

THE SEDONA
GUIDELINES:
*Best Practice Guidelines
& Commentary for
Managing Information
& Records in the
Electronic Age*

A Project of The Sedona ConferenceSM
Working Group on
Best Practices for Electronic Document
Retention & Production

September 2004 Public Comment Draft



THE SEDONA GUIDELINES:
*Best Practice Guidelines & Commentary for
Managing Information & Records in the
Electronic Age*

Editors in Chief:

Charles R. Ragan
Jonathan M. Redgrave
Lori Ann Wagner

Senior Editors:

Christine M. Burns
David Kittrell
Judy Van Dusen

Editors:

Jacqueline M. Algon
Thomas Y. Allman
M. James Daley
James L. Michalowicz
Timothy L. Moorehead
Kate Oberlies O'Leary
Robert F. Williams
Edward C. Wolfe

Copyright © 2004 The Sedona ConferenceSM
All Rights Reserved.

REPRINT REQUESTS

Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference,
at tsc@sedona.net or 1-866-860-6600.

wgsSM

Copyright © 2004,
The Sedona ConferenceSM

Visit www.thesedonaconference.org

Foreword

Welcome to the second major publication in The Sedona ConferenceSM Working Group Series (the “WGS”). The WGSSM is designed to bring together some of the nation’s finest lawyers, consultants, academics and jurists to address current problems in the areas of antitrust law, complex litigation and intellectual property rights that are either ripe for solution or in need of a “boost” to advance law and policy. (See Appendix G for further information about The Sedona ConferenceSM in general, and the WGSSM in particular). WGSSM output is published and widely distributed for review, critique and comment. Following this period of peer review, we will review and republish the original piece, taking into consideration what has been learned during the comment period. The Sedona ConferenceSM hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law and policy, both as they are and as they ought to be.

This is the public comment version of *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, a companion piece to *The Sedona Principles on Electronic Document Production*. The subject of information management and record retention is of critical importance in the digital age and subject of many treatises and publications, yet the members and participants of the Working Group believed that there was a need to distill existing thoughts and, in doing so, reach across the boundaries of legal compliance, records management and information technology. The Steering Committee and Participants of the Working Group on Electronic Document Retention and Production are to be congratulated for their efforts in developing these Guidelines and their continued dedication to the project since the first meeting of this Working Group in October of 2002. I especially want to acknowledge the contributions of Jonathan M. Redgrave in organizing and leading the Working Group, and Chief Editors Chuck Ragan and Lori Wagner for leading this particular aspect of the Working Group’s effort.

Finally, the peer review period is an important part of the balanced development of these guidelines and commentary. This document is being published for a six-month public comment period, after which the editorial board will review the thoughts and comments received; we plan to issue a final edition of this work product in the late spring of 2005. We welcome all comments and ask that you please submit them in writing to Jonathan Redgrave (jredgrave@jonesday.com) and Richard Braman (tsc@sedona.net) on or before March 1, 2005. Thank you in advance for any thoughts you may take the time to forward to us.

Richard G. Braman
Executive Director
The Sedona ConferenceSM
September 2004

The Sedona Guidelines for Managing Information and Records In The Electronic Age

1. An organization should have reasonable policies and procedures for managing its information and records.

- a. The hallmark of an organization's information and records management policies should be reasonableness.*
- b. Defensible policies need not be universal, nor do they need to address the retention of all information and documents.*
- c. No single standard or model can fully meet an organization's unique needs.*

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

- a. Information and records management is important in the electronic age.*
- b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.*
- c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.*
- d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.*
- e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.*

3. An organization need not retain all electronic information ever generated or received.

- a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.*
- b. Systematic deletion of electronic information is not synonymous with evidence spoliation.*
- c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.*
- d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.*
- e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.*
- f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.*

4. An organization adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

- a. *Information and records management policies must be put into practice.*
- b. *An organization should define roles and responsibilities for program direction and administration within its information and records management policies.*
- c. *An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.*
- d. *An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.*
- e. *An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.*
- f. *An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.*
- g. *An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.*
- h. *Policies and procedures regarding electronic management and retention may be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.*
- i. *Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.*

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, governmental investigation or audit.

- a. *An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.*
- b. *An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.*
- c. *An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.*
- d. *An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.*
- e. *Legal holds and procedures should be appropriately tailored to the circumstances.*
- f. *Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.*
- g. *Documenting the steps taken to implement a legal hold may be beneficial.*
- h. *If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.*
- i. *Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (i.e., there is no continuing duty to preserve the information), organizations are free to lift the legal hold.*

Preface

Today most information created and received in organizations of all sizes is generated electronically in the form of e-mail messages and their attachments, word processing or spreadsheet documents, webpages, databases and the like.¹ Even formal documents—such as tax returns, applications for environmental permits and other documents filed with regulatory authorities—generally originate, and may even be filed, in electronic format. Much of the information is never reduced to paper. Meanwhile, because of how computers operate, vast amounts of electronic data are created and maintained—seemingly forever—often without users even knowing that the data has been created, much less saved. Yet while this data is kept “seemingly forever,” due to changes in technology it may rapidly become inaccessible unless migrated to new formats.²

This document explores how the prevalence of electronic information affects traditional concepts of records management and applicable legal requirements. It suggests basic guidelines, commentary and illustrations to help organizations develop sound and defensible processes to manage electronic information and records.

The guidelines do not specify precise technical means to implement these approaches. Appropriate technical solutions can be devised only after the essential elements of a program are designed, and after reviewing the organization’s operations, risk and regulatory environment and information technology (IT) structure. In all likelihood after such analysis, the application of the guidelines and the particular solutions employed will vary greatly among and even within organizations.

We examine electronic information and records management from three different perspectives—legal, records management and information technology—with legal considerations being our primary focus. In doing so, we recognize that obligations of the litigation process—such as the duty to preserve information that is, or may become, discoverable—differ from the operational, as well as any statutory, regulatory and other legal obligations, which form the basis for records management. In large organizations, these three views are often represented by various (and perhaps well-funded) constituencies; in smaller ones, only one individual may perform two or even all three roles and the resources available may be limited. Regardless of an organization’s size, an effective approach to electronic information and records management should consider all three perspectives and requires appropriate compromises in reaching the best possible solution for an organization.

One may view this document as a type of digital age Rosetta Stone,³ helping translate and harmonize legal, records management and technical jargon and concepts for managing electronic information and records. But, like that ancient stone tablet, this document is not a radical or breakthrough paradigm for managing information and records. The Working Group readily acknowledges that others have promulgated various standards, practices and treatises on retention issues—including those for electronic records—and we do *not* seek to re-create wheels already invented. That said, the guidelines address these issues from a unique multidisciplinary perspective that we believe will help the various constituencies within an organization better understand their obligations and each other, and help persons outside the

organization understand the complex and unique issues involved in managing electronic information and records.

Board of Editors⁴

¹ See Lyman, Peter and Hal R. Varian, "How Much Information" 2003, *accessed at* <http://www.sims.berkeley.edu/research/projects/how-much-info/summary.html>

² On August 3, 2004 the National Archives and Records Administration (NARA) announced the award of design contracts for the agency's new Electronic Records Archive (ERA). http://www.archives.gov/media_desk/press_releases/nr04-74.html. Two selected contractors are vying to create a system that will "capture electronic information, regardless of its format, save it permanently, and make it accessible on whatever hardware or software is currently in use." *Id.* In particular the system is intended to address the quick obsolescence of electronic data: Unfortunately, this concept will not become reality any sooner than 2011, and, even if it proves successful, it only answers the question of "how" to store electronic records and not "what" to retain.

³ The Rosetta Stone is a basalt slab discovered by Napoleon's soldiers in 1799 in Rosette (Raschid), Egypt. Carved in 196 B.C., it contains a decree of the priests of Memphis honoring the Egyptian Pharaoh Ptolemy V, appearing in: hieroglyphs (the script of official and religious texts), Demotic (the script of everyday Egyptian language), and Greek. Because the Rosetta Stone contained the same text in three different scripts, for the first time in 1822 Jean Francois Champollion was able to use it to unlock the mystery of hieroglyphics. Then with the aid of his understanding of the Coptic language (the language of the Christian descendants of the ancient Egyptians), Champollion also discovered the phonetic value of the hieroglyphs, proving they had more than symbolic meaning, but also served as a "spoken language."

⁴ This effort represents the collective view of The Sedona Conference Working Group on Best Practices for Electronic Document Retention and Production and does not necessarily reflect or represent the views of The Sedona ConferenceSM, any one participant, member or observer, or law firm/company employing a member or participant, or any of their clients. A list of all participants, members and observers of the Working Group is set forth in Appendix F. A description of The Sedona ConferenceSM, and its working group series is set forth in Appendix G.

Table of Contents

Foreword..... ii

The Sedona Guidelines iii

Preface v

Table of Contents vii

Introduction. 1

1. What Is a “Guideline”?..... 1

2. The Traditional View of Managing of Information and Records..... 2

3. Understanding “Information” and “Records” 3

4. Existing Resources to Analyze and Guide the Management of Electronic Information and Records..... 4

5. Potential Benefits From Effective Information and Records Management 5

6. Potential Consequences of Inadequately Managing Information and Records in the Electronic Age 6

7. Enormous Challenges and Reasonable Expectations: the Road Ahead 6

The Sedona Guidelines for Managing Information and Records In The Electronic Age..... 11

Guidelines & Comments 13

1. An organization should have reasonable policies and procedures for managing its information and records..... 13

Comment 1.a. The hallmark of an organization’s information and records management policies should be reasonableness. 13

Comment 1.b. Defensible policies need not be universal, nor do they need to address the retention of all information and documents. 14

Comment 1.c. No single standard or model can fully meet an organization’s unique needs. 14

2. An organization’s information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization. 16

Comment 2.a. Information and records management is important in the electronic age..... 16

Comment 2.b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization’s business needs, operations, IT infrastructure and regulatory and legal responsibilities. 16

Comment 2.c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy. 18

Comment 2.d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program..... 20

Comment 2.e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program..... 21

3. An organization need not retain all electronic information ever generated or received. 24

Comment 3.a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it. 24

Comment 3.b. Systematic deletion of electronic information is not synonymous with evidence spoliation. 26

Comment 3.c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail. 27

Comment 3.d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes. 28

Comment 3.e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data. 28

Comment 3.f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata. 29

4. An organization adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.....30

Comment 4.a. Information and records management policies must be put into practice.....30

Comment 4.b. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.....30

Comment 4.c. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.....32

Comment 4.d. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.....33

Comment 4.e. An organization should consider the impact (including potential benefits) of technology on the creation, retention and destruction of information and records.....34

Comment 4.f. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.....36

Comment 4.g. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.....36

Comment 4.h. Policies and procedures regarding electronic management and retention may be coordinated and/or integrated with the organization’s policies regarding the use of property and information, including applicable privacy rights or obligations.....37

Comment 4.i. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.....38

5. An organization’s policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, governmental investigation or audit.....40

Comment 5.a. An organization must recognize that suspending the normal destruction of electronic information and records may be necessary in certain circumstances.....40

Comment 5.b. An organization’s information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.....40

Comment 5.c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.41

Comment 5.d. An organization’s information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.....41

Comment 5.e. Legal holds and procedures should be appropriately tailored to the circumstances.42

Comment 5.f. Effectively communicating notice of a legal hold should be an essential component of an organization’s information and records management program.....44

Comment 5.g. Documenting the steps taken to implement a legal hold may be beneficial.....46

Comment 5.h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.....46

Comment 5.i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.....47

Appendix A: Standards 48

Appendix B: Cohasset Survey Results56

Appendix C: Survey of Data Within an Organization58

Appendix D: Technical Appendix.....68

1. Metadata:68

2. Electronic (Digital) Archives:71

Appendix E: Glossary78

Appendix F: Working Group Participants, Members and Observers85

Appendix G: Background on The Sedona ConferenceSM & its Working Group Series.....96

Introduction

Management of Information and Records in a World of Electronic Documents and Data

One dictionary aptly defines “revolution” as “[a] sudden or momentous change in a situation.” Clearly, the way society communicates and stores information has undergone momentous change over the past twenty years because of the “computer revolution.” And certainly, when viewed in terms of the whole of human history (or even *modern* human history), this change in the way we communicate has been quite sudden.

But consider the parallel development of organizational policies and procedures to manage this new world of electronic information. This development has been a complex and iterative process, both slow and painstaking. A process more akin to “evolution,” which the same dictionary defines as “[a] gradual process in which something changes into a different and usually more complex or better form.” Further supporting this evolutionary paradigm relating to electronic information management, the pertinent trade literature is filled with various proposed procedural and technical adaptations, permutations and solutions¹ to help organizations survive in this new and challenging world of electronic documents and data. But organizations face increasing pressure to “do something” to manage all their information. With technology continuing to advance at a dizzying pace, survey research² and anecdotal evidence indicate that many organizations are struggling to meet the new and unique demands of managing electronic information and records.

There are many ways in which electronic information and records are qualitatively and quantitatively different from paper documents.³ This publication includes guidelines to help organizations address their unique needs and responsibilities in managing electronic information and records in this new and changing environment. Some of the guidelines address the statutory, regulatory and other legal obligations needed to manage and retain valuable information as an ongoing business matter. *See* Guidelines 1-4. Other guidelines deal with specialized responsibilities relating to actual or reasonably anticipated litigation where all types of relevant information must be preserved, regardless of whether that information is identified as “records.” *See* Guideline 5. These distinctions have important resource and operational management consequences but, unfortunately, have become somewhat confused in the discussions we have observed by both courts and commentators.

Before exploring the guidelines and commentary, it is critical to understand what guidelines are—and are not. It is also important to understand certain aspects of traditional records management concepts, as well as the potential benefits and risks attendant to applying records and information management concepts in the electronic age. This background sets the stage for understanding the modern challenges that these guidelines address.

1. What Is a “Guideline”?

The purpose and scope of this document is an important preliminary question. That is, what are these “guidelines” and what weight should they carry? The management of information and records in the digital age is both dynamic and unsettled as noted elsewhere in this document.

These guidelines analyze the philosophies and doctrines advocated by various treatises, white papers and studies as tempered by the real world experiences of those persons in The Sedona Working Group. They are aspirational, in that they suggest or recommend specific actions or behavior for

general consideration. They differ from “standards,” which are usually seen as mandatory and may be accompanied by an enforcement mechanism.

Thus, these guidelines are not mandatory or exhaustive and may not apply in all situations. The objective is to help all persons involved in this area, and particularly the three disciplines already highlighted—lawyers, records managers and information technology professionals—to move towards more defined and better practices in this area. In addition, these guidelines are premised on an understanding that developing and implementing an organization’s best practices should be an evolving process and not simply a momentary project.

2. The Traditional View of Managing of Information and Records

From a traditional records management perspective,⁴ information should be retained as long as it has value to an organization, or is required by law or regulation to be retained. The records management profession defines the various values of information to organizations as “legal values,” “fiscal values,” “operational values,” and/or “historical values.” *See* ARMA Glossary of Records and Information Management Terms (ANSI/ARMA 10-1999). Another way of stating this, which also introduces the related concept of the need to preserve all types of relevant information in the litigation or government investigation context, is that organizations should address the need to identify and retain various types of information when:

- A local, state or federal law or regulation mandates continued availability and accessibility;
- Internal organizational requirements, including policies and contracts or other record keeping requirements, mandate retention, such as records for tax purposes;
- The information is worthy of retention because it has other value to the organization; or
- It must be preserved because it is relevant to actual or reasonably foreseeable litigation, subpoenas or government investigative requests, regardless of whether it meets any of the preceding criteria or constitutes a formal “record” of the organization.

The records management discipline also generally recognizes that information may be destroyed⁵ when it no longer meets any of the above criteria. Traditionally, disposal was done to reduce the costs of storing information that was not legally required to be retained and that had no current or long-term value to the organization. While the cost of storing electronic information is different today from that of warehouses for paper documents, storing and maintaining ever-increasing amounts of essentially valueless electronic information still costs money in the short term, can degrade software performance and may substantially impede access to valuable information. Thus, even as the direct costs of storing electronic information continue to fall, the ancillary costs of retaining and sorting through otherwise valueless information are often disproportionate to the value of its serendipitous use. Stated otherwise, just because electronic records storage systems greatly facilitate the storage of more information, does not mean that organizations should be less diligent about developing and applying meaningful information and records retention policies.

Traditional records management concepts of information value apply equally to electronic information, and, indeed, the ability to manipulate electronic information makes it potentially more valuable than its paper analogues. Yet, while the concept of value is ever-changing for paper documents, the unique characteristics of electronic information and records significantly exacerbate the difficulties in defining and applying valuation standards. For example, on a given day, data encryption codes and routing information may be indispensable to the operation of the organization,

yet the data may be useless (and worthless) the next day. On the other hand, certain financial and operational data may be critical over the entire life-span of the organization; the loss of the data at any point could be crippling to the operation of the organization. There is a wide world between these extremes.

Throughout this document we use the term “information and records management” to refer to the process by which an organization generates (or receives), retains, retrieves and destroys tangible (paper or electronic) information. This “management” may be through highly detailed policies, procedures and records retention schedules, or it may be without such detail. But whatever the terms or methods employed, there are certain benefits and risks attached to these active and passive decisions, which each organization should consider and balance in its best judgment in relation to its own circumstances.

3. Understanding “Information” and “Records”

“Information” is a basic but intangible resource that organizations harness to meet their operational, legal, historical and institutional needs. Every day selected pieces of this “information” are captured as “documents” or “data,” giving this intangible resource tangible form and enhancing the ability to access and share it. Although “information” can refer to everything from telephone message slips to the CEO’s thoughts on next quarter’s forecast, throughout this document the word “information” will be used to refer generally to *all* of an organization’s tangible documents and data—in both electronic and other formats.

“Records” are a special subset of “information” deemed to have business value to an organization and warranting special attention concerning retention, accessibility and retrieval. This declaration of value can be by operation of law or by specific classification by the organization. Designating certain documents or information as “records” can also help an organization compile and preserve its “institutional memory.” A “record” can memorialize business actions or events in a defined and distinct location and form. And, if records are organized, they can be reviewed, analyzed or used to document actions or events.

Some information has value or significance only for short periods. For example, certain event announcements (*e.g.*, that lunch is served) or statements concerning the availability or unavailability of services (*e.g.*, that servers will be down for maintenance briefly) has no long-term value to the organization and normally can and should be discarded. This is just as true in the digital world as it was in the previous paper-driven world, when inconsequential papers were routinely removed from the premises at the end of a shift or a business day.

This subset of information in an organization is generally not classified as a “record,” but it does have value to the organization for some unspecified and perhaps uncertain period of time. In the electronic world, many organizations find it is difficult, if not impossible, to classify large amounts of this type of electronic information for retention under any traditional records management scheme, both because of its nature and its volume. Indeed, this “non-record” information might be most of the electronic information owned by the organization.

However, many organizations do classify at least some of their valuable information (whether paper or electronic) as “records.” For those which do so, a useful illustration of the necessary culling process can be seen in the Federal Government. Consider the following definition of a record under the United States Code:

“[R]ecords” includes 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 data in them.

44 U.S.C. § 3301. This definition highlights that any culling process should:

- (a) Look at content regardless of form (electronic or paper).
- (b) Focus on the operational activities of the organization.
- (c) Involve a policy level decision by the organization as to what has sufficient value to be designated as a “record.”
- (d) Recognize that while the decision-making process has many variables, it should focus on providing access to information that has some continuing value.

4. Existing Resources to Analyze and Guide the Management of Electronic Information and Records

At least three sources provide guidance in assessing appropriate management of information and records: (1) statutory, regulatory and other legal principles (“the law”), (2) professional standards published by specialized industry groups and (3) commonly accepted industry practices prevalent in specific industries. Legal guidance is embodied in a wide variety of statutes and regulations establishing record-keeping requirements for organizations based on their locations, business operations and activities, which typically draw no distinction between electronic and paper records.⁶ In addition, the common law creates obligations to preserve *evidence* (whether designated as records or not) when actual or reasonably anticipated litigation is involved.

Many trade and service organizations recommend that their members follow published standards and technical papers addressing records and information management issues.⁷ Furthermore, within certain industries, trade practices regarding data capture and retention may become standards for all industry members.

Organizations issuing guidance in this area include ANSI (American National Standards Institute), AIIM International (Association for Information and Image Management), ARMA International (Association of Records Managers and Administrators) and ISO (International Organization for Standardization). These organizations take different and sometimes overlapping approaches to the issue, but all agree that standards are essential to manage electronic records. However, these organizations generally do not address specific litigation-oriented evidence preservation duties, a critical consideration in the United States that we address here. *See* Guideline 5 and accompanying text.

Recently, ISO sought an international consensus standard for records management, including electronic records, in its useful guidance document ISO Technical Report 15489-2 (*Information and Documentation—Records Management* (2001)) and its accompanying standard, ISO 15489-1.⁸ The standard establishes requirements to consider legal, statutory and regulatory requirements in setting records retention and disposition policies and procedures. *See* ISO 15489-1, Clause 5. The standard recognizes that there are various methods to analyze operational functions to determine records

management requirements, and the Technical Report is an explicit (but not exclusive) example. Nevertheless, despite its breadth, there is no established mechanism to certify compliance with ISO 15489-1. Various other current standards and guidelines known to the authors of these Guidelines are set out in Appendix A.⁹

Apart from the standards and guidelines offered by standards and trade organizations, many consultants, vendors and software companies offer (for a price) solutions to the complex questions involved in managing information and records in the electronic age. Most of these purported solutions are oriented to specific regulatory needs (such as in the financial services or health fields) and are so new that neutral evaluation is unavailable. Furthermore, many of the white papers and technical reports that do exist often seek to advocate the narrow approach to information management offered by the vendor/author.

Thus, despite the seeming abundance of resources,¹⁰ we believe there is no uniformly recognized single standard regarding policies or procedures to manage electronic information and records. In the absence of uniformity, organizations must focus on their own particular operational and business needs for retaining information and records.

5. Potential Benefits From Effective Information and Records Management

The most appropriate information and records management approach an organization may follow (as well as the resources available to develop and implement that approach) will depend significantly upon the organization's mission, resources, needs and legal responsibilities. There is no single standard or universal policy that can be applied as a talisman to guide all future conduct or judge the wisdom of prior practices. Instead, there is a continuum of possible models, all or many of which may allow an organization to meet its unique business and legal needs. And there are infinite combinations of these approaches that may fall within the boundaries of reasonable, defensible and good management practices. As such, these guidelines do not suggest how an organization should manage its information and records. Rather, they highlight issues to consider in deciding whether and how to approach the issue.

In making that judgment, and in deciding what resources to commit, an organization may wish to consider the following possible benefits of an effective information and records management program:

- Facilitating easier and more timely access to necessary information;
- Controlling the creation and growth of information;
- Reducing operating and storage costs;
- Improving efficiency and productivity;
- Incorporating information and records management technologies as they evolve;
- Meeting statutory and regulatory information and records retention obligations;
- Meeting litigation retention obligations, which may be broader and more extensive than those of its records management obligations;
- Protecting the integrity and availability of business critical information;
- Leveraging information capital and making better decisions; and
- Preserving corporate history and memory.

These potential benefits are hard to quantify, making a traditional cost/benefit analysis difficult. However, in assessing its institutional goals and legal responsibilities, an organization should decide if a refined information and records management approach to electronic documents information and records will help meet these goals and responsibilities at a cost that makes sense.

6. Potential Consequences of Inadequately Managing Information and Records in the Electronic Age

An organization may also wish to consider the possible risks of not actively managing electronic information and records, such as:

- Inability to retrieve and productively use business critical information on a daily or historic basis;
- Loss of strategic opportunities due to the inability to recognize or leverage valuable information;
- Increased costs of doing business from inefficiencies related to disparate or inaccessible data;
- Failure to comply with statutory or regulatory retention requirements;
- Reduced ability to comply with court orders and other litigation-related imperatives requiring access to existing information; and
- Inability to respond promptly to governmental inquiries.

The consequences of a failure will vary depending upon the circumstances, but could range from minor to catastrophic:

- Lost business;
- Lost profits;
- Regulatory fines and penalties, which have recently reached eight figure amounts;¹¹
- Civil litigation consequences, such as increased litigation costs, fines,¹² adverse inference instructions,¹³ default judgment,¹⁴ and civil contempt;¹⁵
- Vicarious liability for responsible senior management;¹⁶ and
- Criminal liability for organizations¹⁷ and individuals.¹⁸

The key management challenge is to weigh the benefits (both in terms of goals achieved and risks diminished) against the potential costs of the various approaches to managing electronic documents and records. This is often described as a “cost-benefit” or ROI (*i.e.*, return on investment) analysis. The increased scrutiny in the regulatory and litigation arenas, combined with the significant complexities of managing electronic, can significantly affect ROI calculations, weighing in favor of more sophisticated management approaches.

7. Enormous Challenges and Reasonable Expectations: the Road Ahead

We submit the following conclusions that can be reasonably drawn from the foregoing:

- Organizations should thoughtfully consider electronic information and records management.

- Solutions for managing electronic information and records must be flexible, reasonable and scalable (*i.e.*, able to adjust from small to large organizations) to the enterprise and its circumstances. Importantly, what is seen as reasonable must be proportionate to the organization and its purpose.
- Pragmatism must guide the scope, content, costs and anticipated results of any policy or technology solution. Even though we can create and store far more than we ever imagined possible in the past, the ability to quickly create, infinitely store and potentially retrieve does not justify legal rules or arguments requiring parties to save forever, retrieve and produce all that is technically possible.
- Regulatory and judicial bodies must recognize that this area is enormously complex, that the boundaries of legitimate policies adopted in good faith must be sufficiently elastic, and that an organization that makes good faith efforts in this area should not be penalized for partial performance or an imperfect implementation. The failure to store or retrieve everything (or even smaller subsets) for all time should not be perceived as hiding or destroying evidence. Indeed, the Federal Rules of Civil Procedure are predicated on substantial limits on discovery that are in place to secure the “just, speedy and inexpensive determination of every action.”¹⁹

We respectfully offer the following guidelines, commentary and illustrations to assist organizations in creating reasonable, effective and defensible policies for managing electronic information and records.

¹ On June 1, 2004, the Association of Records Managers and Administrators, Inc. (ARMA) made available for public comment two documents: *Requirements for Managing Electronic Messages as Records* and *Managing Recorded Information Assets and Resources: Retention and Disposition Programs*. See Randolph A. Kahn and Barclay T. Blair, *Information Nation: Seven Keys to Information Management Compliance* (AIIM International 2004); Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Data*, 24 J. CORP. L. 417 (1999); Timothy Q. Delaney, *Email Discovery: The Duties, Danger and Expense*, 46 FED. LAW. 42 (Jan. 1999); Charles A. Lovell & Roger W. Holmes, *The Dangers of Email: The Need For Electronic Data Retention Policies*, 44 R.I.B.J. 7 (Dec. 1995).

² See, e.g., Appendix B (Summary of Cohasset Associates 2003 Survey Results); see also AMA/ePolicy Institute Research *2004 Workplace E-Mail and Instant Messaging Survey Summary*, available at: <http://www.epolicyinstitute.com/survey/survey04.pdf>.

³ These differences were discussed at length in the Sedona Conference’s sister publication *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (Jan. 2004).

