CREW | citizens for responsibility and ethics in washington

Record Chaos:

The Deplorable State of Electronic Record Keeping in the Federal Government

www.citizensforethics.org

TABLE OF CONTENTS

INTRODUCTION

The importance of maintaining electronic records in this era of government secrecy has never been greater. Email in particular, that most ubiquitous form of communication, plays in increasingly important role in explaining what our government has done and why. Yet even though information technology is advancing by leaps and bounds, the federal government has fallen woefully behind in managing its electronic records. Citizens for Responsibility and Ethics in Washington (CREW), with the assistance of OpenTheGovernment.org, has studied the issue of electronic record keeping in the federal government and prepared this report to identify the most serious government failings and how they can be addressed to bring the federal government into the 21st century.

We looked at the issue from two different perspectives. First, we examined the legal frameworks that guide federal agencies and the private sector in managing their electronic record keeping systems. Analyzing trends in civil litigation, we were able to identify vulnerabilities and potential liabilities that non-complying agencies are likely to face. Second, we looked at specific agency policies and practices to ascertain just how far off course the federal government is. The results confirmed our everyday experience, that the vast majority of federal agencies have made little or no progress in effectively managing their electronic records.

CREW's report is by no means comprehensive, as we had limited means to monitor actual agency practices. Yet across the board our results were consistent and sounded a loud and clear alarm: the federal government is not effectively managing one of its most valuable resources, information. As a result, the public is being deprived of access to government records that shine a public light on what the government is doing and ensure accountability for our government's actions.

The situation is all the more disturbing given the ready availability of off-the-shelf and easily customized software and technology tools and the wealth of guidance that groups such as the Sedona Conference have offered. In this arena there is an ever widening gap between the practices in the private sector -- where companies have embraced technology -- and the practices in the federal government -- where agencies have repudiated or ignored technology in favor of outdated paper record keeping systems and practices.

It is our hope that by highlighting where the federal government has gone wrong in its mismanagement of electronic records, federal agencies and Congress will be spurred to act to give agency record keeping the priority it deserves.

METHODOLOGY

To determine federal agency compliance with electronic record keeping obligations, CREW submitted Freedom of Information Act (FOIA) requests to a variety of cabinet-level agencies seeking their written guidance and policies on electronic record keeping within their agencies. CREW also submitted FOIA requests to a handful of agencies on discrete topics to test the agencies' ability to locate and produce responsive email records. To ascertain actual agency practices, CREW, with the assistance of OpenTheGovernment.org, prepared an on-line survey

on email record keeping practices and policies that it submitted to over 400 agency records managers. CREW received 87 partial or complete responses over a three-week period. On another front, CREW collected legal authorities that guide and compel electronic record keeping in both the federal government and the private sector. We looked at trends in civil litigation as the best indicator of practices that fall outside the norm and are most likely to result in sanctions for inadequate record keeping practices.

SUMMARY OF FINDINGS

The research for this report and most especially our survey make clear that the federal government is not managing its electronic records effectively, despite the fact that the National Archives and Records Administration (NARA) has been issuing guidance and standards for the past decade. Agencies are not taking advantage of a growing body of commercially available products and lag far behind their private-sector counterparts. Responsibility for this state of affairs is shared by both the agencies and NARA. The federal government simply cannot afford to continue ignoring its electronic record keeping obligations.

Our research exposed four overarching problems:

1. Lack Of Progress

Survey responses and agency written record keeping policies reveal that the vast majority of federal agencies treat electronic records like paper records by following a print-and-save policy. We have not found a single federal agency policy that mandates an electronic record keeping system agency-wide.[1] At best discrete agency components appear to use electronic record keeping for only some of their agency records.

2. Widespread Confusion And Lack of Understanding Of Record Keeping Obligations

Survey responses confirm that even knowledgeable agency employees lack a basic understanding of their record keeping obligations and how they can be satisfied. Written policies and guidelines within individual agencies are often inconsistent, confusing or outright misleading. This lack of understanding correlates directly to a lack of compliance with record keeping obligations.

3. Systemic Lack Of Meaningful Oversight

Agencies are not held accountable for complying with mandatory record keeping obligations. The blame falls most squarely on NARA, which has the statutory obligation to not only promulgate standards and guidelines for federal agency records management, but also to

[1] Six respondents to our survey, discussed *infra*, said their agencies preserved emails on an electronic record keeping or electronic records management system, but we do not know if this practice is agency-wide or just within an agency subcomponent or office.

assist agencies in applying the standards to records in their custody.[2] NARA is not fulfilling this statutory mandate, electing instead a passive role limited to providing guidance only with no agency follow-through. NARA has abandoned its previous practice of conducting annual audits of agency compliance and proclaimed publicly that the responsibility rests first and last with individual federal agencies.

4. Exposure To Liability In Other Legal Contexts

The failure of the federal government to adequately meet its electronic record keeping obligations has exposed it to potential liability in a host of other contexts. Inadequate electronic record keeping also means inadequate compliance with the FOIA and other information access statutes. Agencies' ability to meet their litigation obligations is seriously hampered by their inability to deal effectively with electronic records. At best it is a disaster waiting to happen; at worst, the disaster has already occurred.

[2] 44 U.S.C. §§ 2904(c)(1) and 2905(a).

GLOSSARY OF TERMS

Agencies are big and complex and produce a variety of records in a variety of different formats. For example, the IRS alone runs 630 different computer systems.[3] These complexities and differing systems present major hurdles to agencies seeking a records management system that can accommodate all these formats. To better understand the record keeping obligations and challenges that agencies face, we offer the following glossary of terms:

Records

The Federal Records Act (FRA) defines records to include "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them."[4]

Records Disposition

Records disposition refers to what an agency does with its records once it no longer needs them, and encompasses both temporary and permanent records. Permanent records are those that have "significant value," which the federal government must preserve indefinitely.[5] Temporary records do not have long-term value and are scheduled for disposal (i.e. destruction) either immediately or after a set period of time or a certain event.[6] General Records Schedules (GRS) published by NARA determine the schedule for disposition of specific categories of records common to several agencies. If an agency-specific record is not covered by a GRS its disposition is governed by an agency record schedule.[7]

Electronic Records

"Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks.

