteria or upon manual initiation by authorized personnel.
- ❑ Provide for electronic approval of disposal actions, either using disposal lists or via manual entry by personnel authorized by the PTO Records Officer.
- ❑ Provide for a "confirmation" action prior to actually beginning the disposal of case files and records.
- ❑ Provide for the electronic initiation of the disposal process for a specified list of case files, either using an AIS or employing a separate utility specifically designed for disposal actions.
- ❑ Disposal audit trail - extract and save, for a to-be-specified period of time, a subset of the Use History Profile metadata documenting the disposal action taken for each case file.
- ❑ Disposal of a case file should include the complete contents of the case file, all metadata associated with the case file, and the vital records backup of the case file.
- ❑ Disposal should include complete physical destruction (overwrite with unintelligible characters or disposal of a unit of media) of all case file information, not just logical deletion of metadata and pointers to the case file.
- ❑ A sampling of attempted accesses to disposed case files should be conducted in order to assure that the disposal action has been accurately and completely carried out.
- ❑ If a case file or record is hyperlinked to another case file, such as an abandoned patent case file referenced by an issued patent, the abandoned case file should be deleted only when it is eligible for deletion by the referencing case file.
- ❑ Do not delete case files that are the subject of an in-force hold order, which should be reflected in the Disposition metadata of the Case File Profile.

5.10.6.1 Disposal of Working Files

Working files are managed outside of the electronic case file, however, they should be disposed of at the earliest opportunity. Working files should be deleted when the prosecution of the patent or trademark application is completed (issuance, registration or abandonment), or earlier when

they have no expected reference value and are not subject to a hold order. Authorization from NARA is not required to delete working files that are not considered necessary for preservation based on the guidelines stipulated in 36 CFR § 1222.34.

- ❑ Provide a method for authorized users to dispose of working files that are not required for preservation as records by the PTO or by the guidelines provided in 36 CFR § 1222.34.
- ❑ Deletion should include complete physical destruction (overwrite or disposal of a unit of media) of all case file information, not just logical deletion of pointers to the case file.
- ❑ Do not track the disposal activity of working files in the Use History Profile audit trail.

5.11 MIGRATION

Electronic patent and trademark case files must remain accessible and transferable despite changes in information technology. The content, structure and context of the electronic records must be able to be displayed, printed or otherwise reproduced, as they originally were captured, for the complete life cycle of the record.

36 CFR § 1234.28 requires agencies to guard against the loss of information because of technological obsolescence:

> 36 CFR §1234.30 **Selection and maintenance of electronic records storage media.**
>
> (a) Agencies shall select appropriate media and systems for storing agency records throughout their life, which meet the following requirements:
>
> (3) Retain the records in a usable format until their authorized disposition date; and
>
> (4) If the media contains permanent records and does not meet the requirements for transferring permanent records to NARA . . . , permit the migration of permanent records at the time of transfer to a media which does meet the requirements."
>
> (e) Agencies shall ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion.
>
> . . .

Regulations requires agencies to manage its media and regularly recopy, reformat, etc. to ensure the retention and usability of the data.

36 CFR § 1234.32. **Retention and disposition of electronic records.**

(a) Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government. These retention procedures shall include provisions for:

. . .

(c) Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle (see § 1234.28).

5.11.1 Copy, Reformat and Transfer

Technology is certain to change and advance with a frequency that will require multiple migrations of electronic patent and trademark case files and records over most retention periods. This will include the copying and reformatting of the case files to new media and/or the transfer to new AISs or new hardware and software.

- ❑ Develop a strategy and plan, and allocate future funding, to accomplish the copying, reformatting or transfer of electronic case files in a timely and accurate manner, since a break in the migration cycle may make the electronic records effectively irretrievable.
- ❑ The content, structure and context should be accurately preserved through copy, reformat and transfer migrations.
- ❑ Copy and reformat, if required, electronic case file records at the time they are moved from one AIS or one software and or hardware system environment to another.
- ❑ Reformat electronic case files, as required, when new storage devices or media are utilized.
- ❑ When using magnetic tape for either the primary or vital records backup, annually read a statistical sample of all reels of magnetic tape . . . to identify any loss of data and to discover and correct causes of data loss (36 CFR § 1234.30 (g) (4)).
- ❑ When using magnetic tape for either the primary or vital records backup, copy the electronic case files when the annual readability sample of magnetic tape discloses ten or more temporary or read errors.
- ❑ When using magnetic tape for either the primary or vital records backup, copy electronic case files every ten years (36 CFR 123430[g][5]) for the primary and the vital records disaster backup.
- ❑ Transfer electronic patent case files when the current software is upgraded or a new or upgraded electronic records file management system is installed.
- ❑ Ensure the reliability and integrity of reformatted, copied, and transferred electronic patent case files by employing a strict quality control procedure that may include bit/byte comparisons and comparisons of hash digests and Cyclical Redundancy Check (CRC)

- ❑ Document fully all actions taken when reformatting, copying and transferring electronic patent case files and include this information in the Use History Profile metadata associated with each case file.