⁴ The traditional concept of “managing” information and records arose from practices related to paper records and, in large part, the management of inactive paper records (*i.e.*, records that were no longer actively used in the business but retained some value or fell within a legal requirement to retain the records). Records management as a discipline evolved to include paper document generation and management, and is now faced with the challenge of adjusting to the new paradigm of electronic information and records. As noted elsewhere, this challenge is exacerbated by the fact that hardware and software systems were not—and even today largely are not—designed with consideration of records retention policies and requirements.

⁵ As set forth herein, there is legitimate debate regarding whether to describe the end (last) stage of a record’s “life” as “disposal” or “destruction.” There is great merit to the proposition that the broader term “disposal” is better for it encompasses many possible actions and it is not seen as pejorative as “destruction.” This document does *not*, however, take a position on such nomenclature because the important point that must be understood is that organizations can, do and should take steps to eliminate information that need not be retained, whether that is called “destruction,” “deletion,” “disposal,” “shredding,” or the like.

⁶ Most statutes and regulations encompass both electronic and traditional paper records in their definitions of “document” or “record.” In recent years, federal, state and local regulations have given organizations considerable

latitude in maintaining their records in either paper or electronic form. *See, e.g.*, Paperwork Reduction Act (44 U.S.C. § 3501 *et seq.*).

⁷ For example, AIIM International has issued 80 standards, recommended practices and technical reports, many of which have been approved by the American National Standards Institute (ANSI). ANSI has promulgated additional national standards including, for example, storage of magnetic and optical media for records management purposes—ANSI Standard IT9.23-1998. Similarly, ARMA International and ISO (International Organization for Standardization) are accredited international standards development organizations that issue standards and reports regarding records and information management.

⁸ ISO/TR 15489-2 seeks to provide a “benchmark” for “best practice” in record systems and practices, regardless of medium or format. This standard is available for purchase from the ISO online, at www.iso.ch/iso/en/prods-services/ISOstore/store.html or from the ARMA bookstore at: www.arma.org/Bookstore/default.cfm. Australia has incorporated ISO/TR 15489-2 in its national standard for management of all records (Australian Standard AS 4390). Other countries are considering adoption of the ISO standard as well, as reported in ISO’s 2003 international conference report available at: <http://www.iso.org/iso/en/commcentre/events/2003/armaiso15489.html>. For an excellent summary of this ISO standard *see* Sheila Taylor, *Benchmarking for Records Management Excellence*, MUNICIPAL WORLD (Jan. 2003), at: <http://www.condar.ca/CONDAR%20Articles/article%2015%20RM%20Benchmarking.pdf>.

⁹ Most of the identified standards focus on technical issues relating to the use of alternative media for storing records and not on records retention issues.

¹⁰ Even with respect to the general resources that are available, they do not cover the vast majority of information and records generated and retained by most organizations.

¹¹ *E.g.*, Bank of America was fined \$10 million in March 2004 for allegedly misleading regulators and stalling in producing evidence in an investigation of improper trading at its securities brokerage.

¹² *E.g.*, *United States v. Philip Morris USA*, ___ F. Supp. 2d ___, 2004 WL 1627252, at *3 (D.D.C. July 21, 2004) (\$2.75 million sanction for failure of 11 employees to follow litigation hold requirements for e-mails); *SEC v. Lucent Technologies Inc.*, SEC Accounting & Auditing Enforcement Release No. 2016 (Mar. 17, 2004) (\$25 million); *In the Matter of Bank of America Sec. LLC*, SEC Admin. Proc. File No. 3-11425 (Mar. 10, 2004) (\$10 million); *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 617 (D.N.J. 1997) (\$1 million).

¹³ *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2004 WL 1620866, at *13 (S.D.N.Y. July 20, 2004) (“Zubulake V”); *Linnen v. A.H. Robins Co.*, 10 Mass L. Rptr. 189, No. 97-2307, 1999 WL 462015, at *11 (Mass. Sup. Ct. June 16, 1999).

¹⁴ *Metro. Opera Ass’n v. Local 100, Hotel Employees & Rest. Employees Int’l Union*, 212 F.R.D. 178, 231 (S.D.N.Y. 2003).

¹⁵ *Landmark Legal Foundation v. EPA*, 272 F. Supp. 2d 70, 78, 89 (D.D.C. 2003).

¹⁶ Senior management may be identified by the courts with respect to failings in an organization’s handling of its records. *United States ex. rel. Koch*, 197 F.R.D. 463, 483-86 (N.D. Okla. 1998); *In re: Prudential Ins. Co.*, 169 F.R.D. 598, 615 (D.N.J. 1997).

¹⁷ The following exchange between Congressman Billy Tauzin (R. Louisiana) and Arthur Andersen’s in-house counsel (Nancy Temple) and its Managing Partner for Audit Practice (C.E. Andrews) captures the flavor of this issue in today’s political environment:

Congressman Tauzin: Does it have to be raised, Ms. Temple, when you are the counsel representing this company internally on litigation? Does anybody have to raise it? Or is [it] somebody’s responsibility in the company to say, “Stop destroying documents, we’re under investigation.” Whose responsibility was it, if it was not yours? Did somebody have to raise it? Whose responsibility, Mr. Andrews?

Mr. Andrews: In our policy ...

Congressman Tauzin: Was it your president? Was it you? Who was it?

Mr. Andrews: In our policy, that responsibility, a policy that we’re revising and I acknowledge we’re revising, in that policy that responsibility is with the engagement partner.

Congressman Tauzin: With an accountant, not a lawyer? You give the responsibility to an accountant to decide whether it's legally permissible to destroy documents relative to a proceeding?

Let me just tell you, I don't know what's going to happen out of all this. I really don't. I hope you're all OK, I don't know. But I'll tell you this, every accounting firm that is listening to this had better listen very carefully. If all of your policies are to let an accountant decide when it's legal to destroy documents in a pending investigation, an awful lot of people are going to be in trouble down the road, not just in this case.

And I hope you think seriously about what kind of policies you have on retention of documents and whether those policies are clear or vague or whether you just send memos out for somebody else to interpret or whether you eventually recognize, as you did, Ms. Temple, at some point, that they needed guidance.

They needed guidance on what not to do and what to do as you eventually gave them. And they should have gotten that guidance a long time sooner. You see, we wouldn't be here. We'd be scheduling the Enron hearing right now, but we're here discussing what happened at your company because this guidance never went out when it should have gone out and because your company did not have a clear policy on making sure the documents were not destroyed once a notice was given by the SEC that it was checking into your business.

Now that's got to change. And if you don't change it, I promise you, we will.

Hearings before the House Energy & Commerce Oversight & Investigations Subcommittee on the Destruction of Enron Related Documents (Jan. 24, 2002), *available at* 2002 WL 93115, at *73 (F.D.C.H.).

¹⁸ A significant and relative new set of obligations (and consequences) arises from the Sarbanes-Oxley Act of 2002 (the "Act"). Though much of the Act is limited to the accounting profession, a number of the provisions could theoretically be applied to anyone altering or destroying relevant electronic data. The general provisions of the Act are as follows:

- Section 802 of the Act, at 18 U.S.C. § 1519, makes it illegal for any person to knowingly alter or destroy records with the intent to "impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States" or in any bankruptcy case. Violation of this section is punishable by up to 20 years in prison and is also punishable by fines.
- Section 802 of the Act, at 18 U.S.C. § 1520(a)(2), makes it illegal for any individual to violate any rules promulgated by the Securities and Exchange Commission ("SEC") concerning the retention of "relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review." Of note, the recordkeeping provisions of the act apply to all domestic companies and corporations, regardless of size.
- Section 1102 of the Act amends 18 U.S.C. § 1512 to create criminal penalties against anyone who "corruptly (1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do." Violation of this section carries a penalty of up to 20 years in prison and a fine.
- Section 802 of the Act, at 18 U.S.C. § 1520(c), provides that nothing in 18 U.S.C. § 1520 "shall be deemed to diminish or relieve any person of any other duty or obligation imposed by federal or state law or regulation to maintain, or refrain from destroying, any document."

The SEC has made clear that the governance reforms of the Act make it "necessary for companies to ensure that their internal communications or procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner . . ." Certification of Disclosure in Companies' Quarterly & Annual Reports, 67 Fed. Reg. 57,276, 57,280-81 (Sept. 9, 2002) (to be codified at 17 C.F.R. pts. 228, 229, 232, 240, 249, 270 & 274). *Cf. In re Tyco Int'l Ltd. Sec. Litig.*, No. 00 MD 1335, 2000 U.S. Dist. LEXIS 11659 (D.N.H. July 27, 2000) (no special preservation order is required to put defendants on notice regarding their obligation to preserve relevant electronic data and other materials, since such an order would unnecessarily duplicate or improperly alter defendants' statutory duty to preserve relevant evidence under the Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u-4).

Finally, the Act imposes sanctions on any person who deletes or destroys relevant information required to be preserved. On one hand, this provides additional incentives for individual employees to comply with corporate retention policies and non-destruct notices. On the other hand, the Act also provides a valuable tool for prosecutors seeking to build cases against senior executives by plea-bargaining with low-level employees who may effectuate orders to delete data.

¹⁹ See Fed. R. Civ. P. 1; *see also* Fed. R. Civ. P. 26(b)(2).

The Sedona Guidelines for Managing Information and Records In The Electronic Age

- 1. An organization should have reasonable policies and procedures for managing its information and records.**
 - a. The hallmark of an organization's information and records management policies should be reasonableness.*
 - b. Defensible policies need not be universal, nor do they need to address the retention of all information and documents.*
 - c. No single standard or model can fully meet an organization's unique needs.*

- 2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.**
 - a. Information and records management is important in the electronic age.*
 - b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.*
 - c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.*
 - d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.*
 - e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.*

- 3. An organization need not retain all electronic information ever generated or received.**
 - a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.*
 - b. Systematic deletion of electronic information is not synonymous with evidence spoliation.*
 - c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.*
 - d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.*
 - e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.*
 - f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.*

4. An organization adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

- a. *Information and records management policies must be put into practice.*
- b. *An organization should define roles and responsibilities for program direction and administration within its information and records management policies.*
- c. *An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.*
- d. *An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.*
- e. *An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.*
- f. *An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.*
- g. *An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.*
- h. *Policies and procedures regarding electronic management and retention may be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.*
- i. *Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.*

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, governmental investigation or audit.

- a. *An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.*
- b. *An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.*
- c. *An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.*
- d. *An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.*
- e. *Legal holds and procedures should be appropriately tailored to the circumstances.*
- f. *Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.*
- g. *Documenting the steps taken to implement a legal hold may be beneficial.*
- h. *If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.*
- i. *Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (i.e., there is no continuing duty to preserve the information), organizations are free to lift the legal hold.*

Guidelines & Comments

1. An organization should have reasonable policies and procedures for managing its information and records.

Comment 1.a.

The hallmark of an organization's information and records management policies should be reasonableness.

An organization's approach to retaining information and records should be reasonable under the circumstances. Usually the reasonableness of an approach (including any policy) will not be subject to external scrutiny, such as a court proceeding. When such scrutiny occurs, it is often in the litigation context of explaining why specific information and records no longer exist—*i.e.*, how they were lost or destroyed. As noted in numerous cases, an established and reasonable policy may be very important in establishing the good faith destruction of the information so that no sanctions should be imposed on an organization. Furthermore, absent evidence that an organization has actual knowledge that specific information would be material to foreseeable claims or legal requirements, its best judgment about what information to retain and for how long will generally be respected. However, as is emphasized in Guideline 5, *infra*, an organization must be prepared to accommodate the often broader demands of litigation which may require suspension of plans to delete or destroy information under a retention schedule based on the end of the useful life of that document. The failure to make such accommodation may call into question the reasonableness of a policy in certain circumstances.

With respect to electronic information and records, a critical issue in determining reasonableness will be the information and technology in place at the time. Unlike paper records, many aspects of the distribution and content of electronic information are dictated by the information technology used. Technology has an important effect on any information and records management approach. Judging reasonableness includes considering the substantial efforts required to understand new technologies and to adopt policies governing the management of electronic information and records. Considering what is reasonable (while balancing costs and benefits) also requires recognizing that the implementation of improved electronic and information management programs may take a significant amount of time and resources to implement.

When evaluating records retention policies and practices, courts routinely examine the reasonableness of the policies and practices given the facts and circumstances surrounding the information or record at issue. See *Lewy v. Remington Arms*, 836 F.2d 1104, 1112 (8th Cir. 1988) (noting that retaining appointment books for three years might be reasonable, while retaining customer complaints about product safety for three years might not be reasonable); see also *United States v. Taber Extrusions L.P.*, No. 4:00CV0025, 2001 U.S. Dist. LEXIS 24600, at *8-9 (E.D. Ark. Dec. 27, 2001). In *Taber Extrusions*, the government had destroyed documents related to government contracts under its document retention policy. In analyzing the reasonableness of the destruction of those documents under *Lewy*, the court first found that the policy of destroying the documents after six years and three months appeared reasonable on its face. The court then found there was no evidence that the government should have known that the documents would become material. Compare *Reingold v. Wet 'N Wild Nev., Inc.*, 944 P.2d 800, 802 (Nev. 1997) (company's policy of destroying documents before statute of limitations on potential—and foreseeable—claims expired was not reasonable).

Comment 1.b.**Defensible policies need not be universal, nor do they need to address the retention of all information and documents.**

There is no general requirement that organizations must retain all information created or received in the ordinary course of business, and statutory and regulatory obligations usually specify categories and types of records to be kept. Even in the context of litigation, where preservation obligations extend to evidence (and not just “records”) relevant to the proceedings, courts have routinely recognized that it is unrealistic—and not mandatory—for organizations to keep *everything*. See, e.g., *Zubulake v. UBS Warburg LLC* (“*Zubulake IV*”), 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (“Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, ‘no.’ Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation.”); *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4, *7 (N.D. Ill. Oct. 27, 2003) (Organization “does not have to preserve every single scrap of paper in its business”; “CBRE did not have the duty to preserve every single piece of electronic data in the entire company”); *Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (“to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail. . . . Such a proposition is not justified.”).

Beyond recognizing the fact that no retention matrix, schedule or practice can realistically describe in detail or capture *all* data and information in an organization,¹ there is also a need to understand that policies and practices cannot possibly anticipate all circumstances. In the world of rapidly evolving technology, can organizations be expected to always have a policy provision or practice to address all of the applied technology and communications channels? At the same time, policies and procedures that are static and inflexible run the risk of becoming outdated and unreasonable.

Comment 1.c.**No single standard or model can fully meet an organization’s unique needs.**

For better or worse, the extraordinary flexibility of computer network configurations directly affects the information and records management analysis. There is no single best answer for all organizations, and the course an organization takes will often depend upon its information technology architecture as well as its relative dependence on technology in its business.

The development of a reasonable approach for retaining and managing electronic information and records must rest on a full understanding of how individual business users actually use the information they need in their work. The information or records management approach must take variances between departments, business units and other groups into account—ideally working around the differences and tailoring solutions that best advance the organization’s corporate mission while meeting basic legal responsibilities.

¹ However, organizations are well served by examining and inventorying their various sources and locations of electronic documents and information. An exemplar “survey of data” containing potential inquiries for self-examination is included as Appendix C.

Factors to consider include:

- The nature of the business;
- The legal and regulatory environment surrounding the organization and particular sub-units;
- The culture of the organization;
- The distributed or centralized nature of data within the organization; and
- The business practices and procedures that have evolved independently of any information or record management approach.

There are many ways that an organization can meet its goals and responsibilities in managing information and records. Some could create a centralized function for education and compliance. Others may delegate significant responsibilities to individual employees. Others may look to automated technology solutions for records management that search content and metadata to identify, maintain and dispose of records according to pre-defined retention periods. There is no way to judge one right and one wrong in the abstract—the “best practice” for any one organization could be an impractical and unwise approach for another.

Critically, outsiders who one day may have to evaluate a policy or approach (whether courts, auditors, investigators or others) must recognize the fundamental reality of such variability. Indeed, this variability itself makes it difficult for the organization to benchmark its own practices to gauge success.

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

Comment 2.a.

Information and records management is important in the electronic age.

The fundamental transition to an electronic data environment in most organizations has resulted in an increased need for better information and records management controls and programs. Furthermore, pressures from regulators, investors and the legal sector, placing a greater emphasis on good corporate governance practices, have exacerbated the need for the development of effective policies and procedures.

As a result, identifying and managing information and records should be a business priority for every organization. This may require a significant shift in the organization's mindset. Elevating records management to the level of asset management and including electronic information and records assets in the matrix are first steps in promoting the program and increasing its visibility. Organizations should recognize that effectively implementing an information and records management program may require significant financial and human resources.

In short, managing electronic and other information is not merely a clerical or technical matter. Instead, it is a core component of resource management and enhancement. The organizations that best manage and leverage information assets are likely to thrive in their respective disciplines, and success in this area demands a priority commitment from senior management to develop and support effective processes.

Comment 2.b.

Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.

An information and records management program must reflect the actual use of information within an organization. It should *not* reflect an unrealistic view of how the Legal Department "would like things to be" or how the Information Technology Department would prefer to organize the company's information for system performance or software architecture reasons, notwithstanding practical issues. Although both perspectives are important components of the ultimate design, an information and records management program with idealized or unrealistic standards (*i.e.*, ones not reasonably tailored to the organization's actual needs and usage) probably will not be appropriate for the organization's culture and will not be effective. At the same time, the records management perspective cannot dictate results that are technically or economically infeasible, or legally impermissible or unsound.

Decisions about what electronic information should be retained and how it should be handled involve many cutting edge technological issues and conflicting policy interests. Ideally, an organization's approach to information and records management should be discussed and developed with input from legal counsel, information technology representatives, records management representatives, and representatives from the business functions of the organization to which it will apply. One possibility for larger organizations is an oversight committee composed of representatives from the functions named. In some organizations, this list may be expanded to include internal audit, human resources and other groups. In smaller companies, the responsibilities may be delegated to a very small group or even an individual. In any event, support from senior management is also important.

The information and records management policy should recognize and be consistent with an organization's culture, actual experience and needs, as well as pre-existing structures and policies. Ivory tower drafting of a policy that states what the organization "should" do (but perhaps cannot do or never has previously done) may be worse than no policy at all.

There is no "one size fits all" information and records management policy. In some cases, an organization may focus on amending an existing policy and delegating responsibility to a traditional records organization. In another, individual units may be empowered to develop and apply reasonable practices that focus on the information needed by that unit. *See* Comment 1.c, *supra*. Although examples of successful models, including exemplary written policies, are available from various sources, an organization's approach must be tailored to the specific needs and circumstances. Policy drafters should consider what is reasonably possible, given the organization's structure, culture and resources. The organization should strive to demonstrate reasonable compliance with policies instituted in good faith. And, in all cases, any approach adopted must contemplate the unique needs triggered by litigation. *See* Guideline 5, *infra*.

The factors in formulating an information and records management policy are numerous and complex. Among the variables to be considered, which are discussed in these Guidelines, are:

- The scope and structure of the policy (*e.g.*, whether a uniform approach is adopted worldwide, regionally, etc., and whether it applies to the organization and all wholly owned subsidiaries, etc.);¹
- Roles and responsibilities for creating, implementing and revising the policy. *See* Comments 4.b and 4.d;
- The types and forms of information or records that should be retained to meet operational and legal needs, including a recognition that computers produce information that must be managed in accordance with the policy. *See* Comments 2.c and 2.d;
- How the organization will document its records retention requirements (*e.g.*, through published retention schedules or through means embedded within software applications or in business procedures or some combination thereof);
- The general record-keeping practices required to manage records from point of creation or receipt to final disposition;
- Methods for monitoring and assessing compliance with the policy. *See* Comment 4.q;
- The costs and burdens that may be imposed by various approaches and policies; and
- Procedures for suspending normal destruction, as appropriate, because of actual or reasonably anticipated litigation, an investigation or audit, *i.e.*, instituting a "legal hold" on the information and records. *See* Guideline 5; *see also* Appendix E (Definition of "Legal Hold").

Perfection should never be allowed to become the enemy of good. No policy can be drafted that will be truly omnibus—there is simply too much information in too many places to cover every

¹ It should be noted that the less variation in a policy between departments and locations, the easier (and less expensive) it will be to train and enforce the policy across the organization.

possible variation of facts and circumstances. Good faith efforts to develop and implement a policy should be viewed as reasonable.

Comment 2.c.

An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.

A critical step in drafting an information and records management policy is identifying the applicable legal requirements concerning the retention and destruction of information. An organization must consider the externally mandated laws and regulations that govern it (*e.g.*, IRS, SEC, DOD, Department of Labor/EEOC, EPA, etc.), as well as its duties to preserve data relevant to actual or reasonably anticipated litigation. *See, e.g., Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 281 (E.D. Va. 2004); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

The organization's research likely will result in a matrix of retention obligations similar to those that were typical in traditional hard copy retention policies. Traditionally, the matrix of time periods and classifications was documented in a records retention schedule.² Regardless of nomenclature, the process should be the same for electronic records as for paper records, for the content rather than the format is what matters (*i.e.*, the retention schedule is generally media neutral).³

Beyond the strict legal requirements,⁴ a reasonable policy can serve the legitimate information storage, access and retention needs of the organization.⁵ An information and records management policy should identify and prescribe time periods for the retention of information and records that are appropriate to an organization's needs and legal responsibilities. Such a policy serves a legitimate business purpose and is not designed to eliminate potential "smoking guns." *See Lewy v. Remington Arms*, 836 F.2d 1104, 1112 (8th Cir. 1988) (part three of three-part test to evaluate the reasonableness of defendant's document retention policy is whether policy was instituted in bad faith).⁶ An organization focusing on eliminating "bad" documents not only risks accusations of bad faith (or worse) but also fails to recognize the value of contextual documents to mitigate the so-called "bad" documents and potentially exonerate the organization from allegations of misconduct or wrongdoing. *Cf. United States v. Arthur Andersen, LLP*, ___ F.3d ___, 2004 WL 1344957, at *12

² Many organizations already have such retention schedules for their paper records. Often, however, the schedules have not been updated and are not specifically tailored to address or incorporate electronic records.

³ There are a number of "off the shelf" software packages that, combined with regular updates, can provide a cost effective way to identify retention statutes and regulations, provided there is a way to apply changes to the manner by which the organization manages its information and records.

⁴ Some organizations separately schedule those documents subject to identified legal retention requirements, from those documents that are kept for business needs. Other organizations combine the categories together.

⁵ Reasonableness standards for traditional records management programs were previously established by *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984) and *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988) and still serve as the basis for assessing good faith efforts. At the same time, organizations need to recognize that, as technology changes, information and records management policies may need to be revisited and evolve as necessary to remain reasonable under the circumstances.

⁶ The mere existence of a written policy will not establish that document destruction was justified. Without a sound monitoring and compliance program, a records management policy may be criticized as eliminating only "bad documents." *See Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 485 (S.D. Fla. 1984) (failure to implement the document retention policy in a consistent manner was a significant factor in finding that the destruction of certain evidence relevant to legal proceedings could not be explained or excused as compliance with the policy).

(5th Cir. June 16, 2004) (“There is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation. A company’s sudden instruction to institute or energize a lazy document retention policy when it sees the investigators around the corner, on the other hand, is more easily viewed as improper.”).

Illustration i. Beta Company recently went through a merger in which the FTC required that volumes of documents, including electronic documents, be produced for antitrust review. Beta devoted substantial resources both inside and outside the company to retrieving the documents, reviewing them for relevance and copying them for the FTC. In the process, Beta concluded that many documents it reviewed served no continuing business purpose and were not responsive to the government’s inquiries. It cost an additional \$100,000 to review these documents. Beta has since determined that it needs a records management and retention program (with appropriate legal holds provisions) to maintain and access records for business purposes and to dispose of the records after their useful life is over. Beta’s policy will likely be viewed as legitimate because it can demonstrate that business purposes were advanced by implementing the policy (and, indeed, drove its evolution).

The consequences for ill-conceived document management policies that merely serve as vehicles to “cleanse” files in advance of anticipated litigation or investigation can be severe. Indeed, a focus on concealment and damage control, as opposed to targeted retention based on operational, legal or institutional value, may even result in criminal penalties. Sections 802 and 1102 of the Sarbanes-Oxley Act of 2002 provide for fines and/or up to 20 years’ imprisonment for destroying or concealing documents or other evidence with the intent to impair their availability for use in a proceeding or with the intent to impede, obstruct or influence federal investigations or bankruptcy proceedings.

In civil litigation, records management programs that focus on eliminating “bad documents” may be criticized as illegitimate “document destruction” policies that may result in severe sanctions, including default judgment. See *Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 286 (E.D. Va. 2004) (finding policy was developed and implemented with intent to destroy documents relevant to anticipated litigation); *Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73 (D. Mass. 1976) (a party cannot adopt a records management system designed to obstruct discovery); *Reingold v. Wet ‘N Wild Nev., Inc.*, 944 P.2d 800, 802 (Nev. 1997) (finding a one-season retention policy at a water park was unreasonable as “deliberately designed to prevent production of records in any subsequent litigation”; remanding for a new trial and holding that an adverse inference instruction was appropriate in the circumstances); cf. *United States v. Arthur Andersen, LLP*, ___ F.3d ___, 2004 WL 1344957 (5th Cir. June 16, 2004) (jury verdict finding accounting firm guilty of obstructing an official proceeding of the Securities and Exchange Commission, in violation of 18 U.S.C. § 1512(b)(2)).

Illustration ii. Acme Corporation’s stock prices have been dropping and it suspects that in its last securities offering some corners may have been cut. It reasonably anticipates that it may be named in a class action securities lawsuit or investigated for securities fraud in the foreseeable future. It implements a records management policy focused on destroying, among other things, high level e-mail communications that will probably be the focus of discovery in the investigation. Acme’s policy may be viewed with a high level of scrutiny and be considered geared

toward destruction of evidence, potentially subjecting it to spoliation claims and possible criminal sanctions.

For organizations with international operations or data, determining all applicable legal requirements can be very complicated. For example, the Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that each person has a right to the protection of personal data and that such data must be processed fairly, for specified purposes and on the basis of the consent of the person or some other legitimate lawful basis (Article 8). This right includes the fundamental right to access personal data and to correct any mistakes in that data. The legislation protecting individuals' rights in relation to personal data is mostly contained within Directive 95/46/EC on Data Protection (the "Directive"), which seeks to harmonize the applicable national legislation for each member state. In the People's Republic of China, on the other hand, there is limited regulation on document retention in place, but it is generally understood that the civil law principle protecting the right to privacy also applies in relation to the protection of personal data. *See also* Comment 4.h, *infra*.

Comment 2.d.

An organization should assess the operational and strategic value of its information and records in developing an information and records management program.

Information and records can be valuable strategic assets. Indeed, organizations invest substantial capital in generating and storing electronic information representing a wealth of institutional knowledge. The value of these assets often depends on the accessibility of the information. An effective program should reflect the value of an organization's information and records.

An organization's information and records management program will necessarily reflect judgments on how best to capture and manage records, including electronic records, which have lasting value to the organization.⁷ *Cf. Pub. Citizen v. John Carlin*, 184 F.3d 900, 910-11 (D.C. Cir. 1999) (finding it appropriate under federal statute to allow agencies to maintain record-keeping systems in the form most appropriate to the business of the agency, reflecting its administrative, legal, research and other values, and without regard to the prospective interests of future researchers).

Illustration iii. A large pharmaceutical manufacturer has developed several promising new leads on anti-viral drugs, but has suffered significant turnover in its lead researchers. Because the company's information and records management program specifies that all records relating to research projects should be kept for one year past the time a product resulting from the research is brought to market or three years after the research is officially terminated, the company's newest researcher is able to review the work of her predecessors and determine what areas deserve greater study without the amount of trial and error that might otherwise be necessary.