---

[3] Joab Jackson, *Records Managers see value of Enterprise Architecture*, Federal Computer Week, March 7, 2008 (Exhibit 1).

[4] 44 U.S.C. § 3301

[5] *Frequently Asked Questions about Records Scheduling and Disposition*, available at http://www.archives.gov/records-mgmt/faqs/scheduling.html (Exhibit 2).

[6] Id.

[7] Id.

Unless otherwise noted, these [electronic records] requirements apply to all electronic information systems, whether on microcomputers, minicomputers, or main-frame computers, regardless of storage media, in network or stand-alone configurations. Electronic records include federal records created by individuals using electronic mail applications.[8]

Backup Tapes and Recycling

Backup tapes, often referred to as disaster recovery tapes, are "[p]ortable media used to store data that is not presently in use by an organization to free up space but still allow for disaster recovery."[9] Backups are commonly used as a last backstop for retention of email messages. As backup tapes become full they are "recycled," which the Sedona Conference defines as

> a process whereby an organization's backup tapes are overwritten with new backup data, usually on a fixed schedule (e.g., 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).[10]

Traditional Records Management

Traditionally records management is defined as the "systematic control of the creation, maintenance, use and disposition of records."[11] For federal agencies, this usually means organizing physical files that fit the definition of a federal record together in what is known as a record series. A series is a group of records that all relate to the same subject, function or activity of an agency.[12]

Electronic Records Management

---

[8] 36 C.F.R. § 1234

[9] See *Best Practices Recommendations & Principles for Addressing Electronic Document Production* (July 2005), available at http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf (hereinafter "Sedona Best Practices") (Exhibit 3).

[10] Id.

[11] *Context for Electronic Records Management*, available at http://www.archives.gov/records-mgmt/initiatives/context-for-erm.html (hereinafter "Context for Electronic Records Management") (Exhibit 4).

[12] *Frequently Asked Questions about Federal Records Management*, available at http://www.archives.gov/records-mgmt/faqs/federal.html#series (Exhibit 5).

NARA defines electronic records management (ERM) as "using automated techniques to manage records regardless of format. Electronic records management is the broadest term that refers to electronically managing records on varied formats, be they electronic, paper, microform, etc."[13] When referring specifically to the electronic management of electronic records NARA uses the term electronic record keeping or ERK.[14]

Email Records and Metadata

Email records include a variety of information, known as metadata, that must be preserved along with the body of an email.[15] Metadata includes the names of the sender and addressee(s) and date the message was sent. Nicknames, codes and distribution lists are not adequate for this purpose. Agencies are required to make sure email records have this data "in order for the context of the message to be understood."[16]

DOD 5015.2-STD

Department of Defense 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, is a criteria by which record management applications (RMAs) are tested by the Joint Interoperability Test Command of the Department of Defense. DOD 5012.2-STD provides a baseline standard that RMAs must meet to be used by DOD components.[17] Since it was endorsed by NARA the standard is also now the baseline for RMAs across the federal government.[18]

There are currently 48 products certified as compliant with DOD 5015.2,[19] but NARA warns that these products are not "out-of-the-box" solutions. NARA does not "endorse specific commercial

---

[13] *Context for Electronic Records Management* (emphasis added) (see Exhibit 4).

[14] Id.

[15] Armstrong v. Executive Off. of the President, 1 F.3d 1274 (D.C. Cir. 1993).

[16] 36 C.F.R. § 1234.24(a)(1).

[17] U.S. Dept. of Defense, Electronic Records Management Software Applications Design Criteria Standard, Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, DOD 5015.2-STD, April 25, 2007 (Exhibit 6).

[18] National Archives and Records Administration, NARA Bulletin 2003-03, Endorsement of DoD Electronic Records Management (RMA) Design Criteria Standard, version 2 (2003) (Exhibit 7).

[19] *DoD 5015.2-STD Compliant Product Registers*, available at http://jitc.fhu.disa.mil/recmgt/register.html (hereinafter "DOD Compliant Product Register") (Exhibit 8).

products”[20] and agencies will need to integrate RMAs into existing systems and retrain employees.[21] DOD 5015.2-STD is not a catch all solution to records management, but a very good tool for agencies and commercial suppliers.

[20] Memorandum from Michael L. Miller, Director, Modern Records Programs, NWM 04.2001 (Nov. 27, 2000) (hereinafter “Miller Memo 2000") (Exhibit 9).

[21] Memorandum from Michael L. Miller, Director, Modern Records Programs, NWM 03.99, (Nov. 19, 1998) (hereinafter “Miller Memo 1998") (Exhibit 10).

LEGAL FRAMEWORK FOR FEDERAL AGENCIES[22]

1. The Federal Records Act

Federal agency record keeping obligations stem from the Federal Records Act, a collection of statutes that governs the creation, management and disposal of federal records.[23] Among other things, the FRA ensures "[a]ccurate and complete documentation of the policies and transactions of the Federal Government," as well as "judicious preservation and disposal of records."[24]

To fulfill this purpose, the FRA requires the head of each agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[25] Under the FRA, each agency must also "establish and maintain an active, continuing program for the economical and efficient management of the records of the agency,"[26] and must "establish safeguards against the removal or loss of records" the agency head determines are necessary and required by regulations of the archivist.[27]

Penalties for noncompliance under the FRA are limited to the unlawful removal or destruction of federal records. Violations can result in fines, up to three years in prison, or both.[28] While rare, instances of enforcement of this provision (section 2071) are not without precedent.[29]

Overall responsibility for federal government records management rests with NARA.[30]

---

[22] This section is not intended to be comprehensive, but rather identifies some of the most pertinent authorities governing federal agency record keeping.