- ❑ Provide for vital records backup and disaster recovery by creating two copies of electronic patent case files at the time of reformatting, copying, or transfer and store one copy at a separate geographical location.

Transfer of electronic case files to NARA is covered separately in Section 5.12.

5.11.2 Media Management

The manufacturer's specifications for both the *"pre-written"* media life and the *"post-written"* archival life must be followed.

- ❑ Determine and follow the media manufacturer's specifications for pre-written and post-written life.

  The *pre-written* media life is the time period from the date of manufacture until the date after which the *initial* writing of information to the media is not recommended. The *post-written* archival life is the period from the date of manufacture until the media should be copied to a new unit of media.

- ❑ Store the physical media in accordance with the manufacturer's environmental requirements for temperature and humidity controls, etc.

- ❑ Periodically check the media for read-errors and read-error correction rates, even if the manufacturer's specifications for temperature and humidity controls are followed.

- ❑ When read-error correction rates meet or exceed the tolerance level or when the post-written archive life is imminent, copy the digital data to "fresh" media. This practice of copying the records before the media expires is an effective preservation technique only as long as the existing media is readable.

5.12 TRANSFER TO NARA

36 CFR § 1234.30 requires agencies to plan for the transfer of electronic records and index to NARA.

> 36 CFR § 1234.30. **Retention of electronic records.**
>
> Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government. These retention procedures shall include provisions for:
>
> . . .

(b) Transferring a copy of the electronic records and any related documentation and indexes to the National Archives at the time specified in the records disposition schedule in accordance with instructions found in § 1228.188 of this chapter. Transfer may take place at an earlier date if convenient for both the agency and the National Archives and Records Administration.

. . .

5.12.1 Transfer

- ❏ Transfer only the "selected" electronic case files and records and associated metadata to NARA, as designated by the Instruction Code and Action Code in the Case File Profile.
- ❏ Generate all required forms to transfer records, such as the Standard Form (SF) 135.
- ❏ Provide for the transfer of case files and records into the file formats and media types that are approved by NARA.
- ❏ Verify the quality of the records and associated metadata being transferred.
- ❏ Update the Transfer Profile metadata as a means of keeping a detailed audit trail of records transferred to NARA - - and also transfer the Transfer Profile metadata to NARA as documentation of the successful transfer and for future reference.

5.12.2 Media and File Format Requirements

NARA currently accepts only selected types of media and file formats for transfer. Thus, for any permanent records, the requirements of the National Archive must be met (36 CFR 1234.30). The following requirements state the currently acceptable media and file formats accepted by NARA. It is expected that NARA will be evaluating and adding new media types and file formats over the next one to five years - - at which time these requirements will be updated.

- ❏ Media types currently accepted by NARA include: CD-ROM, 6250 bpi tape and 3480 tape.
- ❏ File formats currently accepted by NARA are: ASCII text, and SGML.

5.13 RECORDS HOLD

Records should be held (not deleted) when government investigation, audit or litigation is imminent or would be foreseen by an average person.

- ❏ Identify which records are subject to the hold.

- ❏ Mark the metadata for the records as requiring a hold; identify the specific hold(s) that affect the record; and automate the release of the record, once the hold order is lifted. (One record may be subject to multiple hold orders.)

- ❏ Only the PTO Records Officer can authorize selected personnel to create, change, or release a case file hold order.

APPENDIX A – METADATA GUIDELINES

METADATA GUIDELINES

For

REFORMAT, COPY AND TRANSFER PROFILES

REFORMAT METADATA PROFILE

This metadata profile is divided into input metadata and output metadata elements. The purpose of these metadata elements is to capture detailed information about status of a case file before and after reformatting in order to establish the foundation for its trustworthiness over time. At the time of the first reformatting, many of the input data elements most likely would be extracted from the Case File or Case File Records Metadata Profiles. Subsequent reformattings would link backward to the most recent processing, which could be reformatting, copying, or transferring, and extract the relevant metadata elements.