Illustration iv. PatentCo is involved in a dispute concerning the validity of certain patents it owns, alleging that they are being infringed by several of its competitors. In developing its processes, PatentCo's scientists kept electronic laboratory notebooks detailing each step of their research and their discovery of the

⁷ Appendix C to this document provides a sample assessment tool that can be used as a starting point by organizations addressing records management issues, with particular emphasis on electronic information. Of course, this form is generic and will need to be tailored to fit particular circumstances.

process that resulted in the patented invention. PatentCo's records management policy and retention schedule requires that laboratory notebooks be kept permanently so that it can re-create the inventive process if necessary. When patent litigation occurs later, PatentCo is able to show that it filed its patent application less than one year from the date of its scientist's discovery of a successful process, avoiding a claim that its patent is invalid.

The value of information will vary greatly from organization to organization, and even within an organization. How an organization chooses to capture this value may also vary accordingly. One organization may choose to concentrate its resources on capturing the value in its research or product development records while another may emphasize its sales or marketing resources. The solutions, policies, practices and training employed, as well as the technological resources invested, will reflect internal business judgments as to the best approach for that entity. This makes it impossible to develop a "generic" information and records management policy appropriate for every organization. *See* Comment 1.c, *supra*. Organizations should make a conscious effort to recognize and make accessible the information necessary to meet the organization's needs and responsibilities. Conversely, information not of value may and should be discarded, *see* Guideline 3, subject, of course, to the need to preserve all discoverable information needed for litigation purposes. *See* Guideline 5.

Comment 2.e.

A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

Business continuation or disaster recovery plans and programs, such as those employing backup systems, allow an organization to rebuild its electronic information systems and to continue operations despite a significant network failure. *Cf.* Marianne Swanson et al., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (2002). What must be stored in order to achieve this goal and the manner and length of storage time will generally be decided by an organization's information technology professionals (with substantive input from the other disciplines—operational, records management and legal) as the individuals who will be relied on to manage the recovery. Consideration should typically be given to making the storage time period as short as possible—only that amount of time that is truly necessary to recover from a disaster.

There is general consensus that regardless of the various capabilities of different backup systems, those systems are designed for the purpose of business continuity and should not be used as a substitute for records management. While the back-up systems can provide critical capabilities to recover data when necessary, those capabilities are fundamentally different from what is required for information and records management. Moreover, after a relatively short period of time, it is simply impractical for back up systems to retrieve efficiently or effectively specific, targeted information. Accordingly, it would be useful and reasonable to reflect this in the policies, procedures and programs by separately providing for disaster recovery systems and procedures applying to electronic information and records management.

The policy for disaster recovery for electronic information should describe:

- What constitutes a "disaster" requiring information restoration;

- What must be retrieved when there is a “disaster;”⁸
- What will be stored for access in the event of a “disaster;”
- Who has responsibility for duplicating and managing electronic information;
- Where and how it will be stored;
- How often on-line (active or archived) electronic information will be duplicated to ensure retrieval and system recovery; and
- How long duplicate copies of electronic information must be kept before they are destroyed (through deletion or otherwise).

If disaster recovery storage devices and procedures are separate from the organization’s systems for normally managing electronic information and records, then cycles for re-use of disaster recovery backup media should be relatively short, resulting in significant cost savings. *Cf.* Comment 5(e).

Illustration v. Acme Corporation maintains disaster recovery backup tapes in the event of a system failure at its headquarters. One of the Vice-Presidents of Operations routinely deletes documents and e-mail messages that he later determines he needs to review again. He has instructed the IT staff at Acme to retain disaster recovery backup tapes indefinitely so they can find any documents he loses in the future, thinking that the cost is the incremental cost for additional storage tapes. The real costs to the company are far greater. They include: storing the extra backup tapes in a logical manner to allow retrieval if needed, having enough time to mount and load disaster recovery backup tapes to locate the server and file in question, and, most importantly, the labor costs involved in loading the data, restoring the system and locating the file. Due to Acme’s recovery system configuration this process takes many hours. Thus, the cost of this *ad hoc* plan to recover a single lost document can quickly run into thousands of dollars, making such a program inefficient and ill-advised. Moreover, this practice may increase the risk that a court may determine the organization’s backup tapes are “accessible” and hence should be part of the organization’s initial response to routine discovery requests. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003).

The use of backup data for near-term recovery of deleted, corrupted or otherwise damaged files should not alter the consideration of disaster recovery data as an inappropriate substitute for a retention program. In particular, larger organizations today often use enterprise backup systems that maintain sophisticated database structures permitting specific files on the system to be identified and recovered with relative ease in the short term. This functionality can be very important for business purposes when an employee accidentally deletes or ruins a file that embodies significant work, or where the file becomes corrupt or damaged. Most IT organizations look at the ability to assist the business in this way as a key feature of a good backup system. Yet, the ability of the system to recover files is typically limited to a very short time period because tracking the files requires a database that soon would grow to unmanageable proportions if retention were extended. Thus, whether the “disaster” is a natural catastrophe (*e.g.*, flood) or one of the digital age (*e.g.*, corrupted

⁸ See, for example, the concept of “vital records protection” as described in ANSI/ARMA 5-2003, *Vital Records Programs: Identifying, Managing and Recovering Business Critical Records*.

files), systems that address business continuity concerns are not substitutes for records management policies and programs.

Having a meaningful policy and procedures for disaster recovery does not require that the related systems and technology must be separate from other information technology solutions for the enterprise. However, any combination must be done consciously, recognizing that the electronic information may be serving multiple functions.

3. An organization need not retain all electronic information ever generated or received.

Comment 3.a.

Destruction¹ is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.

At the heart of a reasonable information and records management approach is the concept of the “lifecyle” of information based on its inherent value. In essence, this means that information and records should be retained only so long as they have value as defined by business need or legal requirement. Thus, while some documents contain information which is deemed irreplaceable and must be indefinitely retained (or “archived”), information and records that do not have such continuing value to the organization can be destroyed or deleted when the organization, in its business judgment, determines it is no longer needed, regardless of the form (*i.e.*, paper or electronic). Of course, this destruction in the ordinary course is subject to suspension when there is actual or reasonably anticipated litigation. *See* Guideline 5 and commentary; *see also* *The Sedona Principles: Best Practices, Recommendations, and Principles for Addressing Electronic Document Production*, Principle No. 5 (Jan. 2004) (“The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.”) and associated commentary.²

Retaining superfluous electronic information³ has associated direct and indirect costs and burden that go well beyond the cost of additional electronic storage. The direct costs include additional disk space, bandwidth, hardware, software, archival systems and the cost of their related media migration requirements and possibly even storage area networks to store such information. The cost of storage alone can be significant, particularly where minimum standards exist concerning the storage media for such information.⁴

The indirect costs include the cost of technical staff for maintaining such information, the cost of personnel classifying such information, and the potential cost of outside counsel to review and exclude irrelevant electronic information in the discovery process.

There is no question that managing unneeded information increases an organization’s costs, burdens, and ability to fashion an adequate and timely defense in litigation. For example, irrelevant electronic information can hamper efforts to locate and produce information or records that are requested in litigation. This can lead to substantial monetary sanctions when required records or information are not timely produced. An organization can control these costs by identifying information of value to it, and reducing the amount of irrelevant electronic information that it

¹ We use the word “destruction” so there is no ambiguity. An organization, in drafting its policy, may use different terminology.

² It is important to note that not all threatened litigation or conceivable disputes will trigger preservation obligations. The analysis, however, must be done on a case-by-case basis and organizations should be prepared to analyze such situations as they arise. *See* Guideline 5.

³ If it is superfluous (*i.e.*, unnecessary), it would, by definition, not have even marginal value.

⁴ *See* ANSI standards for storage of magnetic and digital information, which include monitoring of temperature and humidity levels, physical security, magnetic field restrictions, acceptable fire retardants, exercising magnetic tape to prevent stiction, etc.

retains. See *Smith v. Texaco, Inc.*, 951 F. Supp. 109, 112 (E.D. Tex. 1997), *rev'd on other grounds*, 263 F.3d 394 (5th Cir. 2001) (court upheld temporary restraining order prohibiting defendants from altering or destroying documents related to employment discrimination litigation; however, given the high cost of electronic storage, court permitted deletion of electronic documents in the ordinary course of business so long as hard copies were kept).

Managing superfluous information does not merely result in unnecessary costs. It also drains an organization's limited internal and external human and material resources. It diverts the organization's internal resources from advancing the organization's principal business objectives of efficiency and productivity. It diminishes the organization's ability to compete in the marketplace, while unduly increasing the cost of doing business. Dealing with the issues that can arise from having too much information in litigation can also divert the attention of an organization's outside counsel from the strategic and substantive issues to matters of discovery and process.

Courts routinely acknowledge that organizations have the "right" to destroy (or not track or capture, whether or not it is consciously deleted) electronic information that does not meet the internal criteria of information or records requiring retention. See *McGuire v. Acufex Microsurgical, Inc.*, 175 F.R.D. 149, 155-56 (D. Mass. 1997) (in the employment context, while there is no broad right to "broom clean" internal investigation files or edit personnel records "willy-nilly," employers may call for and edit drafts, and discard them where there are errors made by someone other than the accuser; "to hold otherwise would create a new set of affirmative obligations for employers, unheard of in the law—to preserve all drafts of internal memos, perhaps even to record everything no matter how central to the investigation, or gratuitous"); cf. *United States v. Arthur Andersen, LLP*, ___ F.3d ___, 2004 WL 1344957, at *11 (5th Cir. June 16, 2004) ("A routine document retention policy, for example, evidences an intent to prevent a document from being available in any proceeding. But it does not alone evidence an intent to "subvert, undermine, or impede" an official proceeding."); *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 748-49 (8th Cir. 2004) (recognizing legitimate aspects of a retention program that resulted in the destruction of materials). But see *Morris v. Union Pac. R.R.*, 373 F.3d 896 at 900-01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper, distinguishing facts in *Stevenson*).

It should be noted, however, that deciding not to track or capture electronic information does not render it immune from discovery should litigation ensue. An organization may thus reduce the amount of superfluous electronic information that it retains even where litigation is involved, provided that its preservation obligations are met.

Illustration i. Company A, which does not have an automated program to enforce e-mail retention and disposition, collects 1 million pages in e-mail and associated attachments from 25 employees in preparing a response to a government investigation. All pages are data converted and scanned at a cost of \$0.20/page, a total of \$200,000. A team of attorneys reviews the collection for relevance to the request and for privilege determinations at a cost of \$0.50/page, \$500,000 total. Upon completion of the culling process it is found that 10%, or 100,000 pages were responsive to the request. Company A has spent \$700,000 to produce 100,000 pages. It is safe to estimate that between 50–75% of the records retained in the employee's e-mail accounts did not have "retention value." Therefore,

Company A has spent between \$350,000–\$525,000 on processing records that had no value and were retained for no purpose.⁵

Comment 3.b.

Systematic deletion of electronic information is not synonymous with evidence spoliation.

Proper destruction of electronic records or other information consistent with a reasonable approach to managing information and records is not synonymous with spoliation of evidence or obstruction of justice. Absent extraordinary circumstances, if an organization has implemented a clearly defined records management program specifying what information and records should be kept for legal, financial, operational or knowledge value reasons and has set appropriate retention systems or periods, then information not meeting these retention guidelines can, and should, be destroyed. Destruction of this information is not spoliation of evidence. *See Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892, 921 (1995) (“good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce documents in discovery”), *overruled on other grounds by Cedars-Sinai Med. Ctr. v. Superior Court*, 18 Cal. 4th 1, 74 Cal. Rpt. 2d 248, 954 P.2d 511 (1998); *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (considerations are: (1) whether the records management policy is reasonable considering the facts and circumstances surrounding the relevant documents; (2) whether the policy was adopted in bad faith; and (3) whether lawsuits have been filed or complaints made in the past with such frequency or in such magnitude that it is obvious that certain categories of documents should be retained);⁶ *see also Vick v. Tex. Employment Comm.*, 514 F.2d 734, 737 (5th Cir. 1975); *Moore v. Gen. Motors Corp.*, 558 S.W.2d 720, 735 (Mo. Ct. App. 1977); *Chrysler Corp. v. Blackmon*, 841 S.W.2d 844, 847-50, 853 (Sup. Ct. Tex. 1992) (in products liability action, extreme sanction of default judgment was not warranted where car manufacturer failed to produce crash-test reports and other documents that had been destroyed pursuant to document retention policy); *Stapper v. GMI Holdings, Inc.*, No. A091872 2001 WL 1664920, at *9 (Cal. App. Dec. 31, 2001) (not officially reported) (finding trial court did not abuse its discretion when it refused to allow evidence that copies of complaints made before 1995 had been destroyed pursuant to a document retention policy when there was no evidence of a willful attempt to suppress evidence and plaintiff had access to computer records with brief summaries of complaints dating to 1982).

Where an organization in good faith adopts a reasonable document retention policy, and its operation and procedures are rational, it should be permitted to continue those procedures after commencement of litigation, assuming reasonable steps have been taken to preserve data relevant to actual or reasonably anticipated litigation, governmental investigation or audit. *See* Martin C. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L. J. 561, 621 (2001) (“(1) Electronic evidence destruction, if done routinely in the ordinary course of business, does not automatically give rise to an inference of knowledge of specific documents’ destruction, much less intent to destroy those

⁵ The figures used are hypothetical and other approaches and cost figures would yield different results.

⁶ Some commentators argue that *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002) (“RFC”) creates a pure negligence standard for spoliation, which may be seen as casting doubt on the continued validity of these cases. RFC does hold that “discovery sanctions, including an adverse inference instruction, may be imposed upon a party that has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence.” This may be an overbroad interpretation of the importance of the RFC case, which read carefully may be significantly limited by its facts. Furthermore, the recent case, *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 745-51 (8th Cir. 2004), makes it clear that the requirement for intentional or bad faith destruction is critical to analyzing “culpability” to determine what sanctions, if any, should attach to the loss of evidence.

documents for litigation-related reasons, and (2) to prohibit such routine destruction could impose substantial costs and disruptive burdens on commercial enterprises.”) Similar rules should apply before the formal commencement of litigation. *See generally Morris v. Union Pac. R.R.*, 373 F.3d 896 at 900-01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper); *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 748-49 (8th Cir. 2004); *Vick v. Texas Employment Comm’n*, 514 F.2d 734, 737 (5th Cir. 1975); *Moore v. Gen. Motors Corp.*, 558 S.W.2d 720, 735 (Mo. Ct. App. 1977); *Chrysler Corp. v. Blackmon*, 841 S.W.2d 844, 847-50, 853 (Tex. 1992). It is imperative, however, that destruction is carried out consistently and non-selectively in conformance with the standard operating procedures for the organization.

Comment 3.c.

Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.

Unless there is an applicable retention obligation imposed by statute or regulation, or there is a legal hold imposed by virtue of litigation, audit or investigation (*see* Guideline 5), organizations can legitimately prescribe retention (or deletion) periods for recorded communications, such as electronic mail, instant messaging, voice over IP, text messaging and voice-mails. There are several ways to approach the management of these communications. Some organizations impose space requirements (*e.g.*, 1 MB limit for e-mail boxes where users are unable to send new messages once the limit is reached). Others impose time restrictions (*e.g.*, all non-folded e-mails more than thirty days old will be automatically deleted). Indeed, organizations can set up Instant Messaging so that archiving of the typed conversation is not allowed and the text disappears when the session is closed. Other organizations have used a hybrid approach, which provides that most communications are to be deleted within a prescribed number of days, but communications that have a true business critical nature can be retained for a longer period in public or shared folders. For example, if there is a construction project, e-mails relating to that construction project may be maintained for the life of the project in a public or shared folder, but should be deleted after the conclusion of the project.

As noted earlier, the selection of any particular solution involves complex and competing policy issues best resolved by careful discussions among an interdisciplinary team. For example, while the IT group may effectively advocate a policy against using a network for individual archiving, employees can often archive messages on their own local hard drives (*e.g.*, with .pst files for e-mail within a Microsoft Outlook environment). This ad hoc “work around” will result in additional time and cost if the scattered information needs to be retrieved or reproduced. Organizations that rely heavily on e-mail may find it difficult to implement a strict disposal period without sufficient safeguards to protect against the loss of important information. This highlights how important it is for organizations to adopt policies, procedures and processes that best meet their business needs, while satisfying their legal obligations.

In addition, there may be some circumstances where an organization is legally obligated to retain all forms of communications. For example, the investment industry is under a requirement to maintain for a specified period all communications with certain investment customers. Alternatively, some organizations actually use e-mail to document specific transactions and, therefore, the e-mail itself might be a transactional record that should be retained under the tax laws and regulations. Before implementing a policy regarding the automatic destruction of electronic communications, the organization must have a good understanding of its legal obligations as well as its business practices.

Moreover, any organization that regularly deletes data based on a regular time period may need to be able to suspend such automatic deletion (*i.e.*, as part of a legal hold) for some or all users, or otherwise provide a retention process or mechanism, as may be necessary to comply with preservation obligations. *See generally* John C. Montaña, *Legal Obstacles to E-Mail Message Destruction* (ARMA Int'l Educ. Foundation 2003). Furthermore, organizations that adopt a time or space based approach should consider that the varying usage levels of different employees may result in the disparate application of policies and inadvertent loss of valuable information unless there is adequate education and effective procedures to cull records from non-relevant information. Indeed, a policy that routinely deletes "old" data (such as e-mail messages) without any other protections can be analogized to destroying boxes in a warehouse based on where they are on the shelf without any regard to the contents.

Organizations should also be free to migrate data from one form to another to create the record of an event or transaction. For example, many organizations have customer call centers where voice messages or customer conversations may be recorded. In the absence of a regulatory obligation, the organization, in the reasonable exercise of its business judgment, may choose to transcribe part or all of the recorded message, preserving the transcription and deleting the recording in the ordinary course. Similarly, some organizations employ unified messaging systems which convert recorded voice messages into digital formats including e-mail, and vice versa. In the absence of a regulatory obligation, the organization, in the reasonable exercise of its business judgment and consistent with a retention policy it may adopt, may choose to retain the message in only one format, or not at all.

Comment 3.d.

Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.

If an organization has duplicated and retained data to ensure business continuity in the event of a disaster (such as a system failure), the organization may routinely recycle that hardware or media (and destroy the temporarily retained contents) as a matter of course. *See* Comment 2.f.

The mere existence of actual or reasonably anticipated litigation, investigation or audits should not ordinarily alter such routine recycling and destruction provided that there are reasonable steps taken to preserve the relevant data maintained in other locations within the organization for such purposes. However, each organization should consider and be prepared to react to any unique circumstances that may require suspending the ordinary recycling and destruction process if it is required by court order or otherwise (*i.e.*, where the data is relevant and not being saved through some other means). *See generally* Guideline 5 and commentary.

Comment 3.e.

Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.

In the ordinary course of business, organizations routinely migrate information from old to new hardware and software platforms at various times. An organization need not copy and retain the residual, shadowed or deleted data⁷ that may reside on the old hardware, media or system platform. Instead, as part of the migration and recycling process, such data can be routinely destroyed. In addition, organizations may routinely use processes that delete temporary data (such as residual, shadowed or deleted data) from company computers. This would include temporary files such as

⁷ *See* Appendix E for the definition of these terms.

cached website files. Absent a specific legal or business need, there are no impediments to such a process.

However, an organization that employs a routine system or program to destroy such data should undertake reasonable steps to identify and retain unique data that must be retained in accordance with legal obligations and also institute reasonable processes to suspend the routine destruction as may be required by court order or otherwise. *See generally* Guideline 5 and commentary.

Comment 3.f.

Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

In the ordinary course of business, organizations routinely migrate information from one form to another. For example, some organizations use a printed or imaged document as the final or official version of a record. Printing an electronic document to an image (such as .tif or .pdf formats) or paper can eliminate some or all of the metadata associated with the electronic version of the document. This metadata can include system information (such as file identification tags) or it can contain potentially more meaningful information (such as author, editors, and dates associated with creation, editing or printing of the file).

Absent a specific legal or business need, an organization need not retain the electronic version of a document and its associated metadata. Indeed, the National Archives has mandated the paper retention of records in a number of instances. *Cf. Pub. Citizen v. John Carlin*, 184 F.3d 900, 909-11 (D.C. Cir. 1999) (finding it appropriate under federal statute for agencies to maintain record-keeping systems in the form most appropriate to the business of the agency, reflecting its administrative, legal, research and other values, and without regard to the prospective interests of future researchers).

This is another instance where what is legally required and what an organization might do could diverge. For example, metadata may provide a wealth of information that can allow an organization to better retain and organize its information. Many organizations employ information and records management programs that specifically use metadata tags to cull and organize information. And, it may be that certain metadata is critical to an organization's ability to audit and track access to information so that it can, for example, identify and stop any improper access to sensitive information by unauthorized personnel. Thus, for some organizations it may be unworkable and unwise to routinely discard metadata. An organization should consider the best format in which to retain information to meet good business practices as well as legal requirements. *See* Comment 4.e and Appendix D.

If an organization migrates electronic versions with associated metadata to other versions without that metadata, the organization should consider if and how it would preserve electronic versions including metadata if it has actual notice (by court order or otherwise) that the metadata is material and needs to be preserved. For example, lawsuits may involve a need to examine the metadata associated with documents to establish facts regarding the document and its genesis, modification or distribution in particular instances. In those specific situations where particular metadata is known to be material to the dispute, the loss of such metadata may be seen as spoliation of evidence, which can have negative consequences for the organization. *See generally* Guideline 5 and commentary.

4. An organization adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

As explained earlier, an organization has considerable latitude in choosing how to manage its information and records. In this section we examine issues an organization may consider in formulating procedures to create or maintain a successful retention program. As noted earlier, there is no “one size fits all” approach to such retention programs. Organizations will take different approaches, even internally, based upon their unique history, facts and circumstances. Importantly, there must be an explicit recognition that there will be substantial differences in the approach of a 20-employee local operation versus that of a 100,000 employee multinational corporation. That said, like other aspects of corporate governance, the consistent application of the specific policies and procedures that are adopted will greatly enhance the likelihood that the program will meet its intended objectives. *See* ISO 15489-1.

Comment 4.a.

Information and records management policies must be put into practice.

The responsible handling of electronic information and records should be considered a core value of an organization. To be effective and defensible, policies should not be written and then filed on a shelf, never to be looked at again. Indeed, a policy in name only may be worse than no policy at all. Incomplete or inadequate execution of an electronic information and records management policy may result in the loss of valuable business information. For example, employees may unknowingly destroy electronic information before the end of its useful life, or store so much useless electronic information that useful information is difficult to identify or access when needed.

An organization that has adopted a retention policy should also consider documenting its records retention efforts. This documentation could include copies of the training materials and resources, as well as any documents reflecting changes to the policy or implementation of its provisions.

Comment 4.b.

An organization should define roles and responsibilities for program direction and administration within its information and records management policies.

Effective implementation of a reasonable information and records management policy requires the participation of individuals throughout the organization. However, some individuals necessarily have greater responsibilities in ensuring the policy’s success. In larger organizations prepared to invest in the process, those individuals with greater responsibilities could include:

- ***Executives and senior management***, who may oversee the creation of the information and records management policy and strategy, should provide the resources for initial and ongoing implementation and compliance, and periodically review operational realities of the program;
- ***Records officers***, who may be responsible for overall design and management of the information and records policy and the overall records management program;
- ***Legal department or compliance officers***, who should be responsible for coordinating legal retention obligations, including legal holds;
- ***Business unit managers***, who should establish internal procedures to ensure that records of business transactions and events are created, received and retained to meet business and legal requirements; and

- **System managers and administrators**, who should be responsible for the reliability and continuing operation of systems used to generate, retain and dispose of electronic information and records.

Not all organizations will have the resources or personnel available or will identify a need to fill such positions. However, the manner by which an organization addresses its responsibilities is not as important as the basic identification and distribution of responsibilities so that the information and records management program can succeed in practice.

The absence of a well-coordinated multidisciplinary approach has hurt organizations in the litigation context when the preservation of data was at issue: *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2004 WL 1620866, at *1 (S.D.N.Y. July 20, 2004) (failure to communicate within organization and with counsel led to late productions and loss of data); *Keir v. UnumProvident Corp.*, No. 02 Civ. 8781, 2003 WL 21997747, at *6-8 (S.D.N.Y. Aug. 22, 2003) (failure to communicate order to preserve clearly, directly, timely and effectively to IT staff and outside vendor led to overwriting and loss of some electronic data); *GFTM, Inc. v. Wal-Mart Stores, Inc.*, 49 Fed. R. Serv. 3d 219, No. 98 Civ. 7724, 2000 WL 335558, at *2 (S.D.N.Y. Mar. 30, 2000) (counsel failed to discuss the company's computer capabilities with knowledgeable person in the MIS department before representing to court that company did not have centralized computer capability for tracking locally purchased goods; information existed at that time but was eliminated from company system in year following and before person-most-knowledgeable deposition, resulting in order that company pay expenses and legal fees); *United States v. Koch Industries, Inc.*, 197 F.R.D. 463, 486 (N.D. Okla. 1998) (court permitted plaintiffs to inform jury that relevant computer tapes were destroyed, but did not permit adverse inference instruction where "[defendant]'s uncoordinated approach to document retention ... denied plaintiffs potential evidence to establish the facts in dispute"); see *Landmark Legal Foundation v. EPA*, 272 F. Supp. 2d 70, 79 (D.D.C. 2003) (at hearing on preliminary injunction, government represented that it would preserve responsive materials but, on motion for contempt following issuance of injunction, plaintiff established that EPA had failed to distribute preservation order widely enough to include IT staff responsible for preserving of e-mail backup tapes, to several individuals at the agency who had the requested data, or to the acting administrator); *Linnen v. A.H. Robins Co.*, No. 97-2307, 1999 Mass. Super. LEXIS 240, at *5-7, 25-33 (June 16, 1999) (where counsel for responding party did not understand client's systems for maintaining e-mail, including backup tapes, and consequently provided erroneous information to opposing counsel and the court for more than 18 months, substantial monetary sanctions were inappropriate; however, because poor communications resulted in recycling of certain backup tapes, adverse inference instruction was appropriate).

Special attention should be given to identifying an individual with broad understanding of the process who, if necessary, may serve as the declarant or witness if the policy becomes an issue. Indeed, under recent proposals at the state and federal court levels, such a witness may need to be identified early in any litigation.

The policy should be visibly supported by senior management. Courts in the discovery context expect that management within organizations will attend to document retention issues in a meaningful fashion. See *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *40-41, 53 (N.D. Ill. Oct. 23, 2000) (failure to take reasonable steps to preserve data at the outset of discovery resulted in a personal fine levied against the defendant's CEO); *In Re Prudential Ins. Co. of Am. Sales Practice Litig.*, 169 F.R.D. 598, 615 (D.N.J. 1997) ("The obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers."); see also Daniel L. Pelc and Jonathan M. Redgrave, *Challenges for*

Corporate Counsel in the Land of E-Discovery: Lessons from a Case Study, 3 ANDREWS E-BUSINESS LAW BULLETIN 1 (Feb. 2002). In determining the reasonableness of a retention policy, courts may also look to the level of support from senior management.

Comment 4.c.

An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.

An organization's technology and information created with that technology are not the property of the individual. They are assets of the organization and should be managed accordingly. The organization's policy should set forth a process used to identify what should be retained and establish parameters to be used when selecting the most appropriate media for retention.