[23] See generally 44 U.S.C. §§ 2101 et seq., 2901 et seq., 3010 et seq., and 3301 et seq.

[24] 44 U.S.C. § 2902.

[25] Id. at § 3101.

[26] Id. at § 3102.

[27] Id. at § 3105.

[28] 18 U.S.C. § 2071(a).

[29] See, e.g., United States v Salazar, 455 F.3d 1022 (9th Cir. 2006) (affirming defendant's conviction for destroying documents filed and deposited with the Immigration and Naturalization Service).

[30] 44 U.S.C. § 3303a.

Created in 1984, NARA is headed by the national archivist,[31] who administers the provisions of the FRA and may authorize an agency to dispose of records that the agency no longer needs and that do not have "sufficient administrative, legal, research, or other value to warrant their continued preservation by the Government."[32]

The archivist also has an affirmative duty to guide and assist federal agencies to ensure the adequate and proper documentation of their policies and transactions.[33] Toward that end, the archivist must establish standards and guidelines for federal agency records management, standards for an agency to selectively retain records of value and must assist agencies in applying those standards to records in their custody.[34]

2. NARA Regulations and Policies

NARA specifies that the agency bears the responsibility to "[d]evelop and implement an agency wide program for the management of all records . . ."[35] According to NARA, agencies must also provide record management training for employees.[36] These responsibilities are rooted in the FRA, which requires each agency head to maintain an active records management program that provides for effective controls over the creation and use of federal records and that ensures the application of the archivist's standards and procedures for the preservation of federal records.[37]

For those agencies that use paper files for record keeping, NARA requires that the agencies "print their electronic mail records and the related transmission and receipt data."[38] For those agencies using electronic record keeping systems, NARA requires that records be easy to retrieve and be accessible to individuals who have a business need for them.[39] Our research shows that the "print and file" practice dominates the federal government, even though it is a

---

[31] 36 C.F.R. § 1220.2.

[32] Id. at § 3303a(a).

[33] Id. at § 2904(a).

[34] Id. at §§ 2904(b), (c)(1), 2905(a).

[35] 36 C.F.R. § 1234.10(a).

[36] 36 C.F.R. § 1234.10(e).

[37] 44 U.S.C. § 3102.

[38] 36 C.F.R. § 1234

[39] *Examples of System Functions for Electronic Recordkeeping (ERK) and Electronic Records Management (ERM)*, available at http://www.archives.gov/records-mgmt/policy/prod6b.html (Exhibit 11).

demonstrably flawed electronic record keeping method in the modern federal work place. Given the volume of e-mail records that a typical agency creates and receives, "[i]t's generally a disaster waiting to happen" in the words of one expert.[40]

NARA has taken some steps to try and move agencies away from antiquated paper records system. In 1998, NARA endorsed DOD 5015.2- STD as an acceptable standard for records management software.[41] In addition, NARA has identified nine reasons, separate and apart from formal record keeping regulations and statutes, why agencies should adopt electronic record keeping (ERK) practices.[42] Specifically, ERK has the following benefits:

> 1. It allows agencies to "manage information as an asset, rather than a liability";
>
> 2. Records in legacy systems will be accessible in the future;
>
> 3. ERK reduces the costs of complying with the Freedom of Information Act (FOIA) and discovery;
>
> 4. ERK facilitates resolution of contract disputes;
>
> 5. By reducing the need for both a paper and electronic record keeping system ERK results in long-term cost savings;
>
> 6. ERK improves productivity;
>
> 7. ERK ensures integrity and security of critical records;
>
> 8. Agencies that implement ERK now will minimize the future impact on their IT infrastructures; and
>
> 9. "ERK increases the likelihood of success of any records migration/preservation strategy."[43]

In addition, from 2003 to 2006, NARA published a series of six guidance documents, based on the experience of the Environmental Protection Agency, to aid agencies in selecting an electronic records management system. The guidance addresses: (1) capital planning and

---

[40] Aliya Sternstein, *Probes Highlight Problems with Agencies' E-mail Storage*, Government Executive, May 3, 2007 (Exhibit 12).

[41] See Miller Memo 1998.

[42] See *Why Federal Agencies Need to Move Towards Electronic Recordkeeping*, available at http://www.archives.gov/records-mgmt/policy/prod1afn.html (Exhibit 13).

[43] Id.

investment control; (2) determining agency-unique requirements; (3) evaluating commercial applications; (4) governance structure; (5) developing a pilot program; and (6) a summary of lessons learned.[44] Essentially, NARA has provided a step-by-step guide for agencies committed to implementing agency-wide electronic records management.

In sum, NARA has provided a wealth of resources for federal agencies outlining the reasons for improving records management and, in some cases, providing step-by-step guides to implementing new technologies. Notwithstanding this guidance, agencies are not taking advantage of available technologies and lag far behind the private sector in the area of electronic record keeping. In addition, NARA has done little, if anything, to follow through with agencies. In order to move record keeping in the federal government into the 21st century, NARA needs to assume a much more active role to fulfill its statutory responsibilities.

3. Other Statutes That Bear On Agency Record Keeping Practices

A series of other statutes and legal authority bear on the record keeping obligations of federal agencies. These include amendments to the FOIA, enacted in 1996, that require agencies to provide electronic access to certain agency records, essentially creating "electronic reading rooms." 5 U.S.C. § 552(a)(2)(D). The amendments also require that upon request agencies must provide records to a FOIA requester electronically as long as "the record is readily reproducible by the agency in that form or format." Id. at § 552(a)(3)(B). The U.S. Department of Justice, in its bi-annual Freedom of Information Act Guide, has stated that

> [g]iven 'that computer-stored records, whether stored in the central processing unit, on magnetic tape, or in some other form, are records for the purposes of the FOIA,' agencies should endeavor to use advanced technology to satisfy existing or potential FOIA demands most efficiently – including through 'affirmative' electronic disclosures.