REFORMAT METADATA PROFILE (INPUT)

Date of Reformatting

Reformat Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

TIFF

XML

SVG

JPEG

CNG

MPEG

Other

Case File or Record Byte Count

Record Authentication (If Used)

CRC

Hash Digest

Storage Media

Vendor

Type (e.g., RAID, 3480 or DLT Tape)

Product Name

Volume ID

Software Used in Reformatting

Name Of Product

Version Number

REFORMAT METADATA PROFILE (OUTPUT)

Date of Reformatting

Reformat Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

TIFF

XML

SVG

JPEG

CNG

MPEG

Other

Case File or Record Byte Count

Record Authentication (If Used)

CRC

Hash Digest

Storage Media

Vendor

Type (e.g., RAID, 3480 or DLT Tape)

Product Name

Volume ID

Comparison

Byte Count

CRC

Hash Digest

Visual Inspection

Discrepancies (If Any)

Corrections (If Any and Explanations)

Supervisor Review

Physical Storage Location

Primary

Backup

COPY METADATA PROFILE

The purpose of the metadata elements in the copy format template is to capture detailed information about status of a case file before and after copying in order to establish the foundation for its trustworthiness over time. Consequently, the Copy Metadata Requirements are divided into two categories -Input and Output. Copying patent and trademark case files can occur at the time after closure, after initial reformatting, or in conjunction with transfer (discussed later). At the time of the first copying many of the input data elements most likely would be extracted from the Creation-Use or Reformat Template. Subsequent copying would link backward to the most recent processing, which could be reformatting, copying, or transferring, and extract the relevant metadata elements.

COPY METADATA PROFILE (INPUT)

Date of Copying

Copy Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

- **TIFF**
- **XML**
- **SVG**
- **JPEG**
- **CNG**
- **MPEG**
- **Other**

Case File or Record Byte Count

Record Authentication (If Used)

- **CRC**
- **Hash Digest**

Storage Media

- **Vendor**
- **Type (e.g., RAID, 3480 or DLT Tape)**
- **Product Name**
- **Volume ID**

Software Used in Reformatting

- **Name Of Product**
- **Version Number**

COPY METADATA PROFILE (OUTPUT)

Date of Copying

Copy Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

- **TIFF**
- **XML**
- **SVG**
- **JPEG**
- **CNG**
- **MPEG**
- **Other**

Case File or Record Byte Count

Record Authentication (If Used)

- **CRC**
- **Hash Digest**

Storage Media

- **Vendor**
- **Type (e.g., RAID, 3480 or DLT Tape)**
- **Product Name**

Volume ID

Comparison

Byte Count

CRC

Hash Digest

Visual Inspection

Discrepancies (If Any)

Corrections (If Any and Explanations)

Supervisor Review

Physical Storage Location

Primary

Backup

TRANSFER METADATA REQUIREMENTS

Like the Reformat and Copy Metadata Requirements, the purpose of the Transfer Metadata Profile is to capture information that documents fully the actions taken in this activity that will help support the trustworthiness of electronic patent and trademark case files despite changes in technology. The metadata elements in this profile capture detailed information about status of a case file before and after transfer. It is likely that at the time of the first transfer many of the input data elements most likely would be extracted from either the Reformat or Copy Templates. Subsequent transfers would link backward to the most recent processing, which could be reformatting, copying, or transferring, and extract the relevant metadata elements.

TRANSFER METADATA PROFILE (INPUT)

Date of Transfer

Transfer Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

- **TIFF**
- **XML**
- **SVG**
- **JPEG**
- **CNG**
- **MPEG**
- **Other**

Case File or Record Byte Count

Record Authentication (If Used)

- **CRC**
- **Hash Digest**

Storage Media

Vendor

Type (e.g., RAID, 3480 or DLT Tape)

Product Name

Volume ID

Software Used in Transferring

Name Of Product

Version Number

TRANSFER METADATA PROFILE (OUTPUT)

Date of Transfer

Transfer Iteration Number

Case File Identifier

Case File Record Identifier (If Appropriate)

File Formats Used

TIFF

XML

SVG

JPEG

CNG

MPEG

Other

Case File or Record Byte Count

Record Authentication (If Used)

CRC

Hash Digest

Storage Media

Vendor

Type (e.g., RAID, 3480 or DLT Tape)

Product Name

Volume ID

Comparison

Byte Count

CRC

Hash Digest

Visual Inspection

Discrepancies (If Any)

Corrections (If Any and Explanations)

Supervisor Review

Physical Storage Location

Primary

Backup