The records management profession generally speaks in terms of an "official record" or the official version of a record. The legal profession has long used the term "original," at least with regard to evidentiary requirements. See FED. R. EVID. 1002 ("To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."); cf. FED. R. EVID. 1003 ("A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."). With electronic information, such distinctions may be elusive. An organization should seek to establish criteria for determining the form and version of a record that is most appropriate to meeting its business and legal needs.

An organization should also consider the issue of "draft" documents and make rational decisions concerning their retention or destruction based on articulated business needs or legal requirements. Designating one version of data or an electronic record as the authoritative or official version does not eliminate the need to manage other versions of that electronic information which may exist as drafts or duplicates saved by the author or recipient(s). See Donald Skupsky, *Establishing Records Retention Periods for Electronic Records*, INFORMATION RECORDS CLEARINGHOUSE (2000), at <http://www.irch.com/articles/articl09.pdf>.¹ Draft records include working files such as preliminary drafts, notes, supporting source documents and similar materials. Retaining draft records may assist in reconstructing events, such as the negotiations of a contract or license, and for that reason may have value to the organization. If draft records are shared with outsiders, it may also be useful to retain one complete set of those drafts that were exchanged (but not all internal drafts and comments) as proof of the development of the final document.

Illustration i. The Director of Global Research for a company is engaged in biotechnology licensing negotiations with another company that is a direct

¹ See Donald S. Skupsky, *Legal Issues in Records Retention and Disposition Programs*, at http://www.irch.com/articles/article_frame.htm (setting forth factors, legal requirements, and guidelines to be considered in the creation of an overall records retention and disposition program, and the procedures to be followed in developing the legal requirements section of the records retention program); Donald S. Skupsky, *Applying Records Retention to Electronic Records*, INFO. MGMT. J., July 1999, at 28 (reviewing special retention problems posed by electronic records and suggesting a methodology for developing and implementing electronic recordkeeping systems); David O. Stephens and Roderick C. Wallace, *Electronic Records Retention: Fourteen Basic Principles*, INFO. MGMT. J., October 2000, at 38 (examining how electronic records have transformed the nature of information management and discussing the application of traditional records retention principles for visible media to electronic recordkeeping environments; the article also suggests a practical methodology for developing electronic records retention schedules).

competitor in some markets. A license is obtained and later there is a dispute about the scope of its terms. The Director is certain that a key term to support his company's position was inserted by a member of the opposing negotiation team. Others from his own team have left the company or have no memory of the exact negotiations. With the help of his lawyers he is able to reconstruct the drafting history from the set of exchanged drafts retained by the legal department.

However, absent a specific legal requirement, in most circumstances drafts of policies, memos, reports and the like will not have continuing value to the organization and need not be retained once a final record has been created. For example, draft employee evaluations could conceivably contain unique information and mental impressions concerning a decision or action, yet some courts recognize they need not be retained. *See, e.g., McGuire v. Acufex Microsurgical, Inc.*, 175 F.R.D. 149, 153-56 (D. Mass. 1997) (no obligation to preserve all drafts of internal memos and no sanctionable conduct in deleting a paragraph from personnel evaluation even after state discrimination commission proceedings commenced; court found that employer had no obligation to make sure that no false information was placed into personnel file; employer could review drafts of personnel memoranda and discard them with the editing related to obvious errors made by other than the accused harasser). On the other hand, drafts must be retained if they are relevant to actual or reasonably anticipated litigation, governmental investigation, or audit. *Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 288-91 (E.D. Va. 2001) (breach of duty to preserve drafts of expert reports warrants sanctions). In such instance a legal hold should be issued to specify the need to retain records that could otherwise be discarded.

In short, the organization should consider procedures by which it captures versions of the information or record that have a separate business need for retention (*e.g.*, meaningful drafts, etc.), but then presumptively discard the rest (absent some preservation requirement).

Comment 4.d.

An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.

Electronic information and records management is enhanced when records have custodians throughout their existence to ensure their credibility, reliability, accessibility and ultimate disposition or destruction. Accordingly, an organization may consider defining (formally or informally) the roles and responsibilities of employees regarding electronic information and records. The identification and role of actual "custodians" will vary with the types of tasks to be done and the point in its lifecycle of the electronic information or record. A record may require several custodians throughout its lifecycle, including a "content" as well as a "technology" custodian.

Content custodians can address creation and preservation of the information, while technology custodians may be responsible for its logical and physical care. Content custodians may include the business unit or process owners who establish and maintain procedural controls to ensure that appropriate electronic records are created, received and retained to meet business and legal requirements. Content custodians can also include the originator or recipient of an electronic record, or their successors in the business unit function, during the normal course of business activities. These individuals are responsible for authorizing the destruction of electronic information and records in accordance with approved retention policy, and any preservation obligations due to actual or reasonably anticipated litigation, governmental investigation or audit.

Technology custodians can ensure that the automated environment used to generate or receive electronic records: (a) maintains appropriate metadata and content infrastructure; (b) provides

mechanisms to validate electronic records authenticity and ownership; (c) protects active electronic records by implementing a comprehensive disaster recovery strategy; (d) archives inactive electronic records needed to satisfy long-term operational, historical or compliance requirements; (e) preserves electronic records and information as needed to meet litigation, investigation or audit requirements; and (f) applies the disposition requirements specified in the retention policy established by the organization to those electronic records that have exceeded their approved retention periods and that are not subject to any legal holds.

Content custodians and technology custodians can also establish procedures to transfer the ownership of electronic information and records from one business function to the next, for example, during the course of organizational changes such as reorganizations, acquisitions/divestitures and employee retirement, termination or reassignment. *See* Comment 4.i.

An organization is responsible for managing its information and records even when it uses outside contractors to create, manage, store and dispose of information and records. As a best practice, records retention policies should extend to an organization's outside contractors, consultants and other service providers, when they are used to create, manage, store or dispose of information and records. Specific record retention requirements may need to be set forth in contracts or statements of work with those third parties.

Comment 4.e.

An organization should consider the impact (including potential benefits) of technology on the creation, retention and destruction of information and records.

For many reasons, identifying, capturing and managing electronic information and records may be a more difficult task than for paper records. The volume of electronic information generated, received and at least temporarily retained as a function of technology is significantly greater than the volume of paper information previously generated. This creates challenges in identifying and managing this greater scope of electronic information.

As a best practice, organizations should consider IT functions, structure and capabilities in developing an information and records retention policy and program. Indeed, emerging technical solutions may obviate a number of previously required human steps in classifying data in some organizations. Further, an organization should consider the impact on its retention program of proposals to migrate to new technologies or applications. As but one example, adopting a unified messaging system that translates recorded voice messages into digitized text files that can be stored and searched just like e-mail may have significant implications for an organization's retention program.

Metadata: An organization's information and records management policy should consider whether to preserve metadata² for purposes of authentication, security, data integrity, search, retrieval and analysis. Much of the metadata stored by computer systems may be meaningless from the legal or records management perspective. For example, when documents are created, the system automatically generates a variety of identifying numbers and addresses that are used purely for systems purposes. In some types of records management systems, retaining excessive metadata can needlessly increase costs of storage and complexity of a records management system. Therefore, establishing standard metadata criteria (*i.e.*, what information will be preserved and in what form) can also result in substantial savings in retrieval and storage costs.

² *See* Glossary, Appendix E.

Illustration ii. Beta Corporation does not have a formal document management system, and it has discovered that it often has difficulty locating records that are needed for reporting purposes. Beta's records management specialist has recommended the use of document profiling within its document management software. By automatically recording basic information about the document that is supplemented by the author, important records can be located much more quickly through the use of simple searches within the document management system.

A technical discussion about metadata and various implications in the records management context may be found in the Technical Appendix to this document, Appendix D.

Electronic Archives: An organization should consider whether, and to what extent, it uses electronic archives to store data with long-term operational, legal or historical value. Electronic archives preserve and support access to digital information and records with long retention periods that are at risk from technological obsolescence. Ensuring access to electronic archives may be a component of an organization's best practices approach to an information and records management policy. Electronic records with continuing operational, legal or historical value may be transferred from active systems to an electronic archive. A comprehensive archive may act as a repository for both electronic and non-electronic records and can facilitate an integrated search of all records in all formats in the event of litigation, investigation or audit.³ If an organization does not have an archive, special care should be taken that these records and information are otherwise properly protected.

Electronic archives are covered in greater detail in the Technical Appendix, Appendix D.

Automated Tools: An organization should consider whether, and to what extent, automated tools may be useful in managing the information and records contained in its e-mail and other systems. Users of e-mail face the challenge of dealing with many incoming and outgoing e-mail messages daily, even hourly. The life cycle of such electronic information is often extended, not because of determined value or record-keeping requirements, but because of the sheer quantity of material requiring some action. Software programs exist to facilitate automated management of e-mail messages, including "janitor" programs that dispose of e-mail based on given criteria (e.g., time period expiration—30, 60, 90 days after receipt—subject line content matches, etc.), "filtering" programs that screen content and/or direct messages to appropriate parties for response, and "archiving" programs that copy messages to long-term storage and provide message indexing and security functions. These tools should be viewed as reasonable information and records management protocols with two caveats. First, the routine destruction of e-mail based on date or account size alone, such as may occur with the use of janitor programs, can result in the loss of valuable information (e.g., records required to meet regulatory provisions). If janitor programs are used, care should be taken to ensure that valuable e-mail messages are protected from the operation of the janitor program. Second, the tool must allow for the preservation of relevant e-mails in the case of legal holds. See Guideline 5, Comment 5.e.

Should an organization always automatically suspend its e-mail management program when faced with a triggering event such as litigation? If an organization has a function or procedure in place so that e-mails and associated attachments relevant to litigation or investigation are identified and

³ See *Electronic Records Archives Concept of Operations (ERA.DC.COP.1.1.doc)*; National Archives and Records Administration Electronic Records Archives Program Management Office, 2002, available at http://www.archives.gov/electronic_records_archives/about_era/documentation.html.

segregated to preserve them (whether by means of employees segregating the information or by use of automated tools), then it should not have to suspend this part of its record management program, just as it would not suspend the remainder of its program for information not subject to the legal hold.

Comment 4.f.

An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.

Organizations should strive to ensure that employees understand their responsibilities for the appropriate creation, use, retention and destruction of electronic information and records. Different organizations may rely on different means to communicate their policies and procedures. No one method is “best” for every organization. An organization should determine the most effective method of communicating with its employees given the nature, size and culture of the organization. Often, multiple “channels” of communication, including e-mail, voice mail, computer based training, and use of company intranets can be helpful, though such multiple approaches are certainly not mandated.

Illustration iii. Acme Company posts its records management policy on an internal website, along with a list of frequently asked questions and the names and phone numbers of persons to call with respect to different kinds of questions (*e.g.*, legal, technical, tax) about retention issues on its intranet site. The site hosts an on-line training program where an employee answers questions about the policy and its implementation and can sign a certification that the employee has read and understands the policy.

Illustration iv. BasicCo employs 50 individuals in one location and has found that company-wide meetings where policy highlights are discussed and hard copies of policies are given to each employee are the most effective means of communicating important information.

An organization’s training and communication about its information and records management policy and procedures should emphasize the importance of protecting the information assets of the organization and that risks and consequences exist when this responsibility is ignored.

Documentation of the organization’s efforts to educate and instruct employees can support the administration and consistent application of the policy. It may also assist an organization in defending its policy in legal proceedings.

Comment 4.g.

An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.

When implementing a program, an organization should be clear about its expectations for individual responsibility of employees in managing information and records. Organizations should also consider performing periodic compliance reviews of their policies and procedures for managing information and records, and respond to those reviews as necessary through use of appropriate sanctions for failure to comply (*e.g.*, under-retaining, over-retaining and failing to adhere to legal hold requirements). *Cf.* ISO 15489-1 §§ 10-11 (describing possible contours of training and auditing/monitoring programs).

Monitoring compliance with the information and records management policy is not required by law, but is a matter of sound practice. An organization can enhance its prospects for a successful retention program—and reduce its risk of exposure—if it conducts periodic reviews and takes meaningful steps to improve compliance with the program.

Some organizations require employees to acknowledge in writing their understanding of, and responsibility for adhering to, the organization's policies and procedures regarding information and records management. The use of such a procedure is highly dependent upon the organization's culture and, although not necessary for a reasonable policy or practice, it may be useful in certain organizations to assist with policy compliance. In any event, the organization's policies and procedures should also specify that policy adherence will be viewed as a component of an individual's job performance and that appropriate curative steps, including sanctions, may be administered if an employee continually fails to comply.

The review of habits concerning information housekeeping during an annual review, or the process of a litigation collection, may also uncover electronic “pack rats” or the improper use of the organization's information assets. While not part of a formal review process, some channels for feedback to those responsible for monitoring and updating the company's records management program can be beneficial.

Comment 4.h.

Policies and procedures regarding electronic management and retention may be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.

Most organizations have policies that deal with the proper use of facilities and equipment primarily, if not exclusively, for business purposes. Any policies and procedures addressing information and records management ideally should dovetail with such use edicts.

In addition, most organizations have policies and procedures addressing the protection of trade secrets and competitive commercial information (such as employee non-disclosure covenants). Because much of this valuable information is now stored electronically, the need for close integration of efforts is clear.

Furthermore, statutes and regulations addressing the privacy rights of individuals (such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996) have increased the burdens on organizations to ensure that covered personal data is not improperly disclosed. Again, since most of this data resides in electronic format, the advantages of relating (if not marrying) corporate policies and objectives to technical and records management solutions becomes evident.

As noted earlier, *see* Comment 2.d, *supra*, the protection of personal data in the European Union (“EU”) countries is an area that also requires special attention. The Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that each person has a right to the protection of personal data and that such data must be processed fairly, for specified purposes and on the basis of the consent of the person or some other legitimate lawful basis (Article 8). This right is mostly contained within Directive 95/46/EC on Data Protection (the “Directive”) and applies to any data that identifies an individual, including name, address, telephone number or specific physical characteristics. The collection, storage, retrieval, transmission and destruction of data all fall within the definition of “processing” under the Directive. The majority of the obligations with respect to personal data fall on “data controllers,” defined as those responsible for processing personal data. The Directive establishes that data controllers must the following key rules:

- Personal data may only be processed as described to the data subject and with the data subject's consent, unless a specified exception applies (such as when the processing is necessary for performance of a contract to which the data subject is party).
- Data subjects must be given the opportunity to rectify, erase or prevent the use of incorrect personal data.
- Personal data must not be kept longer than is necessary in the circumstances.
- Except in certain circumstances personal data may not be exported from the European Economic Area ("EEA").
- The processing of sensitive data (race, ethnicity, political opinions, religion, trade-union membership, health or sexual preference) is subject to further restrictions, including the need for the data subject to give informed consent to the processing.

U.S. companies have been fined for providing unsatisfactory protection of personal data. For example, in 2000 Microsoft was fined approximately \$60,000 by the Spanish Data Protection Agency for failing to implement sufficient controls when it transferred employee data outside of the EU. As of the time of this publication, the EU has determined that generally the United States does not provide adequate protection for personal data, except for: (a) the specific provisions of the U.S. Department of Commerce's Safe Harbor Privacy Principles; and (b) the transfer of Air Passenger Name Record to the United States Bureau of Customs and Border Protection.

Comment 4.i.

Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

The complexity of managing disparate and ever-changing electronic records is heightened by the fact that most organizations themselves are dynamic—organizations grow and shrink, businesses and assets are bought and sold, employees come and go. Policies and procedures should remain relevant and evolve with changes in legal requirements, organizational structure, business practices and technology. The information and records management policy should be periodically reviewed and revised as required to address changes in business processes that may affect the organization's information and records management practices.

From an operational and records management perspective, organizations should develop procedures to address the disposal and/or transfer of electronic information and records in such a dynamic business and technology climate. For example, when businesses sell information assets, knowing what should and should not be retained is critical. The transition program should address these data ownership issues.

A more common example is where an employee leaves a particular job function or the organization. Procedures governing what to do with electronic information and records associated with that employee will reduce risk (loss of assets) and manage costs (storage of records without owners). One possible approach (among many) is to inventory the employee's electronic records and to assign custody of them to the employee's manager. The manager can then coordinate the review, inheritance and retention of these records, as appropriate. And the manager, or delegate, can provide the appropriate direction to IT concerning the migration or other disposition of the information.

From a legal perspective, there may be circumstances when the legal department should determine whether some or all of the electronic information associated with certain departing employees should be retained. In developing its policies and procedures, an organization should consider the circumstances in which the legal department's involvement is important and provide for mechanisms to incorporate it. It is important to coordinate the efforts of the human resources, law and IT departments closely in these situations, to avoid unintended consequences.

5. **An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, governmental investigation or audit.**

Comment 5.a.

An organization must recognize that suspending the normal destruction of electronic information and records may be necessary in certain circumstances.

An organization's information and records management policy must recognize that certain events will impose a duty to preserve potential evidence or otherwise justify suspending the normal course of records destruction, including the normal procedures for disposing of electronic information and records. Circumstances that may require suspending normal destruction of electronic information and records would include, among others: actual or reasonably anticipated¹ litigation; governmental investigation or audit; preservation orders issued in active litigation; and certain business-related scenarios (*e.g.*, mergers or acquisitions, technology reviews, bankruptcy). *See* Comment 5.e.

Comment 5.b.

An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

Ideally, an organization's information and records management program should have an established process by which it evaluates whether a duty to preserve arises as a result of actual or reasonably anticipated litigation, governmental investigation or audit. Circumstances constituting such notice from a defendant's perspective may include an inquiry from the government, service of a complaint or petition commencing litigation or a third-party request for documents, although other circumstances may lead an organization to consider suspending a destruction schedule. *See United States v. Arthur Andersen, LLP*, ___ F.3d ___, 2004 WL 1344957 (5th Cir. June 16, 2004) (accounting firm had actual knowledge of likely SEC investigation of Enron-related work yet nevertheless failed to suspend ordinary destruction practices (and actually initiated dormant destruction practices under retention policy) until receipt of subpoena for records; court upheld jury finding that accounting firm's actions violated criminal statute prohibiting obstruction of justice); *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 747-48 (8th Cir. 2004) (where defendant railroad was aware that accidents resulting in death or serious injury were likely to result in a lawsuit and that audio tapes were the sole source of particularly relevant evidence, appellate court upheld district court's determination that it was bad faith to destroy the tapes after learning of such an accident even prior to litigation being commenced); *Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 286-87 (E.D. Va. 2004) (where plaintiff knew it was likely to bring litigation it could not create program with intent to destroy relevant evidence); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57, 61-62 (2003) (defendant put on reasonable notice of litigation, and duty to preserve triggered when dispute arose, and defendant's officer issued cure notice to plaintiff); *Applied Telematics, Inc. v. Sprint Communications*, No. 94-4603, 1996 U.S. Dist. LEXIS 14053, at *6 (E.D. Pa. Sept. 17, 1996) (duty to preserve arises when party possessing the evidence has notice of relevance; this may be triggered as soon as complaint is served,

¹ Some courts and commentators refer to "reasonably anticipated litigation" as "threatened" litigation. The terminology employed is not as important as the concept: there must be some specific set of facts and circumstances that would lead to a conclusion that litigation is imminent or should otherwise be expected. The mere fact that litigation regarding a topic (such as a product or a contract) is a general possibility is ordinarily not enough to trigger preservation obligations.

but certainly arises once discovery request has been propounded); *Lombardo v. Broadway Stores, Inc.*, Case No. G0 26 581, 2002 WL 86810, at *9-10 (Cal. Ct. App. 4 Dist. Jan. 22, 2002) (breach of duty to preserve occurred when defendant permitted destruction of electronic evidence after commencement of class action suit and plaintiff had twice requested that defendant preserve relevant data in the months prior to litigation); *cf. Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003) (“*Zubulake IV*”) (in employment discrimination case, duty to preserve attached as soon as plaintiff’s supervisors became reasonably aware of the possibility of litigation, rather than when EEOC complaint was filed several months later). *But compare Morris v. Union Pac. R.R.*, 373 F.3d 896 at 900-901 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper, distinguishing facts in *Stevenson*).

The analysis of the need for a “legal hold” is usually done by the legal department, but it may involve other departments as there may be a wide variety of reasons to institute hold orders (such as financial audits, compliance and litigation matters). A recommended practice is for the legal department to have a separate checklist of circumstances by which it considers whether a preservation obligation has been triggered and, if so, what steps need to be taken to identify the scope of the obligation and what has to be done to meet the obligation. The exact manner in which this is done may vary as long as there is a process by which circumstances can be evaluated to determine if there needs to be a suspension of ordinary destruction practices.

Comment 5.c.

An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

Organizations need to identify a chain of command to decide when normal records retention procedures should be suspended. Ideally, organizations can identify in advance one or more “point” persons responsible for managing this process. Contact information should be easily accessible to employees.

An organization’s information and records management policy should provide specific direction concerning hold notices. This generally includes: (1) who has the authority to impose a legal hold on records otherwise scheduled for disposition; (2) who is responsible for communicating the legal hold requirements; (3) who is responsible for implementation; and (4) who has authority to determine that the need for a legal hold no longer exists. The policy could also provide a typical form of notice and channels for communicating when it is necessary to suspend the normal course of records retention and destruction. Of course, the content of the notice will vary depending on the particular circumstances. *See* Comment 5.e-f, *infra*.

Comment 5.d.

An organization’s information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.

Once a duty to preserve is triggered and a legal hold is required, the organization needs to take steps to implement the hold. The procedures if set forth in the policy can help clarify the requirements for a reasonably diligent search to identify, locate, collect and appropriately handle relevant documents when notice is received of actual or reasonably anticipated litigation, governmental investigation or audit. For all the reasons identified in describing why a multidisciplinary team may be important to the successful launch of a retention program, *see* Comment 1.b, *supra*, an effective litigation response team may often include persons in the organization responsible for oversight and

administration of the information and records management policy, representatives from the legal department (preferably with some litigation experience), representatives of the IT department, other senior level managers or executives as may be appropriate to the matter or case, as well as sufficient staff to implement the response.

Litigation response issues the organization may wish to address include:

- How are potentially responsive records and other information identified?
- Who is involved in the identification?
- Who will be contacted?
- Where and how will records and other information subject to the legal hold be stored?
- Who collects and coordinates the retention of the records and other information subject to the legal hold?
- Whether and how to regularize and document the team process?
- What metadata, if any, may be material to a particular dispute and thus may need to be preserved?
- Whether records and other information must be “frozen” in a snapshot?
- Whether “point-in-time” information needs to be preserved on an ongoing basis (future snapshots), and, if so, when and how will this be done?
- Is there a particular need to preserve legacy on backup media or systems?

Comment 5.e.

Legal holds and procedures should be appropriately tailored to the circumstances.

Any suspension of the normal course of information and records retention and destruction—or “legal hold”—should be informed by legal judgment, should be tailored to the legal requirements of the case, and should apply only to the life of the litigation, investigation, audit or other circumstance giving rise to the suspension.

The obligation to preserve evidence does not require that all electronic information be frozen. *See Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (organizations need not preserve “every shred of paper, every e-mail or electronic document, and every back-up tape”); *see also Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003) (“A party does not have to go to ‘extraordinary measures’ to preserve all potential evidence ... [i]t does not have to preserve every single scrap of paper in its business.”) (citing *China Ocean Shipping (Group) Co. v. Simone Metals Inc.*, No. 97 C 2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999)) and *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *32 (N.D. Ill. Oct. 20, 2000). The scope of what is necessary to preserve will vary widely between and even within organizations depending on the nature of the claims and the information at issue. *See Zubulake*, 220 F.R.D. at 218 (“In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task [of retaining relevant documents] is accomplished.”); *see also The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production*, Principle No. 5 (Jan. 2004).

The legal hold must cover relevant electronic information and records, and the legal hold notice should specifically state that relevant electronic information and records must be preserved. *See The*

Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production, Principle No. 5 at 20 (Jan. 2004). In the civil litigation discovery context, the obligation to preserve and produce relevant evidence is generally understood to require that the producing party exert only reasonable efforts to identify and manage the relevant information readily available to it. See *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) (describing how contours of preservation obligation are defined); *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 532 (1st Cir. 1996) (“In determining whether material is ‘discoverable,’ the court should consider not only whether the material actually exists, but the burdens and expenses entailed in obtaining the material.”); MANUAL FOR COMPLEX LITIGATION, § 21.446 (4th ed.) (“For the most part, [computerized] data will reflect information generated and maintained in the ordinary course of business.”).

In particular circumstances, implementing a legal hold may also require a change to the organization’s backup procedures for business continuation or disaster recovery. A legal hold should address what actions, if any, are to be taken to suspend recycling of disaster recovery backup tapes, either on a temporary or ongoing basis, pending further litigation developments. Compare *Zubulake*, 220 F.R.D. at 218 (holding that “as a general rule” litigation holds do not apply to “inaccessible” backup tapes, *i.e.*, those maintained solely for purposes of disaster recovery, but distinguishing backups used for information retrieval that would be subject to such holds), with *Applied Telematics, Inc. v. Sprint Communications Co.*, No. 94-4603, 1996 WL 33405972, at *3 (E.D. Pa. Sept. 16, 1996) (holding defendant at fault “for not taking steps to prevent the routine deletion” of backup files); and *Keir v. UnumProvident Corp.*, No. 02 Civ. 878, 2003 WL 21997747, at *3 (S.D.N.Y. Aug. 22, 2003) (preservation obligations include backup tapes); see also *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, Comment 5.h (Jan. 2004).²

In certain circumstances, legal hold procedures may require the suspension of certain automatic deletion programs or processes that continuously delete information without intervention (such as e-mail janitor programs). Suspension may be necessary when the organization knows that the program or process will lead to the loss of relevant records or other relevant information that is not otherwise preserved or available. Of course, if adequate policies and procedures are in place to preserve relevant information, there may be no need to alter the standard operating practices of the business (such as e-mail janitor programs) in this regard.

Illustration i. Under its records management policy and procedures, a company requires that its employees limit the quantity of electronic information that is stored, or limit the time that communications that do not constitute records of the organization can remain, in the employees’ respective active e-mail accounts. Upon commencement of litigation, adequate steps are taken to inform the pertinent individuals to save relevant e-mail currently and in the future. The organization is not required to alter the policy, provided that the legal hold procedures are communicated and effective to preserve the relevant documents.

² When required to preserve backup tapes, an organization may elect to preserve a reasonable subset of previously created backup tapes (*i.e.*, keeping some combination of existing incremental, weekly or monthly backups), without in every case needing to indefinitely suspend the further recycling of backups. See *Zubulake*, 220 F.R.D. at 218 (“[i]f a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of ‘key players’ to the existing or threatened litigation should be preserved” if the information is not otherwise available).