(citations omitted).[45]

A presidential decision directive on "Critical Infrastructure Assurance"[46] highlights the significance of electronic systems and the need to make them secure as part of the nation's critical infrastructure. The directive, issued in 1998, requires each agency to reduce its exposure to new threats and ensure it can protect its information systems from intentional acts by 2003. As NARA has explained, "[a]ny attack on a networked information system also affects the

---

[44] *Enterprise-Wide ERM*, available at http://www.archives.gov/records-mgmt/initiatives/enterprise-erm.html (Exhibit 14).

[45] U. S. Department of Justice, Freedom of Information Act Guide, p. 126 (March 2007 Edition) (Exhibit 15).

[46] See Presidential Decision Directive 63 (PDD-63).

agency's infrastructure. For this reason, security of electronic records . . . must be considered when establishing an ERK."[47]

The Government Paperwork Elimination Act, signed into law in 1998, requires federal agencies by October 21, 2003, to accept information electronically from individuals and entities that interact with the federal government, and "to maintain records electronically, when practicable."[48] The Act also affirms the legal effect of electronic signatures. The Office of Management and Budget issued implementing guidance intended to "foster[] a successful transition to electronic government . . ."[49] That guidance also addresses explicitly NARA's role in the area of electronic records management by mandating that NARA "develop, in consultation with the agencies and OMB, policies and guidance on the management, preservation, and disposal of Federal records associated with electronic government transactions . . ."[50]

The courts also have weighed in on some of the responsibilities agencies bear when dealing with electronic records. For example, in Armstrong v. Executive Off. of the President, 1 F.3d 1274 (D.C. Cir. 1993), the U.S. Court of Appeals for the D.C. Circuit affirmed the status of the electronic version of a paper record, including the metadata in the electronic version, as a record. Under the court's ruling, each agency that does not have an electronic record keeping system must print out the entire electronic record, with all of its imbedded text of substantive information (the metadata) and file the paper copy in the agency's paper record keeping system. Although the courts have never mandated that agencies adopt electronic record keeping systems, at least one court expressed the view in 1999 that "[i]t may well be time" for agencies to take "the next step of establishing electronic recordkeeping systems."[51]

4. OMB Guidance

On March 31, 2008, the Office of Management and Budget (OMB) circulated a memorandum to agency chief information officers highlighting tools available to move agencies towards electronic records management.[52] In an effort to encourage agencies to improve their information management, the memorandum explains the benefits of "strategic management of

---

[47] *Why Federal Agencies Need to Move Towards Electronic Recordkeeping* at p. 1 (see Exhibit 13).

[48] OMB, Implementation of the Government Paperwork Elimination Act, p. 2, available at http://www.whitehouse.gov/omb/fedreg/gpea2html (last visited April 4, 2008) (Exhibit 16).

[49] Id. at p. 2.

[50] Id. at p. 7.

[51] Public Citizen v. Carlin, 184 F.3d 900, 910 (D.C. Cir. 1999).

[52] Memorandum from Karen S. Evans, Administrator, Office of Electronic Government and Information technology, Executive Office of the President, Office of Management and Budget, M-08-15 (March 31, 2008) (Exhibit 17).

government information resources." These include "ensur[ing] public accountability," "guard[ing] the legal and financial rights of the government and public" and "promot[ing] public access to information."[53] The memorandum also highlights several available guidance documents;[54] missing is any time-line for compliance or suggested penalties for agency non-compliance.

Moreover, as some records management experts have pointed out, there is only one available records management product for the SmartBuy program that OMB advocates, and that program does not have archiving capabilities.[55]

THE SEDONA CONFERENCE

The Sedona Conference is an organization created to bring together "in conferences and mini-think tanks (Working Groups)" "leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights." Its stated purpose is to "engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way."[56] The Conference seeks to produce "output that is balanced, authoritative, and of immediate benefit to the Bench, Bar and general public" by the Conference's working groups, peer review process and its open Working Group Membership Program.[57]

Over time, the Sedona Conference has grown in stature and been accorded increased acceptance in the legal arena. Its guidance on electronic information serves the public and private sectors alike, and in particular should serve as a paradigm for agency heads, chief information officers and NARA staff when making records management decisions for the federal government.

The Sedona Conference has generated a number of guidance documents; below we highlight two of particular interest and usefulness.

1. The Sedona Guidelines On Managing Information and Records in The Electronic Age

---

[53] Id.

[54] Id.

[55] Joab Jackson, *OMB Issues Records Management Guidance*, Tech Blog, Government Computer Week, April 11, 2008, available at http://www.gcn.com/blogs/tech/46123.html#trackback (Exhibit 18).

[56] *TSC Mission,* available at http://www.thesedonaconference.org/content/tsc_mission/show_page_html (Exhibit 19).

[57] Id.

The Sedona Guidelines on Managing Information and Records in The Electronic Age[58] approach electronic information from a legal, records management and information technology perspective. The authors acknowledge that what they have written will not harmonize perfectly the varied aspects of electronic information, nor are the guidelines rigid standards for effectively handling electronic records. The guidelines also take a nuanced approach to electronic information management rather than the technology "silver bullet" that some in government advocate,[59] which is probably warranted given the size and varied functions of the federal government.

More specifically, the Sedona Conference has identified five over-arching "guidelines" that should govern management of electronic information.[60]

First, an organization should have "reasonable policies and procedures for managing its information and records."[61] This requires a significant investment of human and financial capital, what the Sedona Conference has called "an intelligent blend of people, processes and technology,"[62] particularly because there is not one simple solution.

While the Sedona guidelines focus on the private sector, they are directly analogous to the federal government, which must also deal with oversight requirements, information requests and legal discovery requirements. Yet unlike the trend in the private sector to elevate the importance of information, federal agencies are pushing information-related issues farther down the agency management ladder.[63]

Second, an organization's records management policies and procedures "should be realistic, practical and tailored to the circumstances of the organization."[64] The Sedona Conference encourages organizations to adopt a flexible approach in creating an information

---

[58] Charles R. Ragan et al., ed., The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age. (2005), available at http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf ("Sedona Guidelines") (Exhibit 20).

[59] J. Timothy Sprehe, *Sprehe: E-Mail Records Problems*, Federal Computer Week, May 14, 2007. (hereinafter "Sprehe, *E-Mail Records Problems*") (Exhibit 21).

[60] Sedona Guidelines at pp. vi, vii, 1 (see Exhibit 20).

[61] Id. at p. 13.

[62] Id. at pp. 13-15.

[63] Jason Miller, *Survey Shows CIOs Losing a Seat at the Table,* Federal Computer Week, February 27, 2008 (hereinafter Miller, *Survey Shows CIOs Losing a Seat at the Table*) (Exhibit 22).

[64] Sedona Guidelines at p. 16 (see Exhibit 20).

policy, given that many factors will influence an organization's plans and no two organizations are exactly alike.[65]

In addition, an understanding of the organization's legal obligations should guide its policies and procedures and the organization should not confuse "disaster recovery" with records management.[66] Federal agencies are subject to many of the same legal and regulatory requirements, but this should not result in one electronic information solution, as NARA to date has recognized.[67]

Third, organizations need not retain "all electronic information ever generated or received."[68] Retaining infinite amounts of electronic data results in costs beyond securing enough storage space. For example, retaining too much data makes searching for relevant documents considerably more difficult.[69] As the Sedona Conference cautions, however, document destruction (or "disposition" as NARA terms it) is most safely accomplished only when implemented pursuant to an established retention schedule.[70]

In the federal government, records are managed either as temporary or permanent records and the category in which they fall governs their method and timing of disposition. Like the private sector, it is equally impractical for the federal government to retain the potentially billions of emails it sends or receives.[71] Proper scheduling of agency records through NARA, coupled with effective employee training on records management responsibilities will help ensure retention of appropriate records for the appropriate length of time.

Fourth, and closely related to the third guideline, agencies should develop procedures that address "the creation, identification, retention, retrieval and ultimate disposition or

---

[65] Id. at pp. 15, 16.

[66] Id. at pp. 16-18.

[67] National Archives and Records Administration, Electronic Records Management (ERM) E-Government Initiative, Enterprise-Wide Electronic Records Management Issue Area; Electronic Records Management Guidance on Methodology for Determining Agency-Unique Requirements (2004) (Exhibit 23).

[68] Sedona Guidelines at p. 24 (see Exhibit 20).

[69] Id. at pp. 24, 31.

[70] Id. at p. 26.

[71] Jason R. Baron, *E-Mail Metadata In A Post Armstrong World*, IEEE, 1999 (hereinafter "Baron, *E-Mail Metadata*"), available at http://www.archives.gov/era/pdf/baron-email/-metadata.pdf (Exhibit 24).

destruction of information and records."[72] The Sedona Conference has stressed that just as important as having a policy is actually acting on that policy once it is conceived: "[a] policy in name only may be worse than no policy at all."[73]

Information and records management procedures should clearly spell out individual responsibilities and document information practices.[74] The Sedona Conference also advocates for an effective training program to help employees understand their responsibilities and make them better able to identify records and fully grasp the importance of records management.[75] To ensure that employees are following records policies organizations should conduct "compliance reviews" and "have appropriate sanctions for failure to comply."[76]

Fifth, the Sedona Conference recommends that an organization's policies and procedures mandate "the suspension of ordinary destruction practices and procedures" in order to comply with preservation obligations imposed by actual or anticipated litigation, government investigations, or audits.[77] Specifically, organizations need to have a plan in place to deal with the changes in policy that litigation obligations will require.[78]

2. The Sedona Conference Commentary On Email Management: Guidelines For The Selection Of Retention Policy

Similarly, the Sedona Conference has also offered specific guidance on the selection of an email management policy in a public or private organization.[79] The four guidelines follow:

> Guideline 1: Email retention policies should reflect the input of functional and business units through a team approach and should include the entire organization including any operations outside the United States.

---

[72] Sedona Guidelines at p. 31 (see Exhibit 20).

[73] Id.

[74] Id.

[75] Sedona Guidelines at pp. 31-38 (see Exhibit 20).

[76] Id. at p. 38.

[77] Id. at p. 42.

[78] Id. at pp. 42-46.

[79] Thomas Y. Allman, ed., The Sedona Conference Commentary on Email Management: Guidelines for the Selection of a Retention Policy, p. 239 (2007), available at http://www.thesedonaconference.org/content/miscFiles/Commentary_on_Email_Management__revised_cover.pdf (hereinafter "Sedona Conference Commentary on Email") (Exhibit 25).

> Guideline 2: The team should develop a current understanding of email retention policies and practices actually in use within the entity.
>
> Guideline 3: An entity should select features for updates and revisions of email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible.
>
> Guideline 4: Any technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems.[80]

According to the Sedona Conference, the overall "key is to develop and enforce, in good faith those reasonable policies which best fit the entity."[81] In the federal government part of determining the best fit for an e-mail records program will be determined by statutory records requirements, but agencies should also consider the guidance from the Sedona Conference.

LEGAL FRAMEWORK FOR PRIVATE ENTITIES

Notwithstanding the clear benefits of electronic record keeping, agencies almost across the board have been resistant to moving away from paper record keeping systems. By contrast, commercial entities in the private sector have adopted electronic record keeping software systems and practices, a move resulting in "increase[s in] productivity and efficiency" and "seamless management of all record types."[82] Unlike their government counterparts, private companies must contend with market forces that steeply penalize those companies slow to adapt to sweeping changes in the reliability and availability of electronic record keeping software and systems.