For examples of discussions of the various legal hold or preservation “scope” issues that have been identified in the case law, see *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631-32 (D. Utah 1998) (although no discovery order was yet in place, defendant was sanctioned for refusing to preserve corporate e-mails of five individuals it itself had identified as having information relevant to the pending litigation), *reversed in part by Proctor & Gamble Co. v. Hauger*, 222 F.3d 1262 (10th Cir. 2000); *Concord Boat Corp. v. Brunswick Corp.*, Case No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (corporation fulfilled duty to preserve by retaining relevant e-mails subsequent to the filing of the complaint even though pre-litigation e-mails were destroyed: “to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail”; such a holding, the court found, would be crippling to large corporations, which are often involved in litigation); *Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892, 922-24 (1995) (no duty to preserve documents relating to design of tractor that had been out of production for 20 years and where there were no known claims as to which the documents might be relevant; wrongfulness of evidence destruction is tied to temporal proximity between destruction and litigation interference, and foreseeability of harm to the non-spoiling litigant), *overruled on other grounds by Cedars-Sinai Med. Ctr. v. Superior Court*, 18 Cal. 4th 1, 74 Cal. Rpt. 2d 248, 954 P.2d 511 (1998).; *Moore v. Gen. Motors Corp.*, 558 S.W.2d 720, 735-37 (Mo. Ct. App. 1977) (declining to find spoliation where records were destroyed in accord with policy to destroy at end of model year and with no knowledge of pending litigation, there was no evidence manifesting fraud, deceit or bad faith, and plaintiff had made no effort to obtain through discovery once suit began); see also *Kucala Enterprises, Ltd. v. Auto Wax Co.*, No. 02C1403, 2003 WL 21230605, at *8 (N.D. Ill. May 27, 2003) (magistrate recommended that plaintiff’s suit be dismissed and attorneys’ fees awarded to defendant when court found that plaintiff had flagrantly violated duty to preserve by installing a software program designed to cleanse a hard drive of evidence; plaintiff’s fear that defendant would not adhere to protective order was not justifiable and did not excuse duty to preserve); *McGuire v. Acufex Microsurgical, Inc.*, 175 F.R.D. 149, 153-56 (D. Mass. 1997) (no obligation to preserve all drafts of internal memos and no sanctionable conduct in deleting paragraph from personnel evaluation—even after state discrimination commission proceedings commenced; court found that employer had obligation to make sure that no false information was placed into personnel file; employer could review drafts of personnel memoranda and discard them when the editing related to obvious errors made by other than the accused harasser, and modified memorandum was promptly produced when it was later found on the home computer of the original author).

Comment 5.f.

Effectively communicating notice of a legal hold should be an essential component of an organization’s information and records management program.

Once events occur requiring that a legal hold be imposed, court decisions make clear that the notice should be communicated to appropriate custodians of affected records and individuals who may have other relevant information. Courts have identified the following factors as significant, so an organization imposing a legal hold should evaluate:

- ***The person providing the notice.*** Courts have repeatedly stated that document retention issues are significant matters for corporations and organizations and there must be sufficient attention and resources devoted to meeting preservation duties in light of the circumstances. See *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *39-41 (N.D. Ill. Oct. 20, 2000). In large organizations with thousands of employees, it should be sufficient that the notice come from senior representatives of the

legal department or some other department charged with the responsibility for preserving records for the organization. *Cf. In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 612, 615-16 (D.N.J. 1997) (found that defendants' earlier preservation hold notices were inadequate and required senior management to advise employees of the pending litigation, provide them with a copy of the court order and inform them of their potential civil or criminal liability for noncompliance).

- ***The contents or scope of the notice.*** The notice need not be, and most likely should not be, a detailed catalog of documents to be retained, but instead can provide a sufficient description of the subject matter of the documents to be preserved that would allow the affected document custodians to segregate and preserve identified information and records. *See Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *5 (N.D. Ill. Oct. 27, 2003) (Initial notice sent to employees to preserve documents only pertaining to the one named plaintiff in a putative class action addressing employment issues was insufficient as it did not properly reflect scope of preservation obligation; broader revised notice was sufficient).³
- ***The means and extent of communicating the records hold.*** The notice does not need to reach all employees in the organization, only those necessary to preserve relevant information and records. The communication need not be disseminated beyond the scope of reasonable inquiry absent specific information and knowledge that requires otherwise. The notice should be communicated through means likely to reach the intended audience, and may include electronic and/or paper distribution. *See In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 612-13 (D.N.J. 1997) (noting that e-mails sent to employees did not contain bolded phrases like "DO NOT DESTROY DOCUMENTS," that the e-mails did not mention the specific pending litigation or the possibility that failure to comply could give rise to civil or criminal penalties, that not all employees had e-mail access to receive the e-mails sent, and that not all notices were circulated in paper format as well as electronic).

Illustration ii. Under its policy, a potential producing party enlists the assistance of its employees or agents who are identified as possibly having relevant information by informing them of the nature of the controversy and the time frame involved, and by providing them with a method of accumulating and updating (where disputes are ongoing) copies of the relevant information. The appropriate individuals are instructed to preserve relevant information for the duration of the controversy and steps are established to follow up with the identified individuals and secure the information. The organization has likely fulfilled its obligations.

- ***Whether notice should be sent to third parties.*** Consideration should be given to sending the notice of the legal hold to third parties if such third parties possess documents or data that effectively are in the possession, custody or control of the producing party.

³ This aspect of the *Wiginton* case is troubling for it uses a subsequent remedial measure (a more precise preservation notice) as evidence that the first notice was insufficient. *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *5 (N.D. Ill. Oct. 27, 2003).

- **Updated notices.** Consideration should be given as to whether notices of the legal hold should be updated as the litigation proceeds (*e.g.*, where new parties or claims are added or eliminated). Care must be given, however, to ensure appropriate consistent direction among all preservation notices. In certain circumstances, organizations may want to consider repeating notices or periodic general reminders that employees need to adhere to previously issued legal holds. *Cf. Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2004 WL 1620866, at *9 (S.D.N.Y. July 20, 2004) (recommending periodic re-issuing of litigation hold notices).

Comment 5.g.

Documenting the steps taken to implement a legal hold may be beneficial.

Organizations should consider ways in which the legal hold process—either generally or in a given case—is recorded. This should usually include a copy of any legal hold notice(s) that have been issued, and a distribution list for the notice(s). Some organizations may wish to create checklists which outline the steps taken from the point of notice through the decision to release a legal hold. Such documents may assist in the development of affidavits or testimony which might be required should the preservation process be challenged. Some organizations require employees to certify receipt of, and compliance with, legal hold instructions. Other organizations rely on the legal hold notice combined with other steps, such as witness interviews, to ensure appropriate preservation steps have been taken. Regardless of the steps taken, a record of compliance can be very useful in defending any challenges to the organization's good faith efforts to meet its preservation obligations. *Cf. Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2004 WL 1620866, at *9-10 (S.D.N.Y. July 20, 2004) (noting roles of counsel and client in implementing legal hold notices and procedures).

Although documenting preservation efforts is a recommended practice, there is no legal requirement mandating the creation of such a "paper trail." Likewise, the absence of such documentation in a particular instance or organization should not be viewed as evidence that the organization did not act in good faith or that its efforts were not sufficient to meet its legal obligations.

Comment 5.h.

If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

As noted elsewhere, courts have imposed severe sanctions on organizations that have been found to have allowed the spoliation of evidence by either reckless or intentional conduct attributed to the organization. *See Kucala Enters., Ltd. v. Auto Wax Co.*, No. 02C1403, 2003 WL 21230605, at *8 (N.D. Ill. May 27, 2003). Some courts have stated that negligent conduct may be sufficient to warrant sanctions in certain circumstances. *See Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2nd Cir. 2002). These courts have not, however, explicitly described how a party's good faith and reasonable efforts to implement legal hold procedures may insulate it from liability for the spoliation of evidence by employees who have failed to follow the organization's policies and directives.

The recognition of the availability of a "safe harbor" against culpability in such circumstances is essential. As is abundantly clear from the body of this document, the nature and volume of electronic documents is such that there is no possibility that any preservation system can be perfect. *See Comment 1.b, supra, see also Zubulake v. UBS Warburg LLC ("Zubulake IV")*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.'")

Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation.”); *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4, *7 (N.D. Ill. Oct. 27, 2003) (Organization “does not have to preserve every single scrap of paper in its business”; “CBRE did not have the duty to preserve every single piece of electronic data in the entire company”). In addition, economic incentives for the creation of reasonable and effective litigation hold procedures will be eroded if there is no benefit absent a guarantee that the process will be perfect.

Consistent with the legal authority examined in this document, although no court has expressly so ruled, the authors believe that if an organization takes reasonable and appropriate steps to ensure that relevant information is preserved, but an employee engages in conduct inconsistent with the organization’s directions (express and implied), it *may* be appropriate to hold the individual, but not the organization, responsible provided that the organization can demonstrate it applied and enforced its policy and did not condone or adopt the actions of the employee. At a minimum, if the organization took reasonable steps in good faith to preserve evidence, the organization will, typically, not be held accountable for “willful” spoliation, which carries with it the most severe penalties. Courts should examine the specific facts and circumstances of each case before determining that an organization should be held responsible for spoliation despite the implementation in good faith of a demonstrable and reasonable “legal hold” process.

Comment 5.i.

Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

An organization’s policy and procedures can explain not only who in the organization has authority for determining that the need for a legal hold no longer exists, but also what factors or information should be considered, and what procedures should be followed, to remove the legal hold.

Considerations may include:

- The form and content of notice that the legal hold has been lifted;
- Whether there is a post-case obligation to maintain some records or other information pursuant to normal retention schedules or otherwise;
- Whether the records or other information that can now be destroyed, are subject to another legal hold, or may be needed for another special purpose (*e.g.*, needed in whole or in part for other litigation);
- Whether records or information in third-party custody can be destroyed; and
- Whether the records or other information can be disposed of as soon as the legal hold is lifted, or whether the organization should wait until the next scheduled disposition.

Appendix A: Standards

The following entries constitute a selected list of organizational Web sites providing information on international, national, and state government standards relevant to electronic records, with citations to specific standards where applicable. The list does not purport to be comprehensive; in many cases, the Web sites themselves operate as portals to much richer array of information located on the Web. The entries below contain a current direct link pointing to the “standards” information on the Web site; however, given the frequency of Web page updates and the possibility of broken links to sub-URLs, a home page also has been provided for each main organization. Short descriptions for the listed organizations have been mostly taken verbatim from the Web sites themselves.

1. **AIIM International (Enterprise Content Management Association)**

- <http://www.aiim.org>
- <http://www.aiim.org/standards.asp?ID=24488>

AIIM Standards is comprised of twenty-plus committees and working groups. Over 80 of AIIM's standards, recommended practices and technical reports have been drafted and approved by ANSI.

AIIM holds the secretariat for ISO/TC 171 SC2, Document Imaging Applications, Application Issues. AIIM is also the administrator for the U. S. Technical Advisory Group (TAG) to ISO TC 171, Document Imaging Applications that represents the United States at international meetings.

2. **American National Standards Institute (ANSI)**

- <http://www.ansi.org>
- http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3

ANSI is a private, non-profit organization (501(c)(3)) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

- ANSI/AIIM TR31, Performance Guideline for the Legal Acceptance of Records Produced by Information Technology

3. **ARMA (The Association for Information Management Professionals)**

- <http://www.arma.org>
- <http://www.arma.org/standards/index.cfm>

Standards development is a major activity for ARMA International at both the national and international levels. ARMA is an accredited standards development organization with the American National Standards Institute (ANSI). ARMA also participates in

applicable ISO standards development committees such as TC 46/SC 11 Archives/Records Management.

4. Cohasset Associates, Inc.

- <http://www.cohasset.com>
- http://www.merresource.com/library/index.php?dir=policies_and_guidelines

Cohasset is a private consulting firm specializing in document-based information management, and is host to the Managing Electronic Records (MER) Conferences.

5. Committee on Institutional Cooperation (CIC), University Archivists Group (UAG)

- <http://www-personal.umich.edu/%7Eederomedi/CIC/cic.htm>

This website sets out CIC UAG Standards for an Electronic Records Policy.

6. The Document Site

- <http://www.thedocumentsite.co.uk>
- http://www.thedocumentsite.co.uk/RM_resources.html

The site is published and maintained by Reynold Leming, Managing Director of Mint Business Solutions Ltd., an information management consultancy.

7. Electronic Media Group

- <http://aic.stanford.edu/sg/emg/>

The mission of the Electronic Media Group (EMG) is two-fold: (1) preservation of electronic art, electronic-based cultural materials and tools of creation; and (2) to provide a means for conservators and related professionals to develop and maintain knowledge of relevant new media and emerging technologies.

- <http://info.wgbh.org/upf/> (Universal Preservation Format)

8. Electronic Resource Preservation and Access Network (ERPANET)

- <http://www.erpanet.org>

The European Commission—funded ERPANET Project will establish an expandable European Consortium, which will make viable and visible information, best practice and skills development in the area of digital preservation of cultural heritage and scientific objects. ERPANET will provide a virtual clearinghouse and knowledge base on state-of-the-art developments in digital preservation and the transfer of that expertise among individuals and institutions.

9. IEEE Computer Society

- <http://www.computer.org>
- <http://www.computer.org/standards>

With nearly 100,000 members, the IEEE Computer Society is the world's leading organization of computer professionals. Founded in 1946, it is the largest of the 37 societies of the Institute of Electrical and Electronics Engineers (IEEE).

The Society is dedicated to advancing the theory, practice, and application of computer and information processing technology.

10. Indiana University Bloomington Libraries, University Archives

- <http://www.indiana.edu/%7Elibarch/ER>

Website includes citations to white papers and standards on methodologies for designing record-keeping systems, evaluating information systems as record-keeping systems, functional requirements for record-keeping systems, record-keeping metadata specifications, and records policies and guidelines.

11. International Council on Archives

- <http://www.ica.org>

The International Council on Archives (ICA) is a decentralized organization governed by a General Assembly and administered by an Executive Committee. Its branches provide archivists with a regional forum in all parts of the world (except North America); its sections bring together archivists and archival institutions interested in particular areas of professional interest; its committees and working groups engage experts to solve specific problems. The ICA Secretariat serves the administrative needs of the organization and maintains relations between members and cooperation with related bodies and other international organizations.

- <http://www.ica.org/biblio.php?pbodycode=CER&ppubtype=pub&plangue=eng>
ICA Committee on Current Records in Electronic Environments
- <http://www.ica.org/biblio.php?pbodycode=CDS&ppubtype=pub&plangue=eng>
ICA Committee on Descriptive Standards

12. International Organization for Standardization

- <http://www.iso.org>
- <http://www.iso.org/iso/en/ISOOnline.openerpage>

A network of national standards institutes from 148 countries working in partnership with international organizations, governments, industry, business and consumer representatives. The source of ISO 9000, ISO 14000 and more than 14,000 International Standards for business, government and society.

- ISO 15489-1 and 2:2001(E), International Standard: Information and Documentation – Records Management

13. International Research on Permanent Authentic Records in Electronic Systems (InterPARES Project)

- <http://www.interpares.org>
- <http://www.interpares.org/links.htm>

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) aims at developing the theoretical and methodological knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form. This knowledge should provide the basis from which to formulate model policies, strategies and standards capable of ensuring the longevity of such material and the ability of its users to trust its authenticity.

14. MoReq (“Model Requirements”) Project

- <http://www.cornwell.co.uk/moreq> or http://www.inform-consult.com/services_moreq.asp; also (additional information about MoReq and its place relative to other efforts; from AIIM Europe) <http://www.arkivochdokument.se/library/2003/Konf%20F%20Records%20Management%20-%20About%20MOREQ%20and%20DLM%20-%20Roger%20Crumpton.pdf>

An EEC model records management requirement and specification.

15. Monash University, Australia, School of Information Management and Systems

- <http://www.sims.monash.edu.au/index.html>
- <http://www.sims.monash.edu.au/research/rcrg/links.html>

The mission of the School of Information Management and Systems is to advance through teaching, research and community engagement, the organization, application, management and use of information and information technology, and to enhance our understanding of the impact of information on individuals, organizations, institutions, and society.

16. NAGARA (National Association of Government Archives and Records Administrators)

- <http://www.nagara.org>
- <http://www.nagara.org/links.html>

NAGARA is a professional organization dedicated to the effective use and management of government information and publicly recognizing their efforts and accomplishments.

17. National Archives (United Kingdom)

- <http://www.nationalarchives.gov.uk>
- <http://www.nationalarchives.gov.uk/electronicrecords/advice/default.htm>
Standards on the development and best practices for e-records management systems, includes toolkits and suggestions for developing corporate policies and inventory systems.
- <http://www.nationalarchives.gov.uk/electronicrecords>

18. National Archives of Australia

- <http://www.naa.gov.au>
- <http://www.naa.gov.au/recordkeeping/rkpubs/summary.html> (links to record-keeping publications)

19. New South Wales State Records

- <http://www.records.nsw.gov.au/publicsector/erk/electronic.htm> (electronic record-keeping)

20. OASIS

- <http://www.oasis-open.org/home/index.php>
Non-profit consortium coordinating development of e-business standards; parent organization for LegalXML.

21. Open Archives Initiative

- <http://www.openarchives.org/index.html>
- http://www.oaforum.org/oaf_db/list_db/list_protocols.php

The Open Archives Initiative develops and promotes interoperability standards that aim to facilitate the efficient dissemination of content. The Open Archives Initiative has its roots in an effort to enhance access to e-print archives as a means of increasing the availability of scholarly communication.

22. Research Libraries Group

- <http://www.rlg.org>
- http://www.rlg.org/en/page.php?Page_ID=553

Current Projects, including Encoded Archival Context Activities and Encoded Archival Description activities.

The Research Libraries Group (RLG) is an international consortium of universities and colleges, national libraries, archives, historical societies, museums, independent research collections and public libraries. Its mission is to “improve access to information that

supports research and learning” through collaborative activities and services that include organizing and preserving as well as sharing information resources.

23. Society of American Archivists

- <http://www.archivists.org>
- http://www.archivists.org/governance/handbook/standards_com.asp (Standards Committee)

The Standards Committee is responsible for overseeing the process of developing, implementing, and reviewing standards pertinent to archival practice and to the archival profession and for providing for effective interaction with other standards-developing organizations whose work affects archival practice.

- <http://www.archivists.org/catalog/stds99/index.html> (Standards for Archival Description Handbook)
- <http://www.archivists.org/assoc-orgs/index.asp> (links to related associations)
- <http://www.loc.gov/ead> (Encoded Archival Description website)
- <http://www.archivists.org/saagroups/ers/index.asp> (Electronic Records section)

24. State University of New York, Albany, Center for Technology in Government

- <http://demo.ctg.albany.edu/projects/mfa>

The Center for Technology in Government works with governments to develop information strategies that foster innovation and enhance the quality and coordination of public services, carrying out this mission through applied research and partnership projects that address the policy, management and technology dimensions of information use in the public sector. Website contains references to publications concerning functional requirements for electronic record-keeping.

25. University of Michigan/University of Leeds, CAMiLEON Project

- <http://www.si.umich.edu/CAMILEON/index.html>

The CAMiLEON Project is developing and evaluating a range of technical strategies for the long term preservation of digital materials. User evaluation studies and a preservation cost analysis are providing answers as to when and where these strategies will be used. The project is a joint undertaking between the Universities of Michigan (USA) and Leeds (UK) and is funded by JISC and NSF.

26. University of Pittsburgh, School of Information Sciences

- <http://www.archimuse.com/papers/nhprc/meta96.html>

Metadata specifications derived from functional requirements: reference model for business acceptable communications.

27. University of Virginia Library and Cornell University Fedora Project

- <http://www.fedora.info>

The Fedora project was funded by the Andrew W. Mellon Foundation to build an open-source digital object repository management system based on the Flexible Extensible Digital Object and Repository Architecture (Fedora). The new system demonstrates how distributed digital library architecture can be deployed using web-based technologies, including XML and Web services. Fedora was jointly developed by the University of Virginia and Cornell University.

28. U.S. Department of Agriculture, Records Management

- <http://www.ocio.usda.gov/irm/records>
Comprehensive web site with links to federal resources.

29. U.S. Department of Defense, 5015.2 Standard

- <http://www.dtic.mil/whs/directives/corres/html/50152std.htm>
Design Criteria Standard for Electronic Records Management Software Applications (June 2002). This Standard is issued under the authority of DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000, which provides implementing and procedural guidance on the management of records in the Department of Defense. This Standard sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by DoD Components in the implementation of their records management programs; defines required system interfaces and search criteria to be supported by the RMAs; and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations.
- <http://jitic.fhu.disa.mil/recmgt/standards.htm>.
"Functional baseline requirements" study that provides additional requirements and data element descriptions for records management metadata.

30. U.S. Environmental Protection Agency (Records Management Website)

- <http://www.epa.gov/records/policy/index.htm> (contains links to additional sites)

31. U.S. Library of Congress, Metadata Encoding & Transmission Standard (METS)

- <http://www.loc.gov/standards/mets>
The METS schema is a standard for encoding descriptive, administrative, and structural metadata regarding objects within a digital library, expressed using the XML schema language of the World Wide Web Consortium. The standard is maintained in the Network Development and MARC Standards Office of the Library of Congress, and is being developed as an initiative of the Digital Library Federation.

32. U.S. National Aeronautics and Space Administration, Science Office of Standards and Technology

- <http://ssdoo.gsfc.nasa.gov/nost>
- <http://ssdoo.gsfc.nasa.gov/nost/isoas>

Summarizing U.S. efforts towards ISO archiving standards.

33. U.S. National Archives and Records Administration

- <http://www.archives.gov>
- http://www.archives.gov/records_management
- http://www.archives.gov/records_management/initiatives/transfer_to_nara.html

Expanding Acceptable Transfer Requirements: Transfer Instructions for Permanent Records

34. U.S. National Institute of Standards and Technology (NIST)

- <http://www.nist.gov>
- <http://www.itl.nist.gov/iaui>

The Information Access Division (IAD), part of NIST's [Information Technology Laboratory](#), provides measurements and standards to advance technologies dealing with access to multimedia and other complex information.

- <http://www.itl.nist.gov>

The Information Technology Laboratory (ITL) works with industry, research, and government organizations to make this technology more usable, more secure, more scalable, and more interoperable than it is today. We develop the tests and test methods that both the developers and the users of the technology need to objectively measure, compare and improve their systems.

35. Utah Division of State Archives

- <http://archives.utah.gov/recmanag/electronic.htm>

(Comprehensive web site listing electronic record-keeping related resources including from all 50 states)

36. World Wide Web Consortium (W3C)

- <http://www.w3c.org>
- <http://www.w3c.org/RDF> (Resource Description Framework)
- <http://www.w3c.org/Consortium/Activities>

The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication, and collective understanding.

37. XML.ORG

- <http://www.xml.org>

XML standards for specific industry areas.

Appendix B: Cobasset Survey Results

Summary of Cobasset Associates' 2003 Survey of Records Management Professionals

(Co-sponsored by ARMA International and AIM International)

Dramatic records-related events have played out in boardrooms, courts and the media in the last several years focusing the attention of lawmakers, lawyers, regulators, auditors and investors on one critical aspect of business—the management of information and records. This awakening regarding the intrinsic value of information assets has created an urgent need to refocus on the processes by which business records are managed, particularly those that are produced and stored electronically.

The impetus for the Sedona Guidelines originated primarily within the legal community, but studies and surveys related to information and records management topics spearheaded by those in the records management and information technology industries were an important part of corporate consciousness-raising. The survey summarized in this Appendix, while not a catalyst for the development of the Sedona Guidelines, highlights why organizations should consider the Guidelines' recommendations to improve the management of electronic information and records.

Three leading United States organizations in the field of records and information management teamed together in the fall of 2003 to assess the current state of electronic records management. This assessment was sponsored by ARMA and AIIM International which together enlisted the services of Cobasset Associates, Inc., to conduct a focused survey of key elements of the status quo of electronic records management. Respondents were more than 2,200 members of ARMA and AIIM and subscribers to the Records Management LISTSERV.

The 2003 survey was comprised of 22 close-ended, issue-based questions. To optimize measurement of trends over time, most of the questions were identical or very similar to the questions in two similar surveys conducted in 1999 and 2001 by Cobasset Associates.

Significant challenges and numerous shortfalls in the governance of business records management processes are shown in the survey findings and the trends over time:

- In comparing the data from 1999-2003, a weighted average of 86% of the respondents indicated they have a formal records management program, but those evaluating the program as “marginal” or “fair”—the lowest categories—grew from 31% in 1999 to 41% in 2003.
- 93% of the respondents responded that they believe that the process by which electronic records are managed will be either “very important” (57%), “quite important” (20%) or “important” (16%) in future litigation.
- Only 59% of the respondents stated that electronic records were included in their organization's current records management program (similarly in a separate question 40% reported their records management policies and procedures do not address electronic records), and this number did not change significantly from 1999.

- Nearly half of the respondents (47%) stated that their organizations do not have comprehensive records retention schedules that include electronic records.
- Nearly 40% of the respondents reported that the organization follows its records retention schedule “not regularly” (26%) or “only when time permits” (12%); however, the number of respondents who reported that their organization “always” follows the schedule did increase from 7% in 1999 to 17% in 2003.
- Only 54% of the 2003 survey respondents stated their organizations had a discovery request response plan and the same percentage reported their organizations have a formal system for records hold orders; 65% reported that their organization’s system for records hold orders did not include electronic records.
- Some 62% of the respondents were less than confident—either “not confident at all” (33%) or just “slightly confident” (29%)—that their business organization could successfully demonstrate that its records were accurate, reliable and trustworthy many years after they were created.
- 70% of respondents indicated that their organizations do not have any policies or procedures in place to migrate their electronic records over time.

The complete survey results are reported in “Electronic Records Management Survey: A Call to Action” which is available at <http://www.merresource.com/whitepapers/survey.htm>.

Appendix C:

Survey of Data Within an Organization

An organization's information and records management policy should be based on an accurate and complete understanding of the sources and types of *electronic* records generated, received and used within the organization, as well as an overall assessment of the practices in place regarding the use, retention, storage, preservation and destruction of records generally. During this assessment, the organization should review its current records program: how records are created and maintained; how records disposition decisions are made and implemented; and how records critical to the organization are protected.

Specifically, the organization should plan to gather information on its:

- Size, structure, locations, industry;
- Regulatory requirements for record-keeping;
- Current records management policies and procedures;
- Information systems infrastructure; and
- Methods for ensuring compliance with policies and procedures.

Many models for such record-keeping surveys exist, but no one template can be taken as a talisman for every organization. This Appendix provides a sample that can be used as a starting point by organizations addressing records management issues, with particular emphasis on electronic information. Note, however, that this survey is not exhaustive and that an organization should consult with individuals equipped to assist in a comprehensive review of records management programs and policies. Other samples that may also be useful as a guide in creating a customized assessment tool include:

- National Archives and Records Administration (NARA)'s Records Management Self-Evaluation Guide, *available at* http://www.archives.gov/records_management/publications/records_management_self_evaluation_guide.html#intro
- National Archives of Australia's Record-keeping Policy Checklist, *available at* <http://www.naa.gov.au/recordkeeping/overview/policy/check.html>
- The Center for Technology in Government's The Records Requirements Analysis and Implementation Tool, *available at* <http://www.ctg.albany.edu/publications/guides/rrait>

For organizations that wish to assess their records management, particularly in comparison to the requirements in ISO 15489-1, ARMA International has developed an online assessment tool. It is a high level (rather than in-depth) assessment, but will be valuable in the initial stages of program assessment or development. More information on this assessment product (RIM e-Assessment) can be found on the ARMA website (www.arma.org/standards).

I. Written Policies

- A. Obtain and review any existing records management policies and directives for all media (paper and electronic).
 - 1. Evaluate policy(ies)
 - a. Is it written?
 - b. Is it contained in a single document?
 - c. Is it clear?
 - d. Is it well distributed and easily accessible?
 - 2. What is the scope of the policy?
 - a. Does it apply to all kinds of information? (*i.e.*, paper, e-mail, word processing documents, spreadsheets, databases)
 - b. Does it apply globally?
 - c. Does it apply to subsidiaries and affiliates?
 - d. Does it apply to records in the possession of contractors, outside counsel, etc.?