In both the government and private sectors, there is no one-size-fits-all approach that will work for all entities. Instead, the optimal record keeping system for both will vary depending on unique organizational needs and practices. Record keeping experts stress that notwithstanding individual differences between electronic record keeping systems, the overriding goal and "best practice is to archive and store everything in a system that's searchable for e-mail and kept in an orderly and organized way."[83] In the federal government many, if not most, agencies fail to clear

---

[80] Id. at pp. 239-240.

[81] Id. at p. 239.

[82] *DataSheet, Interwoven RecordsManager,* available at http://www.interwoven.com/media/collateral/datasheet/ds_recordsmanager_20080215_WEB.pdf (Exhibit 26).

[83] See Pete Yost, *Waxman Says New E-Mail Comments Conflict,* Associated Press, January 17, 2008 (quoting Rurik Bradbury, vice president of strategy for Intermedia, a company

even this relatively low bar.

A host of statutes and federal regulations inform the issue of whether, and how, a private company is required to retain its electronic records. Broadly speaking, only selected industries, along with all publicly-traded companies, are subject to such statutes and regulations. The most strictly regulated industries include the health care and financial services industries. Absent federal statute or regulation to the contrary, private entities generally are free to store records in any fashion and for any time period that they see fit.

As outlined below, private sector companies face potential civil fines for noncompliance with the record keeping obligations imposed on them by federal statutes. By contrast, the FRA lacks penalty provisions that apply to agencies on a wholesale basis; for the vast majority of its provisions there simply are no legal consequences for agency noncompliance.

1. Sarbanes-Oxley

The Sarbanes-Oxley Act requires publicly traded companies to "prepare and maintain for a period of not less than 7 years, audit work papers and other information related to any audit report [including emails], in sufficient detail to support the conclusions reached in such report."[84] Penalties for noncompliance range from civil fines to criminal sanctions for knowing "alter[ation], dest[uction], [or] mutilat[ion]" of any document with the intent to impede an investigation.[85]

2. The Gramm-Leach-Bliley Act and Related SEC Regulations

The Gramm-Leach-Bliley Act, passed in 1999, requires financial institutions to store emails for a period of six years. Similar strictures apply to broker-dealers pursuant to SEC Rule 17a-4. Under Rule 17a-4, employers of securities broker-dealers must store any email sent or received by employees for three to six years, to the extent that the email pertains to the employer's business as a broker-dealer. Rule 17a-4 contains significant penalties for noncompliance, including substantial monetary fines. Under this rule the SEC fined Morgan Stanley $15 million for the company's inability to manage email in compliance with SEC orders.[86]

3. Health Insurance Portability and Accountability Act

---

that runs e-mail systems for a quarter of a million companies) (Exhibit 27).

[84] Pub. L. No. 107-204, 116 Stat. 745, § 103 ("Sarbanes-Oxley Act of 2002").

[85] Id. at § 802.

[86] See Jo Maitland, *Morgan Stanley feels e-mail archiving pain*, SearchStorage.com (Feb. 15, 2006) , available at http://searchstorage.techtarget.com/news/article/0,289142,sid5_gci1166670,00.html (Exhibit 28).

Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require health care providers to store health care patient records in an environment that is confidential, secure and searchable for a period of six years from the date of the records' creation.[87] Noncompliance with HIPPA can result in severe penalties; fines ranging from $100 to $250,000 per person, per violation.[88]

4. The "Best Practices" Misnomer

CREW has been unable to identify a single set of industry "best practices" for electronic record keeping; at most entities such as the Sedona Conference have identified "best practice guidelines"[89] in recognition of the varied electronic records management needs of both governmental and private entities. As the Sedona Conference has observed,

> entities of comparable size with similar legal risk and regulatory profiles can and do successfully adopt different retention strategies . . . that . . . can vary over time, depending upon the phase of development, the size and complexity of the organization, and the particular issues most significant to the entity as any particular time . . .[90]

Record keeping experts define the overriding goal for record keeping systems in similarly broad terms; according to one expert, "the best practice is to archive and store everything in a system that's searchable for e-mail and kept in an orderly and organized way."[91]

Even in the more technical aspects of electronic record keeping, such as recycling of backup tapes, we have found no single consensus on a "best practice." The White House recently described its practice of recycling its backup tapes as consistent with "industry best practices relating to tape media management for disaster recovery back-up systems . . ."[92] The

---

[87] 45 C.F.R. § 164.530(j)(2).

[88] 42 U.S.C. § 1320d-6.

[89] See Sedona Best Practices at p. 1 (see Exhibit 3).

[90] Sedona Conference Commentary on Email (see Exhibit 25).

[91] See Yost, Associated Press (Jan. 17, 2008) (quoting Rurik Bradbury, vice president of strategy for Intermedia, a company that runs e-mail systems for a quarter of a million companies).

[92] Declaration of Theresa Payton, Chief Information Officer, Office of Administration, ¶ 12c, filed in CREW v. Executive Office of the President, Civil No. 07-1707 (HKK/JMF) (D.D.C.) (Exhibit 29). The Clinton Administration recycled backup tapes of White House emails every three weeks. See *Electronic Records: ClintonAdministration's Management of Executive Office of the President's E-Mail System*, GAO Report (Apr. 2001), at 8, 10-11.

White House did not, however, specify how often it "recycled" (or overwrote) its backup tapes, nor did the White House identify exactly what constitutes "industry best practices." The Sedona Conference guidelines contain no single "best practice" for how often backup tapes should be recycled or how long emails should be retained generally.[93]

LESSONS FROM LITIGATION

In the absence of defined standards that govern electronic record keeping in the private sector, private party litigation is probably the best indicator of practices that fall outside the norm and are likely to result in sanctions. The Federal Rules of Civil Procedure provide the ground rules for federal civil litigation. Amended substantially in December 2006, the rules now clarify that documents consisting of "electronically stored information (ESI)" are subject to civil discovery. The rules define ESI as including "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained."[94]

Electronic discovery is a rapidly evolving area of the law. New cases have addressed a range of discrete issues such as the standards that should govern the authentication of emails (for admissibility purposes);[95] standards for determining when, and whether, attorney-client privilege should be deemed waived when emails directed from an attorney to his or her client are then forwarded by the client to other parties;[96] and the extent to which a party producing electronic documents is required to organize them for the benefit of the requesting party.[97] More generally litigation reveals four areas to which record managers, both federal and private, should pay close attention: (1) requirements concerning backup tapes; (2) deletion of data from computer hard drives; (3) discovery violations involving electronic documents; and (4) metadata.