II. Identify business needs and regulatory and legal responsibilities

- A. What is the company's:
 - 1. size? (number of employees)
 - 2. structure? (public or private; parent/subsidiary/sister co.)
 - 3. locations? (national and international)
 - 4. industry?
 - 5. products / services?
 - 6. perceived core business functions?
- B. Determine operational and regulatory factors
 - 1. What are the business or legal considerations that drive record-keeping?
 - 2. How does the nature of the business affect the creation and management of information that is vital to business functions?
 - 3. How does the industry in which the business operates affect the kind of information that the business must retain for legal reasons?
 - 4. Does the company belong to any industry or trade organizations, or have another designation, which imposes certain guidelines, standards or requirements?
 - 5. Does the company's specific structure, needs, legal duties or other considerations require that document management policies for electronic records be distinguished from those used for paper records?

- C. Obtain and review any existing records retention schedules
 - 1. Who has authority to create or modify schedules?
 - 2. What is the process for creating or modifying schedules?
 - 3. How are the schedules organized (by business, by function, by topic, etc.)?
 - 4. Do the retention schedules distinguish certain types of documents as “records” and other types of documents as not “records”?
 - 5. Do the retention schedules apply regardless of storage medium? (paper, electronic, microfilm, CD, file server, etc.)
 - 6. Are there “conditional” retention schedules (*i.e.*, triggered by a future event?) “Life of system” or “3 years after termination of employment” are examples.)
 - 7. If an employee is uncertain what retention category applies to a record, what is the mechanism to provide an answer?
 - 8. Has the organization addressed the retention of e-mail messages, voice mail message, instant messages and other electronic communication tools?
 - 9. Are retention times binding policy, recommendations, guidance, etc.?
 - 10. If the retention times are mandatory, how is compliance verified? (Audits? Written certification? Other?)
 - 11. How does the organization publish or otherwise document retention schedules?
 - 12. How does the organization communicate schedules to non-U.S. employees?
 - 13. If the schedules apply globally, how does the organization deal with local requirements?

III. Review how the organization implements retention policy

- A. Does the organization provide guidance on:
 - 1. What records are to be created.
 - 2. What format should be used to capture “original” records, status of drafts, working papers and reference copies of records.
- B. Evaluate how the organization currently manages the disposal of records
 - 1. Determine to what extent the organization relies on each individual to dispose of electronic records?
 - 2. How does the organization educate employees about document retention/disposition responsibilities?
 - 3. How does disposition occur?
 - 4. What “disposal” methods are authorized or required? Is there a difference between paper and electronic?

5. When is information considered “destroyed” within the organization?
 - a. When the “delete” button is pushed (*i.e.*, free space pointers are adjusted)
 - b. When the media has been overwritten? (how many times?)
 - c. When the media have been physically destroyed?
 - d. When backups have been overwritten? (how many times?)
 - e. When an audit log or similar mechanism has been checked, and all copies have been destroyed?
- C. Determine if records are being preserved for the required retention period
 1. How does the organization ensure that records will remain accessible, readable, and usable throughout their scheduled retention?
 2. When records are copied from one medium to another (such as scanning paper records onto optical disk, or microfilming), does the organization retain the originals?
 3. Are there appropriate controls in place to address the:
 - a. life span of the storage medium (*e.g.*, disk or tape decays over time)?
 - b. obsolescence of software (*e.g.*, moving to a new word processing program)?
 - c. obsolescence of hardware (*e.g.*, mainframe systems)?
 - d. obsolescence of the storage medium (*e.g.*, 5.25” disks)?
 - e. backup tapes from a records retention perspective?

IV. Evaluate the organization’s ability to effectively manage records over their entire lifecycle

- A. Estimate records volume
 1. Is the volume of paper records increasing, decreasing or stable?
 2. What is the volume of electronic records on the company’s systems?
 3. How is the volume of paper records managed? For example, does the organization use in-house storage centers, commercial third-party records storage facilities or other solutions? Is the same done with historical electronic records? If not, what is done?
- B. Evaluate the organization’s information services/technology (“IT”) function including:
 1. All hardware used for organization-wide systems (*i.e.*, mainframes, mini computers, e-mail servers, file servers, fax servers, voice-mail servers?)
 2. All operating systems (*e.g.*, Windows NT/2000/XP, Linux, Novell, Unix, proprietary?)

3. All desktop hardware and software, including:
 - a. office document programs (*e.g.*, word processing, spreadsheet programs)
 - b. internet browsers
 - c. electronic mail
 - d. calendar/scheduling
 - e. database management programs
 - f. industry-specific applications
 - g. finance or accounting systems
 - h. remote connection applications
 - i. instant mail or “chat” programs
4. All data storage locations available to users (*e.g.*, local hard drives, network drive locations, removable media, third-party storage locations)
5. All portable hardware and software (*e.g.*, notebook computers, PDA, etc.)
6. All “backup” systems (hardware and software)
 - a. For what purpose(s) does the organization keep backup tapes? (Disaster recovery? To restore individual accounts? As a means to ensure records retention? Other?)
 - b. How often are backups made? Are they complete backups or incremental?
 - c. What is the length of retention of back up tapes?
 - d. Does disposal occur immediately when the retention expires?
 - e. If the tape is simply released for reuse, is there a concern over the passage of time before reuse occurs?
 - f. Is the tape degaussed or otherwise erased as a whole, or simply released for reuse?
7. All electronic data archives
8. All network components and locations (*e.g.*, routers, hubs, firewalls, etc.)
9. All data storage locations outside of the United States
10. All third parties involved in data collection or storage on behalf of the organization
11. If the organization uses file servers, how does the organization assure compliance with retention schedules for:
 - a. the records on the server?
 - b. backup copies of the server?

12. Does the IT function take ownership of records compliance on file servers, or is this left to the users or others?
 13. Does the IT function know all the servers?
 14. Does the IT function know what types of records are on each server?
 15. If an employee places a record on a server (*e.g.*, a draft of a word processing document) and forgets about it, how is compliance with retention policies achieved?
 16. Is compliance with retention policies a mandatory deliverable for hardware and software?
 17. Identify the tools and automation employed by the organization to manage documents in general and records in particular (for example, Accutrac, iManage, Hummingbird, IBM)
 18. Does the organization have a formal electronic records management system?
 19. Has the organization implemented formal technology standards for records management? (ISO 15489, DoD 5015.2, ISO 17799)
 20. Does the organization employ automated assigning of metadata for content management or control issues to documents?
 21. Does the organization use technology to filter outbound content for loss of intellectual property (for example, Sybari for filtering outbound e-mail and attachments)?
 22. Does the organization deploy leveraged Digital Rights Management technology to enforce external parties copyright and license conditions?
 23. If a technology is adopted, and concerns regarding records management implications are identified later, what is the process to address those concerns?
- C. Review e-mail management procedures
1. Are employees allowed/encouraged to store e-mail messages for an extended period?
 2. If messages are stored, does the organization have any guidance on where to store them (*e.g.*, inbox versus personal folders or file server) and how to organize them?
 3. If the e-mail messages contain information which may be needed by others in the organization, how is this addressed?
- D. Identify the procedures used to the storage of confidential, privileged or other restricted access records
1. How does the organization categorize information according to sensitivity?
 2. What information security controls does the organization associate with various types of sensitive information?

3. To what extent is information labeling automated (for example, based upon metadata)?
 4. How does the organization control information that it does not own, but stores or processes on behalf of other entities?
 5. How does the organization control information that it owns, but does not store or process?
 6. What is the level of awareness and understanding of the organization's information classification and labeling controls among employees generally?
 7. What security controls does the organization require for various degrees of sensitive information?
 8. Are any levels of sensitive information prohibited from being stored electronically?
 9. From being transmitted over public networks?
 10. From being sent by facsimile?
 11. When is encryption required?
 12. Are there any guidelines regarding the use of cell phones or cordless phones for certain levels of sensitive information?
 13. What levels of sensitive information require restricted access to hardware?
 14. What levels of sensitive information require audit trails for access?
 15. What levels of sensitive information require special hardware?
- E. Understand policies or procedures in place to monitor or control the release of technical information outside the company
1. Review any employee training program regarding the release of proprietary information
 2. Are there processes to review, monitor or control putting confidential information into external e-mails?
 3. Are trade secrets classified in any special way?
 4. Is access to trade secret information limited or controlled in any way?
 5. Does the organization have a way to identify, track or limit the distribution of information that has third party obligations?
 6. Does the organization have a way to track and search for obligations listed in corporate secrecy or non-disclosure agreements?
 7. Does the organization use identity authentication technology (prompt for a specific person's name in a conference call, NetMeeting user identification, etc.)?

V. Evaluate the overall records program

- A. With regard to the current records management function, determine the following:
 - 1. How is it organized?
 - 2. How many employees are in the records management function?
 - 3. What other human resources are utilized?
 - 4. How long has it been in existence?
 - 5. Who is in charge?
 - 6. Is the records management function involved in decisions regarding the selection of emerging technologies and new hardware and software? (PDAs, blackberries, voice mail, instant messaging, e-mail systems, enterprise business systems, etc.)
- B. Evaluate the existing training/education of employees regarding records management
 - 1. How does the company educate, inform or train employees with respect to their responsibilities for records management?
 - 2. What is the current level of awareness of employees?
- C. Review records management compliance methods
 - 1. How does the organization encourage compliance with the records management program's policies and procedures?
 - 2. How does the organization verify compliance?
 - 3. How does the organization staff for compliance overseas?
 - 4. How does the organization verify compliance overseas?
- D. Review methods used to manage the records left by employee termination or transfer
 - 1. What is the process for ensuring compliance with records management policies or guidelines when an employee changes job/role or leaves employment with the company?
 - 2. Does this include electronic records such as e-mail, files on servers, etc.?
- E. Evaluate the organization's historical records audits practices
 - 1. Does the company have an audit program for records management?
 - 2. What are the purposes of the audits?
 - 3. What types of audits occur? (*e.g.*, individual offices? large paper or electronic systems? other?)
 - 4. Who conducts audits?
 - 5. How are the auditors trained?
 - 6. Approximately what is the volume of auditing that occurs?

- F. Evaluate how merger and acquisition (M&A) and divestiture activity have affected the records management program
 - 1. Does the M&A/divestiture transaction result in special agreements about retention?
 - 2. What is the normal expectation about retaining, or not retaining, the records of businesses or subsidiaries that the company divests?
 - 3. Are new subsidiaries or acquired entities expected to follow the records management program? How quickly?
 - 4. If records become “orphaned” as a result of M&A/divestiture activity (i.e., no owner can be identified, and the contents are unknown), what is the process to address this?

VI. Evaluate existing policies regarding litigation or investigations

- A. What is the role of the records management function in addressing litigation or investigations?
 - 1. How are documents identified and retrieved? Who is involved?
 - 2. Does the answer differ for paper versus electronic records?
 - 3. If records are located in a company-provided or off-site records storage facility, how are records sorted to identify individual documents that are needed for the litigation or investigation? By whom?
 - 4. When a case is closed, what records are retained and what records are disposed of?
 - 5. If some records are retained after the case is closed, how long are they retained?
 - 6. If you need to halt the disposal of records, how is this accomplished?
 - 7. Has the company issued any guidance for attorneys to promote uniformity?
 - 8. Who is responsible for determining when a suspension is necessary? To write the instruction to suspend disposal? To approve or authorize the suspension? To communicate the suspension of disposal?
 - 9. How is the suspension communicated?
 - 10. How is the suspension worded to make it understandable?
 - 11. How long does it take to develop and issue an instruction to hold records?
 - 12. What principles govern decisions as to the scope (years and varieties) of records that must be held?
 - 13. Are suspended records held in the normal work area or sent elsewhere?
 - 14. When the suspension ends and normal disposal can resume, how is that communicated? How is compliance with the suspension verified?

Once completed, the survey data can be used to develop a new or updated information and records management policy that addresses the specific needs of the organization. The survey results are also likely to identify those areas of the organization where gaps exist between current record-keeping methods and records management best practices.

Resolving these gaps usually requires the development of supporting procedures, guidelines and directives to address specific records life cycle matters. It will also require technological initiatives to incorporate records management requirements into existing and planned business systems. An action plan that prioritizes these additional activities should be developed so that improvements in record-keeping practices address those shortfalls that expose the organization to unnecessary legal or operational risks.

Appendix D: Technical Appendix

This technical appendix is included to provide an extended description and discussion of two important concepts: (1) metadata and (2) electronic (digital) archives.

1. Metadata:

What it is: Metadata (data about data) includes all the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records. Metadata can come from a variety of sources. It can be created automatically by a computer, supplied by a user, or inferred through a relationship to another document. Metadata is created, modified and disposed of at many points during the life of electronic information or records.¹

Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed.

What it does: Metadata may connect to electronic information or records in a variety of ways. The electronic information or record may contain a reference to the metadata, or vice versa. For example, a hypertext document may contain a link to an index that provides information about its context. A folder or directory listing may contain a reference to the location where the content of the electronic document is found.

Why it may be important: Certain metadata is critical in information management and for ensuring effective retrieval and accountability in record-keeping. Metadata can certify the authenticity of the content of electronic documents, as well as establish the context of the content. Metadata can also identify and exploit the structural relationships that exist between and within electronic documents, such as versions and drafts. Metadata allows organizations to track the many layers of rights and reproduction information that exist for records and their multiple versions. Metadata may also document other legal or security requirements that have been imposed on records; for example, privacy concerns, privileged communications or work product, or proprietary interests.

Metadata's importance in searching: Searching capabilities can be significantly enhanced through the existence of rich, consistent metadata. Searching is generally used in records management to select and/or classify data. For example, proper searching can help with the assignment of electronic documents, files and messages into appropriate records management categories. Metadata such as dates, folder information, subject designations and other properties can help generate or validate classifications of the item. Metadata such as e-mail thread information can be used to help assure that related items are maintained in context and/or treated consistently. If

¹ Examples of metadata (for electronic document files) include: a file's name, a file's location (*e.g.*, directory structure or pathname), file format or file type, file size, file dates (*e.g.*, creation date, date of last data modification, date of last data access, date of last metadata modification), file permissions (*e.g.*, who has read the data, who can write to it, who can run it). Metadata can also include user-input attributes, such as e-mail subject and addressing, keywords, content description, business purpose, and retention codes and classifications, and the person responsible for the record's retention and disposition.

descriptive metadata are the same or can be mapped across different electronic repositories, metadata can also make it possible to search across multiple collections or to create virtual collections from materials that are distributed across repositories.

Metadata and records management: Metadata can also play a crucial role in record lifecycle management. Organizations can design systems that will allow users to input information regarding retention periods and automatically identify or dispose of obsolete records based on those retention periods.

Where it resides: Some metadata is held in structures separate from the core electronic information or record, such as directories, listings and indexes of the files or messages, but may still be regarded as an integral part of the electronic information or record for certain purposes. For example, e-mail messages may be stored with a variety of metadata that may not be viewed by the end-user in the standard setup of the program used to view messages. This metadata may provide important information about a message, such as message thread information that may provide context for the message and a variety of date/time settings. A database may contain metadata, such as the time of entry or modification, the identity of the record's creator, and other information. Document management systems, which are programs designed particularly to preserve tracking and identifying information about electronic documents, hold a great deal of metadata.

The forms it takes: Metadata may be different depending on how or when it is accessed or viewed. For example, when a message is transmitted through an e-mail system it carries with it a variety of metadata, such as the date of creation, transmission to the recipient, and receipt, and the identity of all recipients, including those sent blind carbon copies. After the message has been stored by the recipient, "bcc" information may no longer be directly available to him or her. Yet, when the message is stored by the recipient, "storage level" metadata, not available while the same message is in transmission, may become associated with it. Such storage level metadata may include the folder in which the message is stored and the dates and times it has been re-forwarded or replied to by the recipient.

Metadata migration: For records to remain accessible and intelligible over time, it may be necessary to preserve and migrate the metadata associated with those records. If records that are currently being created are to have a chance of surviving migrations through successive generations of computer hardware and software, or removal to entirely new delivery systems, they will need to have metadata that enables them to exist independently of the system that is currently being used to store and retrieve them. Technical, descriptive and preservation metadata that documents how a record was created and maintained, how it behaves and how it relates to other records will all be essential.

Metadata considerations: There will always be important tradeoffs between the costs of developing and managing metadata to meet current needs, and creating sufficient metadata that can be capitalized upon for future, often unanticipated uses. As organizations develop records systems, they should consider which aspects of metadata are essential for what they wish to achieve and how detailed they need each type of metadata to be. An organization may require frequent ad-hoc discovery searches across information systems, protection from inadvertent destruction of documents or e-mail messages, or it may need to prevent disclosure of sensitive trade secrets from being re-distributed or copied.

It should be noted that some software applications carry forward the original author's name in the metadata. Thus, if another person, in creating a new record (*e.g.*, a letter), copies it and then modifies it with new information, it may still reflect the name of the original creator of the record

used to recreate the format in the metadata of the new record. In such case, the metadata for the new record may be misleading as to the “real” author of the new record.

Metadata standards: National and international guidelines (such as DOD 5015.2, ISO 15849, Model Requirements for The Management of Electronic Records (MoReq), or ISO 23950 (formerly Z39.50) can be extremely helpful in making sure that an organization’s metadata standards meet the needs of the organization’s users.

Transmission of metadata: Individuals who create and transmit electronic documents are often unaware of the existence of readable metadata that may inadvertently reveal privileged or confidential information to adversaries and other outside parties. Organizations should consider adopting policies to provide guidance to users regarding the transmission of metadata. Moreover, many organizations publishing data on “nets” (extra, intra, inter) may not be fully aware of the metadata that may be indexed by outside search engines and viewed by individuals outside the organization.

There are a variety of methods for managing and controlling the extent of metadata transmitted with the core data. Some formats designed for transmission of data, such as XML, provide the functionality for the organization to determine which metadata fields are and are not transmitted with the core data. Other formats, such as the Adobe Portable Document Format (PDF) or Tagged Image Format (TIFF), can be used to remove certain metadata from the core document and to standardize the manner in which the document is maintained. Yet another approach is the use of “metadata stripper” technology, which removes some or all of the metadata from a native electronic file; however, such technology is not available for all types of data and may not be easily usable by end-users. Other technologies may be available for these purposes. Each technology embodies a different approach to the storage and transmission of the core document and metadata, and each may be appropriate in a given set of circumstances, depending on a variety of considerations, including usability of the data, cost, governmental rules and regulations, and other factors.

Metadata and new technology challenges: Emerging technologies may make the management of metadata in the electronic records context much more difficult. For example, “virtual foldering” may allow users to apply several different sets of metadata to a given electronic document depending on the context in which the document is viewed or processed. The metadata in this scenario may not be associated with a single document, but shared across a set of documents through a non-document information stores. As technology advances, metadata continues to evolve.

Some types of metadata continue to undergo changes that may increase the difficulty of electronic records management and production of electronic documents for legal proceedings. For example, on some (but not all) existing systems, the user or system administrator can control access to and usage of files and messages by rights or permissions. These constraints can themselves be important metadata properties for legal or records management purposes, and can also impact an organization’s ability to store or review its own data. In order to assure that all data can be accessed for purposes of the legal or records management function, permissions or rights to the data must be taken into consideration. Likewise, the legal and records management functions can be affected by encryption of data, procedures for compression and encoding, and other technologies that can make data difficult to identify or review.

One emerging technology that may have a significant impact is known as “electronic rights”, which refers to increased control over data access, storage and copying to prevent unauthorized use,

primarily in the copyright-protection area. Technologies designed to enforce electronic rights may cause records to be automatically soft-deleted prior to the expiration of its appropriate retention period, or may prevent the record from being reviewed or copied where necessary for records management or litigation purposes. Particularly in the area of audio-visual files (including voice mail and video recordings) the potential for restrictions in this area are significant.

2. Electronic (Digital) Archives:

What they are: Electronic archives are repositories for electronic records in a form that facilitates searching, reporting, analysis, production, preservation and disposition. When properly set up and maintained, electronic archives are not solely static collections of records (whether on-line or off-line on mass media such as tapes or optical media).

The importance of metadata in electronic archives: The key to maximizing the utility of an electronic archive is the availability of record metadata—especially metadata that cannot be easily derived from the record content—and record management data (such as the business owner, the planned disposition date, various retention factors, etc.) along with the native record. This additional data may add value for searching, reporting and analysis purposes. By adding value for business or user processes, electronic archive systems can present a positive situation for all parties within an organization.

Policies for access to long-term electronic archives should consider requirements for current and post-disposition access to metadata and statistical information.

Long-term business needs for metadata should be weighed against risk and record management requirements for comprehensive removal of both records and their associated metadata at the planned disposition point. These long-term needs may include compliance reporting, productivity analysis, project task and cost analysis, and other forms of detailed and statistical reporting.

Forms of electronic archives: Archives may be monolithic systems encompassing all functions required to create, retrieve, update, and delete electronic records across an organization, or they may be made up of multiple integrated electronic systems. This latter architecture is particularly appropriate for large organizations which already have document management (“DM”) or knowledge management (“KM”) systems in-place.

Integration of DM/KM and RM: The European Communities’ “Model Requirements for the Management of Electronic Records”² (“MoReq”) distinguishes between a DM and RM system (equivalent to an electronic archive in this context) as follows:

DM System ...	RM System ...
Allows documents to be modified and/or to exist in several versions.	Prevents records from being modified.
May allow documents to be deleted by their owners.	Prevents records from being deleted except in certain strictly controlled circumstances.
May include some retention controls.	Must include rigorous retention controls.

² Available at <http://www.cornwell.co.uk/moreq.html>.

DM System ...	RM System ...
May include a document storage structure, which may be under the control of users.	Must include a rigorous record arrangement structure (the classification scheme) which is maintained by the Administrator.
Is intended primarily to support day-to-day use of documents for business.	May support day-to-day working, but is also intended to provide a secure repository for meaningful business records.

Many DM/KM systems contain electronic archive (or electronic records management) functions, either as part of the base system, as add-on components or available through programmatic features. Where those functions do not exist for the system, it may be necessary to integrate stand-alone DM/KM and electronic archive systems by means of a real-time or periodic transfer between the respective repositories. The development effort involved in this integration can be significant. Both the MoReq and DoD 5015.2-STD³ provide useful starting points for defining integration requirements.

Electronic archives and e-mail: For most organizations, the ability of the electronic archive to work with existing e-mail systems will be critical. David Stephens notes:

... the management of e-mail is sometimes characterized as the single biggest records management problem in the USA. Thus, for any organization looking to implement major initiatives in the management of its electronic records, e-mail systems should be the initial focus of such efforts.⁴

Integration of e-mail can vary from simple journaling (also called “logging”) of all messages to the electronic archive, to interactive interfacing with the client e-mail application (for example, adding record classification functions to Microsoft Outlook). At a minimum, electronic archives should be able to serve as a repository for e-mail records exported from the e-mail servers. Many commercial e-mail archive and records management add-on products are available for popular e-mail systems (such as Microsoft Exchange and IBM/Lotus Notes).

Electronic archives and technology changes: As new applications are developed or acquired within organizations, the records management requirements relative to those applications should be anticipated and planned as part of the system development or purchase process. Digital preservation requires routine efforts to migrate records to overcome software and technological obsolescence and from deteriorating media.

Standards for electronic archives: Long-term electronic archive designs should consider incorporation of national or international specifications such MoReq or Open Archival Information System (OAIS). Standards such as ISO 15489⁵ establish guidelines for records management policies and systems but generally fall short of specifying functional details of automated systems. However, DoD 5015.2-STD MoReq contain useful information defining functional requirements for

³ Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (2002), *Design Criteria Standard for Electronic Records Management Software Applications (DoD 5015.2-STD)*.

⁴ David Stephens and Roderick Wallace, *Electronic Records Retention: New Strategies for Data Life Cycle Management* (ARMA International 2003).

⁵ Available at <http://www.iso.org>. The two components of the standard are ISO 15489-1:2001 and ISO/TR 15489-2:2001.

electronic record archives. Both of these also define selected metadata elements required for an electronic records archive. Either document would be appropriate as a starting point for acquisition or construction of an electronic archive system. Finally, both ARMA International and the National Archives Records Administration (NARA) provide planning and guideline documents at their respective web sites.⁶

Tracking non-electronic records: Organizations designing comprehensive long-term electronic archives should consider the need for managing and tracking electronic and non-electronic records. This may include migration from legacy systems tracking paper, film/fiche, artifacts and electronic records.

Electronic archives and storage media: Policies for maintenance of long-term electronic archives should address selection of storage media and formats appropriate for data usage requirements and planned retention periods, including multi-format and multi-media transfers over the life of records. For the purposes of this discussion, “storage media” refers to the physical devices holding records. For electronic records this is typically fixed or removable hard disks, diskette cartridges (“floppy diskettes” of various sizes, high-density cartridge disks such as those manufactured by Iomega (“Zip disks” and “Jaz disks”) and Syquest), optical disks such as CDs and DVDs, or reel and cartridge tape. Excluding the optical disks, all these media store data electromagnetically and are capable of both reading and writing data through many “store-delete-write” cycles. Optical disks, as the name implies, store data by modifying the optical characteristics of a coated plastic disk. Some types of optical disks are capable of both reading and writing through many cycles; others are “Write Once, Read Many” (WORM)—meaning data can be written to the disk only once (that is, it is not updateable) but the disk can be read many times. The most common type of WORM disks are “CD-R” (“Compact Disk-Recordable”).

Storage media can be proprietary (controlled by a single corporation, often with details of the construction not available to other parties) or non-proprietary (typically controlled by a standards organization or a consortium of corporations; details of the construction may be available to other parties or restricted to members of the consortium). All present high-density cartridge disks and some forms of cartridge tapes are proprietary designs.

Significant issues may exist with media volume when used for archive purposes. At present, the highest density optical disks offer roughly 10% of the capacity of the highest density magnetic tape cartridges. Physical storage space requirements are comparable between the two (the amount of physical space required to store a given set of data) and storage arrays (“libraries” of multiple optical disks or cartridge tapes) exist for both media. Magnetic cartridge tape remains significantly more common for large-scale and long-term off-line and near-line storage in the corporate community.

When speaking of storage devices, the physical device is only half of the picture. The other half concerns how data records are stored on the physical device. “Format” refers to the binary representation of the data comprising a record. For electronic records there is usually a “native” format: the binary representation used by the application which normally creates, reads, and modifies the record as it is used during the active portion of its lifecycle. As an example, a project status report may be a Microsoft Excel spreadsheet; its format would be the proprietary binary format used by Microsoft for writing of this spreadsheet to storage media (informally this particular

⁶ Available at <http://www.arma.org>; available at <http://www.nara.gov>.

format is often called an “XLS file” because of the default file naming (“MyReport.XLS”, “Report701.XLS”, etc.) used by the Excel program). This format is called a proprietary format because its structure is “owned” and controlled by one corporation (Microsoft in this case). “Non-proprietary” formats may be public domain or made freely available for use by any organization. Some non-proprietary formats are nationally or internationally standardized. For example, the ASCII (American National Standard for Information Interchange) text representation coding is a North American standard. Others are de facto standards, an example of which is the PDF (Portable Document Format) binary representation for documents; this format is widely used by many Internet systems and document management applications.⁷

Ideally, long-term storage formats should be non-proprietary to avoid issues with technological and business obsolescence. However, in practice, non-proprietary formats may not support content and metadata information with sufficient fidelity to serve for archival purposes.

A well-designed electronic archive should support multiple storage media and provide mechanisms for tracking physical write date and time stamps for a given record (that is, the system should track when a record was stored on a given media—this is significantly different from the record creation metadata tracking when a record’s content was initially produced).

For records with long retention requirements it may be necessary to copy records to fresh media periodically. This process of copying to new media is referred to as “refreshing.” When should refresh copies be made? The National Library of Australia has concluded the best choices for long-term (over ten year) archival media and format are CD-R media and XML data formatting.⁸ Regarding optical media, they note “the lifetime of optical disks of all kinds, and especially CD-Rs, is greater than the technological obsolescence factor of their recording and playback technology.”⁹ NARA, in combination with the National Institute of Standards and Technology (NIST), provides guidance on CD and DVD media and formats in the NIST Special Publication 500-252, *Care and Handling of CDs and DVDs—A Guide for Librarians and Archivists* (NIST October 2003). The results of NIST’s evaluations are controversial and do not agree with manufacturer and independent testing.¹⁰ Given the significant variance among these expected life figures, a reasonable compromise may be to use the best quality media available, maintain both on-line and off-line media in an environmentally controlled space (stability appears more important than specific temperature and humidity values), and plan on refresh copies at intervals of no more than ten years.

⁷ PDF is copyrighted by Adobe Corporation but the specification has been made available for use by any party wanting to read or write documents using this format. Commercial applications writing this format may require a license from Adobe.

⁸ XML—Extensible Markup Language is a WWW (W3) Consortium standard; XML documents are encoded in UNICODE (itself an ISO standard for international character representations). Conceptually XML documents can contain any type of data (text, multimedia, numeric, etc.). In practice, XML documents are best suited for text and numeric information.

⁹ Ross Harvey, Presentation at the 2nd Nat’l Preservation Office Conference: Multimedia Preservation—Capturing the Rainbow in Brisbane (Nov. 28-30, 1995), available at <http://www.nla.gov.au/niac/meetings/npo95rh.html>.

¹⁰ A recent independent test on CD-R media concluded that many brands of inexpensive optical media have a useful life of less than two years. This contrasts dramatically with the NARA/NIST finding of an expected minimum useful life of 57 years. Refer to *PC-Active* (September 2003) for the most recent documented independent tests (available at <http://www.aktu.nl/pc-active/cdr.htm> (Dutch)); see *Development of a Testing Methodology to Predict Optical Disk Life Expectancy Values* (NIST 500-200), available at <http://palimpsest.stanford.edu/byorg/nara/nistsum.html>; last updated March 2002.

Due to rapid technological obsolescence, organizations may wish to consider duplicating particularly valuable records that must be kept for more than ten years to non-electronic media (*e.g.*, computer and output microfilm or “COM;” or archival paper).

Electronic archives and obsolescence: The electronic archive itself may be an application or set of applications. Over time these may change or become obsolete—often in less time than the longest retention period for the records associated with the system. For this reason, the archive architecture must anticipate and support future migration needs to new versions of the archive and the underlying storage media and formats.

Electronic archives and records destruction: Policies for maintenance of long-term electronic archives should address destruction and removal of records (and, as appropriate, their metadata) including any need for forensic-level electronic deletions. Methods for obtaining approval for destruction should be incorporated in the archive system.

Deletion of electronic records has a number of potential issues. In many electronic systems, there are two types of deletion: “logical” (or “soft”) deletions which mark record content as being unavailable (but do not immediately remove the record metadata or content) and “physical” deletions which remove a record’s content from its associated storage media (but do not necessarily remove all record metadata). Physical deletions typically require more time and computing resources than logical deletions. For this reason, physical deletions are often deprecated for systems requiring a high degree of user interactivity. Physical deletions may often be recovered; to prevent such recovery it is necessary to use a “wiping” technology that overwrites the deleted information in such a manner that it would require unusual (and expensive) techniques to accomplish recovery.

Deletion occurs in several levels on modern computer systems:

- (a) **File level deletion:** Deletion on the file level renders the file inaccessible to the operating system and normal application programs and marks the space occupied by the file’s directory entry and contents as free space, available to reuse for data storage.
- (b) **Record level deletion:** Deletion on the record level occurs when a data structure, like a database table, contains multiple records; deletion at this level renders the record inaccessible to the database management system (DBMS) and usually marks the space occupied by the record as available for reuse by the DBMS, although in some cases the space is never reused until the database is compacted. Record level deletion is also characteristic of many e-mail systems.
- (c) **Byte level deletion:** Deletion at the byte level occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file’s content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.

Electronic archives should provide disposition functions for both logical and physical record deletions and permit specification of which, if any, associated metadata elements should be removed.

One issue that often arises is tracking details of when and how a given record may have been removed from the archive. In the paper world, “Certificates of Destruction” exist as proof that a set of records was destroyed by a particular method and by a specific organization on a given date. If a need exists for similar compliance documentation on electronic records, it will be necessary to keep a minimal set of metadata about those records to have a “target” for the data tracking the

disposition. This requirement will only exist if it is necessary to track the disposition information on specific records. Generic statistics (for example, a count of records deleted) can be maintained without retaining record metadata.

Electronic archives and security: Policies for access to long-term electronic archives should consider requirements for ownership and control including, but not limited to, security, traceability, and change-control over the record lifecycle.

The National Archives and Records Administration (NARA) *Concept of Operations*¹¹ provides useful guidelines for typical user functions and associated ownership concerns (references to “NARA” have been changed to “RM electronic archive”):

Access—All record users will be able to search and retrieve unclassified, unrestricted materials, which have been processed into the electronic records archive (ERA), either anonymously or by signing on as a registered user. Users with special access rights (clearances) and privileges will be checked for appropriate clearances by ERA upon accessing the system.

Search—The user searches ERA for information describing records and for actual content within records. Such searching may be done at a variety of levels of aggregation (documentary materials series/collections or individual items). Within the user’s given access rights and privileges, the user may take advantage of available functions and features. ERA responds to queries by identifying either sets of documentary materials, or individual documents, with results constrained by the user’s access rights. The user views and/or sorts the results of the search, modifies the search if necessary, and refines or saves query results as desired. In this manner, the user is able to progress from a query about a general topic to a list of specific documentary materials that the user may wish to view.

Retrieve/Receive—From search results that identify relevant documentary materials, the user views and accesses the records desired. The user directly interacts with the ERA system and accesses records in accordance with established user privileges and access rights.

User roles for electronic archives: When planning for specific control over the access, search, and retrieval rights of records in an archive there are a number of possible user roles. Users serving in these roles work in different ways—and at different times in the record lifecycle—with the archive itself, the record content and metadata, and the records policy infrastructure. Within the electronic archive there may be specific metadata associated with each role. The NARA *Concept of Operations* guide provides a working set of typical roles:¹²

Originating Entity (may also be called the “Author” or “User” in some contexts)—Creates and receives documentary materials and prepares and transfers them to the RM system.

¹¹ *Electronic Records Archives Concept of Operations*, § 6.6.2 (User Activities) available at http://www.archives.gov/electronic_records_archives/about_era/print_friendly.html?page=concept_of_operations_content.html&title=NARA%20%7C%20ERA%20@7C%20Concept. Note that this section defines additional classes of activities, specifically “Mediated Request” and “Fee for Service” functions, which do not apply in typical corporate archive environments.

¹² *Electronic Records Archives Concept of Operations*, § 5.3.1 (User Classes) available at http://www.archives.gov/electronic_records_archives/about_era/print_friendly.html?page=concept_of_operations_content.html&title=NARA%20%7C%20ERA%20@7C%20Concept.

Appraiser—Makes recommendations on materials that will be transferred to (RM system) holdings or will be disposed of by the Originating Entity.

Accession Processor—Accessions and processes a transfer (“accession” is the records management function of receiving a record or set of records into storage).

Preserver—Performs processing activities that ensure the ability to provide long-term access to documentary materials.

Access Reviewer—Reviews documentary materials in (the RM system) custody for access restrictions.

Record User—Uses the system to access documentary materials.

Administrative User—Handles such activities as granting user access rights, monitoring system performance, and scheduling reports.

This set should not be taken as absolute: many organizations will have only some of the roles, and some organizations will have additional roles. In particular, records management policies may define other roles (such as “Official Record Owner”, “Records Contact”, etc.) as appropriate for a given environment and organizational context. Finally, for electronic archives some roles, such as “Accession Processor” may be handled by automated agents (that is, by software rather than people).

There are additional Information Technology or Services (IT/IS) roles that may apply to an electronic archive system. These roles would be responsible for the creation and maintenance of the application software, hardware, and underlying database technology.

User management to control and track access, as well as change ownership and user roles, should be handled by an archive administration role. The NARA *Concept of Operations* guide refers to this role as the “administrative user” and describes three activities associated with the role:¹³

User rights and privileges—The administrative user assigns user rights and privileges based upon clearances held, permissions granted, job roles captured at the time of registration within the system, and RM policy.

Schedule Reports—The request for reports could be based on a specific requirement from RM policy or from a system monitoring need.

Monitor System—The Electronic Records Archive (ERA) provides the administrative user with the ability to monitor system performance and security.

The need for reporting functions: Reporting functions within the electronic archive—or the equivalent facility to report against the data technology underlying the archive (for example, to perform SQL (“Structured Query Language”) queries against an Oracle database on which the archive was built)—should provide access to historical, transactional and current record management metadata sufficient for auditing and verification of the archive. These tools provide the mechanisms critical to on-going validation of archive use, policy compliance, litigation analysis and extraction, and statutory or regulatory processing requirements.

¹³ *Electronic Records Archives Concept of Operations*, § 6.7 (Administrative User Scenario) available at http://www.archives.gov/electronic_records_archives/about_era/print_friendly.html?page=concept_of_operations_content.html&title=NARA%20%7C%20ERA%20@7C%20Concept.

Appendix E: Glossary

This glossary is intended to define terms of art used in this white paper or common to the disciplines of records management and information technology as they relate to topics covered here, including the identification, collection, and analysis of information and records for investigation and litigation. This glossary is not comprehensive or exhaustive of such terms. References to “DoD 5015” refer to Department of Defense “Design Criteria for Electronic Record Management Software Applications” (October 2003).

Active Data: Active Data is information residing on the direct access storage media (disk drives or servers) of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without restoration or reconstruction.

Active Records: Active Records are those Records related to current, ongoing or in-process activities and are referred to on a regular basis to respond to day-to-day operational requirements. An active record resides in native application format and is accessible for purposes of business processing with no restrictions on alteration beyond normal business rules. *See* Inactive Records.

Ambient Data: *See* Residual Data.

Application: An application is a collection of one or more related software programs that enables a user to enter, store, view, modify or extract information from files or databases. The term is commonly used in place of “program,” or “software.” Applications may include word processors, Internet browsing tools and spreadsheets.

Archival Data: Archival Data is information that is not directly accessible to the user of a computer system but that an organization maintains for long-term storage and record-keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other

electronic storage device, or may be maintained on system hard drives or network servers.

Archive, Electronic Archive: Archives are long term repositories for the storage of records. Electronic archives preserve the content, prevent or track alterations and control access to electronic records. *See* the discussion of electronic archives in the Technical Appendix, Appendix D.

Attachment: An attachment is a record or file associated with another record for the purpose of storage or transfer. There may be multiple attachments associated with a single “parent” or “master” record. The attachments and associated record may be managed and processed as a single unit. In common use, this term refers to a file (or files) associated with an e-mail for transfer and storage as a single message unit. Because in certain circumstances the context of the attachment—for example, the parent e-mail and its associated metadata—can be important, an organization should consider whether its policy should authorize or restrict the disassociation of attachments from their parent records.

Attribute: An attribute is a characteristic of data that sets it apart from other data, such as location, length, or type. The term attribute is sometimes used synonymously with “data element” or “property.”

Author or Originator: The author of a document is the person, office or designated position responsible for its creation or issuance. In the case of a document in the form of a letter, the author or originator is usually indicated on the letterhead or by signature. In some cases, the software application producing the document may capture the author's identity and associate it with the document. For records management purposes, the author or originator may be designated as a person, official title, office symbol or code. (DoD 5015)

Backup Data: Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media. Backup data serves as a source for recovery in the event of a system problem or disaster. Backup data is distinct from "Archival Data."

Backup Tape Recycling: Backup Tape Recycling describes the process whereby an organization's backup tapes are overwritten with new data, usually on a fixed schedule determined jointly by records management, legal and IT sources. For example, the use of nightly backup tapes for each day of the week with the daily backup tape for a particular day being overwritten on the same day the following week; weekly and monthly backups being stored offsite for a specified period of time before being placed back in the rotation.

Backup tapes: See Disaster Recovery Tapes.

Compact Disk (CD): A type of optical disk storage media, compact disks come in a variety of formats. These formats include CD-ROMs ("CD-Read-Only-Memory") that are read-only; CD-Rs ("CD-Recordable") that are write to once and are then read-only; and CD-RWs (CD-Read-Write") that are write to in multiple sessions.

Computer Forensics: Computer Forensics (in the context of this document, "forensic analysis") is the use of specialized

techniques for recovery, authentication and analysis of electronic data when an investigation or litigation involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel, and generally requires strict adherence to chain-of-custody protocols.

Custodian: See Record Custodian.

Data Element: A combination of characters or bytes referring to one separate piece of information, such as name, address, or age. (DOD 5015)

Database Management System

(DBMS): A software system used to access and retrieve data stored in a database. (DOD 5015)

Database: In electronic records, a set of data elements, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users. (DOD 5015)

De-Duplication: De-Duplication ("De-Duping") is the process of comparing electronic records based on their characteristics and removing or marking duplicate records within the data set.

Delete, Deletion: The process of permanently removing, erasing or obliterating recorded information from a medium, especially a reusable magnetic disk or tape. (DOD 5015) Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except by using special data recovery tools designed to recover deleted data.

Deleted Data: Deleted Data are data that existed on the computer as live data and

which have been deleted by the computer system or end-user activity. Deleted data may remain on storage media in whole or in part until they are overwritten or “wiped.” Even after the data have been wiped, directory entries, pointers or other information relating to the deleted data may remain on the computer. “Soft deletions” are data marked as deleted (and not generally available to the end-user after such marking), but not yet physically removed or overwritten. Soft-deleted data can be restored with complete fidelity.

Disaster Recovery Tapes: Disaster Recovery Tapes are portable media used to store data for backup purposes. *See* Backup Data.

Disposition: The final business action carried out on a record. This action generally is to destroy or archive the record. Electronic record disposition can include “soft deletions” (*see* Deletion), “hard deletions,” “hard deletions with overwrites,” “archive to long-term store,” “forward to organization,” and “copy to another media or format and delete (hard or soft).”

Distributed Data: Distributed Data is that information belonging to an organization which resides on portable media and non-local devices such as remote offices, home computers, laptop computers, personal electronic assistants (“PDAs”), wireless communication devices (*e.g.*, Blackberry), internet repositories (including e-mail hosted by internet service providers or portals and web sites) and the like. Distributed data also includes data held by third parties such as application service providers and business partners. In the event of litigation, distributed data may present additional issues for collection and analysis. *Note:* Information Technology organizations may define distributed data differently (for example, in some organizations distributed data includes any non-server-based data, including workstation disk drives).

Draft Record: Draft records can include working files such as preliminary drafts, notes, supporting source documents and similar materials. Organizations may determine that drafts should be retained if (1) they contain unique information including the substantive mental impressions of the author as to a business policy, decision, action or responsibility; or (2) they reflect substantive comments, annotations or comments by persons other than the author concerning a business policy, decision, action or responsibility; or (3) they are transmitted, circulated or made available to persons other than the author for business purposes such as approval, comment, action, recommendation or follow-up.

Electronic Mail: Electronic Mail, commonly referred to as “e-mail,” is an electronic means for communicating information under specified conditions, generally in the form of text messages, through systems that will send, store, process, and receive information, and in which messages are held in storage (until the addressee accesses them).

Electronic Mail Message: A document created or received via an electronic mail system, including brief notes, formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message. 36 CFR 1234.2, reference (aa). (DOD 5015)

Electronic Record: Information recorded in a form that requires a computer or other machine to process it and that otherwise satisfies the definition of a record. (DOD 5015)

File Plan: A document containing the identifying number, title, description and disposition authority of files held or used in an office. (DOD 5015)

Forensic Copy: A forensic copy is an exact copy of the entire physical storage

media (hard drive, CD-ROM, DVD-ROM, tape, etc.), including all active and residual data and unallocated space on the media. Forensic copies are often called “image or imaged copies”.

Format: The internal structure of a file, which defines the way it is stored and used. Specific applications may define unique formats for their data (e.g., “MS Word document file format”). Many files may only be viewed or printed using their originating application or an application designed to work with compatible formats. Computer storage systems commonly identify files by a naming convention that denotes the format (and therefore the probable originating application) (e.g., “DOC” for Microsoft Word document files; “XLS” for Microsoft Excel spreadsheet files; “TXT” for text files; and “HTM” (for Hypertext Markup Language (HTML) files such as web pages). Users may choose alternate naming conventions, but this may affect how the files are treated by applications.

Hold: See Legal Hold.

Image Copy, Imaged Copy: See Forensic Copy.

Inactive Record: Inactive records are those Records related to closed, completed, or concluded activities. Inactive Records are no longer routinely referenced, but must be retained in order to fulfill reporting requirements or for purposes of audit or analysis. Inactive records generally reside in a long-term storage format remaining accessible for purposes of business processing only with restrictions on alteration. In some business circumstances, inactive records may be re-activated.

Information: For the purposes of this document, information is used to mean both documents and data.

Instant Message, Instant Messaging (“IM”): Instant Messaging is a form of electronic communication, which involves immediate correspondence between two or

more users who are all online simultaneously. Some IM communications (peer-to-peer) may not be stored on servers after receipt.

Janitor Program: An application which runs at scheduled intervals to manage business information by deleting, transferring, or archiving on-line data (such as e-mail) at specific points in time. Janitor programs are sometimes referred to as “agents”—software that runs autonomously “behind the scenes” on user systems and servers to carry out business processes according to pre-defined rules.

Legacy Data, Legacy System: Legacy Data is information in which an organization may have invested significant development resources and which has retained its importance but has been created or stored by the use of software and/or hardware that has become obsolete or replaced (“legacy systems”). Legacy data may be costly to restore or reconstruct when required for investigation or litigation analysis or discovery.

Legal Hold: A legal hold is a communication issued as a result of current or anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records. The specific communication to business or IT organizations may also be called a “hold,” “preservation order,” “suspension order,” “freeze notice,” “hold order,” or “hold notice.”

Lifecycle: The records lifecycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and archive to final disposition.

Metadata: Metadata is information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted (including data demographics such as size, location, storage requirements and media

information). *See* Technical Appendix D for discussion of Metadata.

Migration: Moving files to another computer application or platform which may require changing their formats.

Mount, Mounting: The process of making off-line data available for on-line processing. For example, placing a magnetic tape in a drive and setting up the software to recognize or read that tape. The terms “load” and “loading” are often used in conjunction with, or synonymously with, “mount” and “mounting” (as in “mount and load a tape”). “Load” may also refer to the process of transferring data from mounted media to another media or to an on-line system.

Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the “native format” of the document. Because viewing or searching documents in the native format may require the original application (for example, viewing a Microsoft Word document may require the Microsoft Word application), documents are often converted to a vendor-neutral format as part of the record acquisition or archive process. *Cf.* “Static” formats.

Near-line data storage: Storage in a system that is not a direct part of the network in daily use, but that can be accessed through the network. There is usually a small time lag between the request for data stored in near-line media and its being made available to an application or end-user. Making near-line data available will not require human intervention (as opposed to “off-line” data which can only be made available through human actions).

Official Record Owner: *See* Record Owner.

Off-line data: The storage of electronic data outside the network in daily use (*e.g.*, on backup tapes) that is only accessible through the off-line storage system, not the network.

On-line storage: The storage of electronic data as fully accessible information in daily use on the network or elsewhere.

Preservation Notice, Preservation Order: See Legal Hold.

Record: Information, regardless of medium or format, that has value to an organization. Collectively the term is used to describe both documents and electronically stored information.

Record Custodian: A records custodian is an individual responsible for the physical storage and protection of records throughout their retention period. In the context of electronic records, custodianship may not be a direct part of the records management function in all organizations. For example, some organizations may place this responsibility within their information technology department, or they may assign responsibility for retaining and preserving records with individual employees. For this reason, this publication discusses the possibility of having a content custodian and a technology custodian.

Record Lifecycle: The time period from when a record is created until it is disposed.

Record Owner: The records owner is the subject matter expert on the content of the record and is responsible for the lifecycle management of the record. This may be, but is not necessarily, the author of the record.

Record Series: A description of a particular set of records within a file plan. Each category has retention and disposition data associated with it, applied to all record folders and records within the category. (DOD 5015)

Records Hold: *See* Legal Hold.

Records Management: Records Management is the planning, controlling, directing, organizing, training, promoting and other managerial activities involving the life-cycle of information, including creation,

maintenance (use, storage, retrieval) and disposition, regardless of media.

Records Manager: The records manager is responsible for the implementation of a records management program in keeping with the policies and procedures that govern that program, including the identification, classification, handling and disposition of the organization's records on all media throughout their retention life. The physical storage and protection of records may be a component of this individual's functions, but it may also be delegated to someone else. *See* Records Custodian.

Records Retention Period, Retention Period: The length of time a given records series must be kept, expressed as either a time period (*e.g.*, four years), an event or action (*e.g.*, audit), or a combination (*e.g.*, six months after audit).

Records Retention Schedule: A plan for the management of records, listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to historical archives.

Records Store: *See* Repository for Electronic Records.

Record Submitter: The Record Submitter is the person who enters a record in an application or system. This may be, but is not necessarily, the author or the record owner.

Recover, Recovery: *See* Restore.

Report: Formatted output of a system providing specific information.

Repository for Electronic Records: Repository for Electronic Records is a direct access device on which the electronic records and associated metadata are stored. (DoD 5015) Sometimes called a "records store" or "records archive."

Residual Data: Residual Data (sometimes referred to as "Ambient Data") refers to data that is not active on a computer system.

Residual data includes (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted, in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

Restore: To transfer data from a backup medium (such as tapes) to an on-line system, often for the purpose of recovery from a problem, failure, or disaster. Restoration of archival media is the transfer of data from an archival store to an on-line system for the purposes of processing (such as query, analysis, extraction or disposition of that data). Archival restoration of systems may require not only data restoration but also replication of the original hardware and software operating environment. Restoration of systems is often called "recovery".

Retention Schedule: *See* Records Retention Schedule.

Sampling: Sampling usually (but not always) refers to the process of testing a database for the existence or frequency of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions about what repositories of data are appropriate to search in a particular litigation and determinations of the validity and effectiveness of searches or other data extraction procedures. Sampling can be useful in providing information to the court about the relative cost burden versus benefit of requiring a party to review certain electronic records.

Slack Space: A form of residual data, slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments and other

information useful for forensic analysis of computer systems.

Spoliation: Spoliation is the destruction of records which may be relevant to ongoing or anticipated litigation, government investigation or audit. Courts differ in their interpretation of the level of intent required before sanctions may be warranted. *See* Guideline 3.

Static formats. “Static” formats (often called “imaged formats”) are designed to retain a “picture” of the document as it would look viewed in the original creating application but do not allow manipulation of the document information; such formats may be well-suited for many records and litigation uses where access to document metadata and preservation of original document structures are not important. *Cf.* Native Formats

Suspension Notice, Suspension Order: *See Hold.*

System: A system is: (1) a collection of people, machines and methods organized to perform specific functions; (2) an integrated whole composed of diverse, interacting, specialized structures and sub-functions; and/or (3) a group of sub-systems united by some interaction or interdependence, performing many duties but functioning as a single unit.

Version, Record Version: A particular form of or variation from an earlier or original record. For electronic records, the variations may include changes to file format, metadata or content.

Vital Record: A record that is essential to the organization’s operation or to the reestablishment of the organization after a disaster.

Web site: A collection of Uniform Resource Indicators (URIs, including URLs (Uniform Resource Locators)) in the control of one administrative entity. May include different types of URIs (*e.g.*, file transfer protocol sites, telnet sites, as well as World Wide Web sites).