---

[93] Real-world examples from the case law document practices ranging from 7 to 10 days (see Connor v. Sun Trust Bank, 2008 U.S. Dist. LEXIS 16917, at *9-*10 (N.D. Ga. Mar. 5, 2008)); to 90 days (see Keir v. Unumprovident, 2003 U.S. Dist. LEXIS 14522, at *4 (S.D.N.Y. 2003)); to 15 weeks (see Quinby v. WestLB AG, 04cv7406, at 20 (S.D.N.Y. 2005)); and as long as nine months (see In re NTL, Inc. Securities Litigation, 02cv3013, at 10-11 (S.D.N.Y. Jan. 30, 2007)).

[94] Fed. R. Civ. P. 34(a). See also Cmte. Note to Fed. R. Civ. P. 26(a)(1) (ESI under amended Rule 26 has "same broad meaning . . . as in Rule 34(a).").

[95] Lorraine v. Markel American Ins. Co., PWG-06-1893, at *9 (D. Md. May 4, 2007) (noting that the "Federal Rules of Evidence . . . do not separately address the admissibility of electronic data.").

[96] Moro v. Target Corp., 2007 U.S. Dist. LEXIS 41442, *11; see also Jennifer M. Moore & Gregory S. Kaufman, *Discovery Can Get Tangled Up in 'Strings': It's Not Yet Clear How Privileges Should Apply to E-Mail Exchanges*, 29 Nat'l L.J. 17 (Dec. 4, 2006).

[97] MGP Ingredients, Inc. v. Mars, Inc. 2007 U.S. Dist. LEXIS 76853 (D. Kan. Oct. 15, 2007).

1. Obligations Concerning Backup Tapes

Amended Rule 26(b)(2) of the Federal Rules of Civil Procedure establishes a new standard for determining when a party must produce electronic documents requested in civil discovery. Under the new rule, a responding party need not produce electronically stored information from sources that it identifies as not "reasonably accessible because of undue burden or cost."

In the area of backup tapes, courts have construed the term "reasonably accessible" as including backup tapes "actively used for information retrieval" by the producing organization in the ordinary course of its business. By contrast, courts do not consider disaster recovery backup tapes to be "accessible."[98]

Backup tapes are subject to other litigation obligations including "litigation holds." Where an entity reasonably anticipates litigation, it must "suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of relevant documents."[99] In the electronic document era, litigation holds extend to all electronic documents known to exist on computer hard drives and servers.[100] Although this obligation does not ordinarily extend to recycling of disaster recovery tapes,[101] a court may require a party to stop its recycling where the backup tapes contain the only available copies of particular electronic documents and the party is aware of this circumstance.[102] Courts may also compel parties, both private and governmental, to produce backup tapes in response to discovery requests at their own expense. At least one court so ordered when the producing party failed to

---

[98] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); see also In re Kmart Corp., 371 B.R. 823, 353 n.15 (Bankr. N.D. Ill. 2007); Consol. Aluminum Corp. v. Alcoa, Inc., 244 F.R.D. 335 (M.D. La. 2006); Semsroth v. City of Wichita, 2004 U.S. Dist. LEXIS 30726, at *7 (D. Kan. 2004); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-432 (S.D.N.Y. 2004); Thompson v. United States HUD, 219 F.R.D. 93, 100 (D.Md. 2003); but see Toussie v. County of Suffolk, 2007 U.S. Dist. LEXIS 93988, at *24 (S.D.N.Y. 2007) (holding that disaster recovery tapes are to be considered accessible).

[99] Zubulake, 220 F.R.D. at 218. The obligation to stop document destruction also extends to anticipated government investigations or audits. See Sedona Guidelines at p. 42.

[100] Zubulake, 220 F.R.D. at 218.

[101] Id.

[102] See, e.g., Oxford House, Inc. v. City of Topeka, Kansas, 2007 WL 1246200 at *4 (D.Kan. April 27, 2007). See also United States v. Phillip Morris, 327 F. Supp. 2d 21, 23 (D.D.C. 2004) (court imposed $2.75 million in monetary sanctions against Philip Morris for e-discovery violations including loss or destruction of relevant emails).

preserve emails at a time when they had not yet been copied onto backup tapes.[103]

The Sedona Conference has emphasized the need to "have a plan in place to deal with the changes in policy that will be mandated by a legal hold."[104] Recommended techniques include anticipating circumstances that will trigger the suspension of normal destruction procedures; identifying those persons with authority to suspend such procedures; creating a stand-alone document that describes processes for suspending normal records destruction; effectively communicating litigation holds once imposed; and documenting the steps taken to implement any litigation hold.[105]

Frequently, public and private sector entities contract with third parties to create and maintain backup tapes. For discovery purposes, producing parties are deemed to have control over the backup tape recycling procedures of their outside vendors.[106]

2. Deletion Of Data From Computer Hard Drives

The Sedona Conference defines "deleted data" as

> data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.[107]

Data is purposefully deleted in both the private and federal sectors for a variety of reasons, some legitimate and some less so. For example, two agency heads of the Environmental Protection Agency requested that their computers be re-formatted prior to administration

---

[103] Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority, 2007 U.S. Dist. LEXIS 39605 (D.D.C. June 1, 2007).

[104] Sedona Guidelines at p. 42 (see Exhibit 20).