Appendix F: Working Group Participants, Members and Observers

Woods Abbott, Esquire
Raytheon Company
870 Winter Street
Waltham, MA 02451
abbott@raytheon.com
781-522-3304
Fax: 781-522-6467
Member

Whitney Adams
Cricket Technologies
12310 Pinecrest Road, Suite 300
Reston, VA 20191
whitneyadams@crickettechnologies.com
703-391-1020
Fax: 703-391-1338
Member

Sharon A. Alexander, Esquire
Jones Day
2727 North Harwood Street
Dallas, TX 75201
salexander@jonesday.com
214-969-4567
Fax: 214-969-5100
Participant

Dr. Jacqueline M. Algon
53 Pine Street
Milburn, NJ 07041
rennipsj@yahoo.com
973-762-8152
Participant

Thomas Y. Allman, Esquire
Mayer, Brown, Rowe & Maw LLP
190 South LaSalle Street
Chicago, IL 60603-3441
tyallman@mayerbrownrowe.com
312-701-8267
Fax: 312-706-8670
Steering Committee Member

Susan Avery
ARMA International
13725 W. 109th St., Suite 101
Lenexa, KS 66215
savery@arma.org
913-217-6023
Fax: 913-341-3742
Member

Jennifer V. Baker
Navigant Consulting, Inc.
175 West Jackson Street, Suite 500
Chicago, IL 60604
jbaker@navigantconsulting.com
312-583-5732
Fax: 312-583-5701
Member

Tom Barnett, Esquire
SPI Litigation Direct
1219 Sixteenth Avenue East
Seattle, WA 98112
t.barnett@spitech.com
Fax: 206-333-1962
Participant

Jason R. Baron, Esquire
Director of Litigation
National Archives and Records Admin.
8601 Adelphi Road, Suite 3110
College Park, MD 20740
jason.baron@nara.gov
301-837-1499
Fax: 301-837-0293
Observer

Jim Barrick
CaseCentral
760 Market Street, Suite 200
San Francisco, CA 94102
jbarrick@casecentral.com
415-989-2300 x-361
Fax: 415-989-2373
Member

Charles A. Beach, Esquire
Coordinator, Corporate Litigation
Exxon Mobil Corporation
5959 Las Colinas Boulevard
Irving, TX 75039-2298
charles.a.beach@exxonmobil.com
972-444-1466
Fax: 972-444-1435
Participant

Steven C. Bennett, Esquire
Jones Day
222 East 41st Street
New York, NY 10017-6702
scbennett@jonesday.com
212-326-3795
Fax: 212-755-7306
Participant

Helen Bergman Moure, Esquire
Preston Gates & Ellis
925 Fifth Avenue
Seattle, WA 98104
helenm@prestongates.com
206-370-8365
Fax: 206-623-7022
Member

Hon. Richard E. Best (Ret.)
Action Dispute Resolution Services
450 Sansome Street, Suite 1100
San Francisco, CA 94111
best@justice.com
Fax: 415-346-8453
Observer

Joanna Blackburn CRM
Union Pacific Railroad
1400 Douglas
Omaha, NE 68179
jsblackb@up.com
402-544-4352
Fax: 402-501-0132
Member

Alan F. Blakley, Esquire
Blakley Law Office
700 Southwest Higgins Avenue, Suite 200
Missoula, MT 59803
alan@blakley.net
406-829-3305
Fax: 406-829-2739
Member

Hildy Bowbeer, Esquire
Assistant Chief Intellectual Property Counsel-Litigation
Office of General Counsel
3M Company
3M Center, P.O. Box 33428
St. Paul, MN 55133-3428
hbowbeer@mmm.com
Member

Kevin F. Brady, Esquire
Skadden Arps Slate Meagher & Flom LLP
One Rodney Square
P.O. Box 636
Wilmington, DE 19899
kfbrady@skadden.com
302-657-3104
Fax: 888-329-8028
Member

Richard G. Braman, Esquire
Executive Director
The Sedona Conference
180 Broken Arrow Way South
Sedona, AZ 86351
tsc@sedona.net
866-860-6600
Fax: 928-284-4240
Observer, *ex-officio* on Steering Committee

Kerry Brennan, Esquire
Pillsbury Winthrop LLP
126 Oaks Road
Millington, NJ 07946
kbrennan@pillsburywinthrop.com
212-858-1723
Fax: 212-858-1500
Member

Christine M. Burns
Senior Consultant
Cohasset Associates, Inc.
1806 S. Cumberland Avenue
Park Ridge, IL 60068-5250
chris@chris-burns.com
847-698-7549
Fax: 847-698-0845
Participant

Paul E. Burns, Esquire
Steptoe & Johnson, LLP
201 E Washington Street, Suite 1600
Phoenix, AZ 85004
pburns@steptoe.com
602-257-5271
Fax: 602-257-5299
Member

Diane Carlisle CRM
ARMA International
13725 W. 109th Street, Suite 101
Lenexa, KS 66215
dcarlisl@arma.org
913-217-6010
Fax: 913-341-3742
Member

The Honorable John L. Carroll (Ret.)
Dean and Professor
Cumberland School of Law
Samford University
800 Lakeshore Drive
Birmingham, AL 35229
jlcarrol@samford.edu
205-726-2704
Fax: 205-726-4107
Observer

Barbara Caulfield, Esquire
Affymetrix, Inc.
3380 Central Expressway
Santa Clara, CA 95051
ba_caulfield@affymetrix.com
408-731-5000
Fax: 408-731-5394
Member

R. Noel Clinard, Esquire
Hunton & Williams LLP
951 East Byrd Street
Richmond, VA 23219
nclinard@hunton.com
804-788-8594
Fax: 804-344-8822
Participant

Andrew M. Cohen, Esquire
EMC Corporation
176 South Street
Hopkinton, MA 01748
cohen_andrew@emc.com
508-560-1726
Fax: 508-497-6915
Member

Matthew Cohen, Esquire
Skadden Arps Slate Meagher & Flom LLP
4 Times Square
New York, NY 10036
mcohen@skadden.com
212-735-2778
Fax: 917-777-2778
Member

Harald Collet
Oracle Corporation
500 Oracle Parkway, MS 50 P-4
Redwood Shores, CA 94065
harald.collet@oracle.com
650-607-6127
Fax: 650-607-6127
Member

Alfred W. Cortese, Jr., Esquire
Cortese PLLC
113 3rd Street, N.E.
Washington, DC 20002
awc@cortesepllc.com
202-637-9696
Fax: 202-637-9797
Member

Jim Coulson
Records Improvement Institute LLC
6 Stone Hill Road
Westboro, MA 01581
jim.coulson@rii-llc.com
508-836-5575
Fax: 508-836-5574
Member

Conor R. Crowley, Esquire
Much, Shelist, Freed, Denenberg, Ament &
Rubenstein, PC
191 North Wacker Drive, Suite 1800
Chicago, IL 60606-1615
ccrowley@muchshelist.com
312-521-2725
Fax: 312-521-2825
Participant

Tim Crouthamel, Esquire
State Farm Insurance Company
1 State Farm Plaza, B-3
Bloomington, IL 61776
tim.crouthamel.bedm@statefarm.com
309-766-7897
Fax: 309-766-6862
Member

M. James Daley, Esquire
Shook, Hardy & Bacon LLP
2555 Grand Blvd.
Kansas City, MO 64108
mjdaley@shb.com
816-474-6550
Fax: 816-421-5547
Participant

Jonathan A. Damon, Esquire
LeBoeuf, Lamb, Greene & MacRae, LLP
125 West 55th Street
New York, NY 10019-5389
jdamon@llgm.com
212-424-8333
Fax: 212-424-8500
Member

Hopkin M. Davies
Navigant Consulting, Inc.
1801 K Street, N.W., Suite 500
Washington, DC 20006
hdavies@navigantconsulting.com
202-973-2479
Fax: 202-973-2401
Member

Martha J. Dawson, Esquire
Preston, Gates & Ellis, LLP
925 Fourth Avenue, Suite 2900
Seattle, WA 98104-1158
marthad@prestongates.com
206-370-7980
Fax: 206-370-6043
Member

Robert J. C. Deane, Esquire
Borden Ladner Gervais LLP
200 Burrard Street, Suite 1200
Vancouver, B.C. V7X 1T2 Canada
rdeane@blgcanada.com
604-640-4250
Fax: 604-622-5876
Member

Trudy Downs
Merck & Co. Inc.
One Merck Drive, Suite WSIB-25
Whitehouse Station, NJ 08889
trudy_downs@merck.com
908-423-7437
Member

David E. Dukes, Esquire
Nelson, Mullins, Riley & Scarborough, LLP
Keenan Building, Third Floor
1330 Lady Street
Columbia, SC 29201-3332
ded@nmrs.com
803-255-9451
Fax: 803-256-7500
Participant

Robert A. Eisenberg, Esquire
CoreFacts, LLC
14030 Thunderbolt Place, Suite 700
Chantilly, VA 20151
reisenberg@corefacts.net
703-375-4340
Fax: 703-375-4343
Participant

Laura E. Ellsworth, Esquire
Jones Day
500 Grant Street, 31st Floor
Pittsburgh, PA 15219-2502
lellsworth@jonesday.com
412-394-7929
Fax: 412-394-7959
Participant

Colin C. Elrod
LECG
2000 Powell Street, Suite 600
Emeryville, CA 94608
celrod@lecg.com
510-985-6897
Fax: 510-653-9898
Member

Amor A. Esteban, Esquire
Drinker Biddle & Reath LLP
225 Bush Street, 15th Floor
San Francisco, CA 94104-4207
amor.esteban@dbr.com
415-591-7535
Fax: 415-397-1735
Participant

Jason B. Fliegel, Esquire
Mayer, Brown, Rowe & Maw LLP
190 South LaSalle Street
Chicago, IL 60603-3441
jfliegel@mayerbrownrowe.com
312-701-8839
Fax: 312-706-8115
Participant

Craig J. Freeman
Navigant Consulting
1801 K Street N.W., Suite 500
Washington, DC 20006
cfreeman@navigantconsulting.com
202-973-4549
Fax: 202-973-2401
Member

Peter Freeman, Esquire
Litigation Services
Ernst & Young
233 South Wacker Drive
Chicago, IL 60606
peter.freeman@ey.com
312-879-2926
Fax: 425-928-2125
Participant

Thomas E. Gaeta
Navigant Consulting
175 West Jackson Street, Suite 500
Chicago, IL 60604
tgaeta@navigantconsulting.com
312-583-5733
Fax: 312-583-5701
Member

Patrick J. Gennardo, Esquire
LeBoeuf Lamb Greene & MacRae, LLP
125 West 55th Street
New York, NY 10019
patrick.gennardo@lbgm.com
212-424-8136
Fax: 212-649-0901
Member

James E. Gordon
Pinkerton Consulting & Investigations
1055 Wilshire Blvd, Suite 1818
Los Angeles, CA 90017
james.gordon@ci-pinkerton.com
310-880-1431
Fax: 626-796-4415
Member

Ross M. Gotler
Practice Support Manager
Paul Weiss Rifkind Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
rgotler@paulweiss.com
212-373-2979
Fax: 212-492-0979
Member

David Grant, Esquire
Senior Associate General Counsel
Wal-Mart Stores, Inc.
702 S.W. 8th Street
Bentonville, AR 72712
david.grant@wal-mart.com
479-204-8662
Fax: 479-277-5991
Member

Ronald J. Green
Bank of America
NCI-014-14-04
200 South College Street
Charlotte, NC 28255-0001
ron.j.green@bankofamerica.com
704-387-2344
Fax: 704-387-0546
Member

Sherry B. Harris
Senior Case Management Specialist
Hunton & Williams LLP
951 East Byrd Street
Richmond, VA 23219
sharris@hunton.com
804-788-8200
Fax: 804-344-8822
Participant

Jeff Hatfield
Director
Jordan Lawrence Group
2630 Highway 109
St. Louis, MO 63040
jhatfield@jlggroup.com
636-527-1025
Fax: 636-527-1809
Member

Kris Haworth
Navigant Consulting, Inc.
One Market Plaza, 12th Floor
San Francisco, CA 94105
khaworth@navigantconsulting.com
415-356-7410
Member

Ted S. Hiser, Esquire
Jones Day
901 Lakeside Avenue
Cleveland, OH 44114-1190
tshiser@jonesday.com
216-586-7266
Fax: 216-579-0212
Participant

Geoffrey M. Howard, Esquire
Bingham McCutchen LLP
Three Embarcadero Center
San Francisco, CA 94111
geoff.howard@bingham.com
415-393-2485
Fax: 415-393-2286
Participant

David A. Irvin, Esquire
Womble Carlyle Sandridge & Rice
One West Fourth Street
Winston-Salem, NC 27101
dirvin@wcsr.com
336-721-3602
Fax: 336-733-8360
Participant

Conrad Jacoby, Esquire
General Counsel
Potomac Consulting Group
2300 4th Place
Dunn Loring, VA 22027
conrad.jacoby@potomac.com
703-869-1669
Fax: 703-783-8798
Participant

John H. Jessen
Chief Executive Officer
Electronic Evidence Discovery, Inc.
The Plaza at Yarrow Way
3933 Lake Washington Blvd.
Kirkland, WA 98033
jjessen@eedinc.com
206-369-3340
Fax: 206-343-0172
Steering Committee Member

Deborah A. Johnson
Tynan Consulting, LLC
622 Third Avenue, 31st Floor
New York, NY 10017
djohnson@tynanconsulting.com
212-722-6552
Fax: 917-658-6552
Member

Larry G. Johnson, Esquire
Legal Technology Group, Inc.
313 Avenue D
Shohomish, WA 98290
johnson@legaltechnologygroup.com
360-568-8131
Member

Jeffrey J. Joyce, Esquire
Jones Day
2727 N. Harwood Street
Dallas, TX 75201
jjjoyce@jonesday.com
214-969-3671
Fax: 214-969-5100
Participant

Sidney Kanazawa, Esquire
Van Etten Suzumoto & Becket LLP
1620 26th Street, Suite 6000 North
Santa Monica, CA 90404
skanazawa@vsblaw.com
310-315-8238
Fax: 310-315-8210
Participant

Dr. Hironao Kaneko
Tokyo Institute of Technology
Graduate School of Decision Science & Technology
2-12-1 Ookayama Meuro-ku (#Ookayama-W903)
Tokyo 1528552 Japan
kaneko@valdes.titech.ac.jp
81-3-5734-3566
Fax: 81-3-5734-3618
Member

Larry Kanter
Alvarez & Marsal
122 West Carpenter Freeway, Suite 200
Irving, TX 75039
lkanter@alvarezandmarsal.com
972-374-4206
Fax: 972-281-5831
Member

Anne Kershaw, Esquire
A. Kershaw PC, Attorneys & Consultants
303 South Broadway, Suite 100
Tarrytown, NY 10591
anne@akershaw.com
914-332-0438
Fax: 914-332-7912
Member

David Kittrell
1228 N.E. Brockman Place
Seattle, WA 98125
dkittrell@attbi.com
206-362-0751
Participant

Gene Klimov, Esquire
DOAR, Inc.
170 Earle Avenue
Lynbrook, NY 11563
gklimov@doar.com
516-823-3905
Fax: 516-823-4400
Member

Monica W. Latin, Esquire
Carrington Coleman Sloman & Blumenthal
200 Crescent Court, Suite 1500
Dallas, TX 75201
mlatin@ccsb.com
214-855-3075
Fax: 214-855-1333
Participant

R. Michael Leonard, Esquire
Womble Carlyle Sandridge & Rice
One West Fourth Street
Winston-Salem, NC 27101
mleonard@wcsr.com
336-721-3721
Fax: 336-733-8389
Participant

Pauline Levy, Esquire
McDonald's Corporation
2915 Jorie Boulevard, Dept. 065
Oak Brook, IL 60523
pauline.levy@mcd.com
630-623-5392
Fax: 630-623-7370
Member

A. John P. Mancini, Esquire
Mayer, Brown, Rowe & Maw LLP
1675 Broadway
New York, NY 10019
jmancini@mayerbrownrowe.com
212-424-8313
Fax: 212-424-8500
Participant

David G. Martin, Esquire
Medtronic, Inc.
710 Medtronic Parkway
Minneapolis, MN 55432
david.martin@medtronic.com
763-505-2682
Fax: 763-505-2685
Member

Wayne Matus, Esquire
Mayer, Brown, Rowe & Maw LLP
1675 Broadway
New York, NY 10019
wmatus@mayerbrownrowe.com
212-506-2122
Fax: 212-849-5922
Participant

J.J. McCracken, Esquire
Associate Counsel, Patent Attorney
Cooper Tire & Rubber Company
701 Lima Avenue
Findlay, OH 45840
jjmccracken@coopertire.com
419-424-4333
Fax: 419-424-7320
Participant

Gregory McCurdy, Esquire
Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
gmccurdy@microsoft.com
425-705-2724
Fax: 425-936-7327
Member

Stephanie Mendelsohn, Esquire
Reed Smith
1999 Harrison Street
Oakland, CA 94612
smendelsohn@reedsmith.com
510-466-6834
Member

James L. Michalowicz
Tyco International (US), Inc.
9 Roszel Road
Princeton, NJ 08540
jmichalowicz@tyco.com
609-720-4337
Fax: 609-720-4319
Participant

Bruce Miller
IBM Canada Ltd.
2670 Queensview Dr.
Ottawa, Ontario K2B 8K1 Canada
bmiller@ca.ibm.com
613-726-5624
Fax: 613-795-3072
Member

Denise M. Mineck, Esquire
Life Investors Insurance Company of America
4333 Edgewood N.E.
Cedar Rapids, IA 52499
dmineck@aegonusa.com
319-369-2048
Fax: 319-298-4980
Member

Timothy L. Moorehead, Esquire
Legal Department, Mail Code 5 West
BP America, Inc.
4101 Winfield Road
Warrenville, IL 60555
moorehtl@bp.com
630-821-2389
Fax: 630-821-3390
Steering Committee Member

Paul J. Neale, Jr.
DOAR
170 Earle Avenue
Lynbrook, NY 11563
pneale@doar.com
516-823-3997
Fax: 516-823-4400
Member

Kate Oberlies O'Leary, Esquire
Counsel-Litigation and Legal Policy
General Electric Company
3135 Easton Turnpike
Fairfield, CT 06431
kate.o'leary@corporate.ge.com
203-373-3520
Fax: 203-373-2523
Participant

Timothy M. Opsitnick, Esquire
Senior Partner and Founder
JurInnov Ltd.
29263 Clemens Road
Westlake, OH 44145
tim.opsitnick@jurinnov.com
440-835-3600
Fax: 440-835-3632
Participant

Robert D. Owen, Esquire
Fulbright & Jaworski, LLP
666 5th Avenue, 30th Floor
New York, NY 10103
rowen@fulbright.com
212-318-3070
Fax: 212-318-3400
Member

Laura Lewis Owens, Esquire
Alston & Bird LLP
One Atlantic Center
1201 W. Peachtree Street
Atlanta, GA 30309-3424
lowens@alston.com
404-881-7363
Fax: 404-881-7777
Participant

Robert W. Pass, Esquire
Carlton Fields
15 S. Monroe Street, Suite 500
Tallahassee, FL 32301-1866
rpass@carltonfields.com
850-513-3608
Fax: 850-222-0398
Participant

Richard Pearce-Moses
Director of Digital Government Information
Arizona State Library, Archives and Public Records
1700 W. Washington, Suite 200
Phoenix, AZ 85007
rpm@lib.az.us
602-542-4035
Fax: 602-542-4972
Observer

Vivian Polak, Esquire
Leboeuf, Lamb Greene & MacRae
125 West 55th Street
New York, NY 10019
vpolak@llgm.com
212-424-8289
Participant

Ashish S. Prasad, Esquire
Mayer, Brown, Rowe & Maw LLP
190 South LaSalle Street
Chicago, IL 60603-3441
aprasad@mayerbrownrowe.com
312-701-8438
Fax: 312-706-8670
Participant

Michael J. Prounis
Chief Executive Officer
Evidence Exchange
21 Penn Plaza, Suite 1500
New York, NY 10001
michael.prounis@evidenceexchange.com
212-594-2500 x314
Fax: 212-594-2803
Participant

Charles R. Ragan, Esquire
Pillsbury Winthrop LLP
50 Fremont Street
San Francisco, CA 94105
chuck.ragan@pillsburywinthrop.com
415-983-1709
Fax: 415-983-1200
Participant

Jonathan M. Redgrave, Esquire
Jones Day
51 Louisiana Avenue, N.W.
Washington, DC 20001-2113
jredgrave@jonesday.com
202-879-3483
Fax: 202-626-1700
Steering Committee Chair

Dan Regard, Esquire
Managing Director
LECG, LLC
1725 Eye Street NW, Suite 800
Washington, DC 20006
dregard@lecg.com
202-973-6481
Fax: 202-550-4764
Participant

Mark V. Reichenbach
Director of Litigation Support
Milberg Weiss Bershad & Schulman LLP
One Pennsylvania Plaza
New York, NY 10119-0165
mreichenbach@milbergweiss.com
646-733-5675
Fax: 212-273-4462
Participant

Mary K. Riley
Bank of America
NCI-014-14-04
200 South College Street
Charlotte, NC 28255-0001
mary.riley@bankofamerica.com
704-386-6323
Fax: 704-386-4314
Member

Louise A. Rinn, Esquire
Union Pacific Railroad Company
1416 Dodge Street, Suite 830
Omaha, NE 68179
larinn@up.com
402-271-3309
Fax: 402-271-7107
Member

Paul M. Robertson, Esquire
Bingham McCutchen LLP
50 Federal Street
Boston, MA 02110
paul.robertson@bingham.com
617-951-8862
Fax: 617-951-8736
Participant

Herbert L. Roitblat, Ph.D.
Executive Vice President, Chief Scientist
DolphinSearch, Inc.
474 E. Main Street
Ventura, CA 93001
herb@dolphinsearch.com
805-585-2102 x124
Fax: 805-648-7150
Participant

James E. Rooks, Jr., Esquire
Center for Constitutional Litigation, P.C.
1050 31st Street, N.W.
Washington, DC 20007-4499
jim.rooks@cclfirm.com
202-944-2841
Fax: 202-588-7795
Member

Andrea D. Rose, Esquire
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, DC 20015
arose@crowell.com
202-624-2557
Fax: 202-628-5116
Participant

John J. Rosenthal, Esquire
Howrey Simon Arnold & White
1299 Pennsylvania Avenue, N.W.
Washington, DC 20004-2402
rosenthalj@howrey.com
202-383-7234
Fax: 202-383-6610
Member

Leigh R. Schachter, Esquire
Legal & External Affairs Department
Verizon Wireless
180 Washington Valley Road
Bedminster, NJ 07921
leigh.schachter@verizonwireless.com
908-306-7597
Fax: 908-306-7766
Participant

Gregory P. Schaffer, Esquire
Alltel Corporation
One Allied Drive, Mail Stop B5F10C
Little Rock, AR 72202
gregory.schaffer@alltel.com
501-905-2952
Fax: 501-905-1116
Participant

The Honorable Shira A. Scheindlin
United States District Judge
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street, Room 1050
New York, NY 10007-1312
shira_a_scheindlin@nysd.uscourts.gov
212-805-0246
Fax: 212-805-7920
Observer

David Schieferstein, Esquire
Philip Morris USA
615 Maury Street, LSC-GOB
Richmond, VA 23224
david.schieferstein@pmusa.com
804-484-8804
Fax: 914-272-0607
Member

Eric J. Schwarz
Legal Technology Services
Ernst & Young LLP
2121 San Jacinto Street, Suite 1400
Dallas, TX 75201
eric.schwarz@ey.com
214-969-8491
Fax: 214-969-8754
Member

Kenneth Shear, Esquire
SPI Litigation Direct
1219 Sixteenth Avenue East
Seattle, WA 98112
k.shear@spitech.com
206-235-3374
Fax: 206-333-1962
Participant

Sonya L. Sigler
Cataphora
1400 Bridge Parkway, Suite 203
Redwood City, CA 94065
ssigler@cataphora.com
650-622-9840, ext. 604
Fax: 650-622-9844
Member

Peter B. Sloan, Esquire
Blackwell Sanders Peper Martin, LLP
2300 Main Street, Suite 1000
Kansas City, MO 64108
psloan@blackwellsanders.com
816-983-8150
Fax: 816-983-8080
Participant

James A. Snyder
BKD, LLP
120 West 12th Street
Kansas City, MO 64106
jsnyder@bkd.com
816-701-0260
Fax: 816-221-6380
Member

Kirke Snyder
LECG, LLC
201 Mission Street, Suite 700
San Francisco, CA 94105
kirke.synder@lecg.com
303-819-9946
Member

George J. Socha, Jr., Esquire
Socha Consulting LLC
1374 Lincoln Avenue
St. Paul, MN 55105
george@sochaconsulting.com
651-690-1739
Fax: 651-846-5920
Participant

Ariana J. Tadler, Esquire
Milberg Weiss Bershad & Schulman LLP
One Pennsylvania Plaza, 48th Floor
New York, NY 10119
atadler@milbergweiss.com
212-946-9453
Fax: 212-868-1229
Member

Judy Van Dusen, President
VanKorn Group, Limited
125 Charrington Court
Beverly Hills, MI 48025
jvanduse@peoplepc.com
248-594-9311
Fax: 248-594-9351
Participant

Lori Ann Wagner, Esquire
Faegre & Benson LLP
90 South Seventh Street
Minneapolis, MN 55402-3901
lwagner@faegre.com
612-766-7910
Fax: 612-766-1600
Participant

Robert F. Williams
Cohasset Associates, Inc.
3806 Lake Point Tower
505 North Lake Shore Drive
Chicago, IL 60611
robertwilliams@cohasset.com
312-527-1550
Fax: 312-527-1552
Participant

Scott L. Winkelman, Esquire
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, DC 20015
swinkelman@crowell.com
202-624-2972
Fax: 202-628-5116
Member

Thomas P. Wisinski, Esquire
Haynes & Boone LLP
901 Main Street, Suite 3100
Dallas, TX 75202
thomas.wisinski@haynesboone.com
214-651-5889
Fax: 214-200-0722
Member

Kenneth J. Withers, J.D.
Research Associate
Federal Judicial Center
One Columbus Circle, N.E.
Washington, DC 20002-8003
kwithers@fjc.gov
202-502-4065
Fax: 202-502-4199
Observer

Edward C. Wolfe, Esquire
Legal Staff MC 482-026-601
General Motors Corp.
400 Renaissance Center, P.O. Box 400
Detroit, MI 48265
edward.c.wolfe@gm.com
Fax: 248-267-4399
Participant

Gregory B. Wood, Esquire
Fulbright & Jaworski LLP
865 Figueroa Street, Suite 2900
Los Angeles, CA 90017
gwood@fulbright.com
213-892-9235
Fax: 213-680-4518
Member

Susan B. Wortzman, Esquire
Lerners LLP
130 Adelaide Street West, Suite 2400
Toronto, Ontario, M5H 3P5 Canada
swortzman@lerners.ca
416-601-2365
Fax: 416-867-2423
Participant

Brian Wycliff
PricewaterhouseCoopers LLP
2001 Ross Avenue, Suite 1800
Dallas, TX 75201-2997
brian.wycliff/us/fas/pwc@americas.us
646-471-3380
Fax: 813-329-1163
Member

Patrick E. Zeller, Esquire
Seyfarth Shaw LLP
55 E. Monroe Street, Suite 4200
Chicago, IL 60603-5803
pzeller@seyfarth.com
312-269-8516
Fax: 312-269-8869
Member

Appendix G: Background on The Sedona ConferenceSM & its Working Group Series

The Sedona ConferenceSM is a nonprofit, 501(c)(3) research and education institute dedicated to the advancement of law and policy in the areas of antitrust, complex litigation and intellectual property rights. The Sedona ConferenceSM meets that goal in part through the stimulation of ongoing dialogues among leaders of the bench and bar in each area under study. To that end, The Sedona ConferenceSM hosts three major conferences each year in unique, retreat-like settings. Fifteen of the nation's finest jurists, attorneys, academicians and others prepare materials for, and lead the discussions during, each two-day conference.

What sets our conferences apart from all other legal study programs is the quality and intensity of the dialogues, generating cutting-edge analyses. To ensure the proper environment for this level of interaction, each conference is strictly limited to 45 experienced participants in addition to the faculty (who remain and participate throughout the entire conference). The best of the written materials are then published annually in *The Sedona Conference Journal*, which is distributed on a complimentary basis to courthouses and public law libraries around the country and by subscription to others. The *Journal* is also available on Westlaw and is listed in H.W. Wilson's *Index to Legal Periodicals*. The Sedona ConferenceSM has received broad and strong accolades from participants since its inception. (See "Raves" section of our website).

The Sedona ConferenceSM Working Group Series is designed as a bridge between our advanced legal conferences and an open think-tank model that can produce authoritative works designed to stimulate the development of the law. Working Groups in the Series begin with the same high caliber of participants as our regular season conference faculty and participants. The total "active" Group, however, is limited to less than 40 (though anyone can join The Working Group Membership Program to gain access to an individual Working Group's work area). The Group circulates ideas, questions, developments and references ahead of a face-to-face meeting. At the meeting, decisions are made regarding the form, direction and content of the output, teams are assembled, and the drafting gets underway. Following a few months of work, a public comment version is then published and subjected to peer review before the "final" work product is published. Consistent with our mission, all "public comment" drafts and completed Working Group publications are available for free download for individual use from our website. For details on reprint permission, see the "publications" area of our website or contact us at tsc@sedona.net.

Funding for The Sedona ConferenceSM comes from individuals, law firms and corporations in the form of conference sponsorships and registration fees. Funding for the 2003-04 Working Group Addressing Electronic Document Retention & Production comes from individual Working Group membership fees, as well as sponsorships provided by *Electronic Evidence Discovery, Inc.*, *Jones Day*, *Mayer Brown Rowe & Maw LLP* (Founding Sponsors), and *ARMA International*, *Carrington Coleman Sloman & Blumenthal*, *EMC Corporation*, *Ernst & Young*, *FTI Consulting*, *Navigant Consulting, Inc.*, *PricewaterhouseCoopers* and *SPI Litigation Direct* (Supporting Sponsors).

If you are interested in contributing to the efforts of The Sedona ConferenceSM or any of its Working Groups, or if you want more information about The Sedona ConferenceSM generally, you can visit www.thesedonaconference.org or contact the Executive Director, Richard G. Braman, at the following address:

The Sedona Conference
180 Broken Arrow Way South
Sedona, Arizona 86351

Voice: 1.866.860.6600 Toll Free or 1.928.284.2698
Facsimile: 1.928.284.4240
E-mail: tsc@sedona.net

wgsSM

Copyright © 2004,
The Sedona ConferenceSM

Visit www.thesedonaconference.org



Cover printed on 50% sugar cane
and 50% recycled fiber.