[105] Id. at pp. 42-48.

[106] See, e.g., Keir v. Unumprovident Corp., 2003 U.S. Dist. LEXIS 14522, at *11 (S.D.N.Y. 2003). The Keir court held that a company had violated a preservation order by not instructing its third-party data vendor to temporarily suspend the default policy of recycling email backup tapes every 90 days. The district court reasoned that the company had "ultimate control over the [third party vendor's] email retention policy" and was also able to "specify a retention policy other than the default policy." Id.

[107] Sedona Best Practices at p. 92 (see Exhibit 3).

transitions to prevent data accumulated during their tenure from becoming accessible to future users of the same computer.[108] More recently, the White House has admitted it has a policy of "wiping" the hard drives of outgoing employees shortly after their departure, purportedly to cut down on the cost of purchasing new computers.[109] The White House also replaces up to one-third of all EOP hard drives annually and destroys the hard drives of the replaced units.[110]

Implementing a policy of wiping hard drives of departing employees, whether undertaken by a public or private sector entity, may constitute spoliation (or destruction) of evidence and lead to civil litigation damages when a "reasonable person should have foreseen that the [data on the wiped computer] was material to a potential civil action."[111] Currently the Court in CREW v. Executive Office of the President is considering whether, in light of evidence that the White House failed to properly archive emails or capture them on backup tapes, the White House should be ordered to create and preserve forensic copies of all data on employee workstations.

3. Discovery Violations Involving Electronic Documents

A party in civil litigation that willfully destroys presumptively relevant documents, including emails, during the course of civil discovery can be held liable for sanctions.[112] Similarly, failure to conduct a diligent search for electronic records may also lead to sanctions.[113]

---

[108] Landmark Legal Found. v. EPA, 272 F.Supp.2d 70, 83-84 (D.D.C. 2003) ("[outgoing EPA Administrator Carol] Browner requested sometime before noon [on January 19, 2001] that her computer be reformatted and/or that all her files be erased that day in preparation for the next administrator . . . Acting Administrator Michael McCabe left EPA on February 2, 2001 . . . At the end of his tenure, he asked that his computer be reformatted as part of his transition out of office.").

[109] Electronic Records Preservation at the White House: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong. 98 (Feb. 26, 2008), available at http://oversight.house.gov/documents/20080228105823.pdf (testimony of Office of Administration Chief Information Officer Theresa Payton that "as employees depart, if we want to be able to reuse their equipment, we actually take the files and store them on a shared drive. And then if we want to reuse their equipment, we would need to wipe their drives so that we're not buying a new PC . . .") (Exhibit 30).

[110] See Second Declaration of Theresa Payton, (March 21, 2008), submitted in CREW v. Executive Office of the President (Exhibit 31).

[111] Forsythe v. Black Hills Corp., 2008 U.S. Dist. LEXIS 10430, at *10 (N.D. Ill. Feb. 8, 2008); see also APC Filtration, Inc. v. Becker, 2007 U.S. Dist. LEXIS 76221 (N.D. Ill. Oct. 12, 2007).

[112] Zubulake v. UBS Warburg LLC, 229 F.R.D. at 439.

[113] Qualcomm, Inc. v. Broadcom Corp., 2008 U.S. Dist. LEXIS 911 (S.D. Cal. Jan. 7, 2008).

For example, one court held that a party responding to a discovery request failed to conduct a diligent search for potentially responsive documents where the party failed to search the email archives of witnesses expected to testify at trial using search terms deemed "relevant" to the case.[114] The responding party represented repeatedly throughout discovery and the trial that it possessed no responsive documents that would have been dispositive of the patent dispute between the parties. The district court had harsh criticism for the in-house attorneys:

> Qualcomm's in-house lawyers were in the unique position of (a) having unlimited access to all Qualcomm employees . . . (b) knowing or being able to determine all of the computers and databases that were searched and the search terms that were utilized, and (c) having the ability to review all the pleadings filed on Qualcomm's behalf which did (or should have) alerted them to the fact that either the document search was inadequate or they were knowingly not producing tens of thousands of requested documents.[115]

4. Metadata

"Metadata" is defined as "information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted."[116] That metadata comprises a component of any federal "record" for Federal Records Act purposes was established in Armstrong v. Executive Office of the President, 810 F.Supp. 335, 341 (D.D.C. 1993), aff'd, 1 F.3d 1274 (D.C. Cir. 1993). In ruling that metadata must be preserved, the Armstrong court reasoned that "[t]his information . . . in combination with the substantive information contained in the electronic material . . . will convey information about who knew what information and when they knew it.[117]

In response to this ruling, NARA adopted regulations requiring agencies to track transmission and receipt-of-data elements of email messages.[118] These regulations recognize the "unique aspects" of electronic mail and mandate that email records residing on a "live" system be placed in some form of agency record keeping system (paper or electronic),[119] "as the best

---

[114] Id. at *11, *23.

[115] Id. at 38-39.

[116] See Sedona Best Practices at 94 (see Exhibit 3).

[117] Armstrong, 810 F.Supp. at 342.

[118] 36 C.F.R. § 1234.24.

[119] 36 C.F.R. § 1234.24(b).

means to preserve the[ir] content, structure, and context . . ."[120]

In the civil discovery context, the amended Federal Rules of Civil Procedure permit a party to request electronic documents "in [the] form or forms in which [such documents are] ordinarily maintained."[121] At least one court has construed this rule as requiring the production of electronic documents in their native, electronic format, to reveal pertinent metadata.[122] If, however, a party normally keeps a certain type of document in paper format, the party requesting documents typically cannot compel the production of such documents in electronic format.[123]

SPECIFIC FEDERAL AGENCY RECORD KEEPING POLICIES

While this report examines electronic record keeping as a whole, we focus on email records due to their ubiquitous nature in the federal government and in the modern office. A 1999 report authored by a Department of Justice lawyer speculated that, in aggregate, federal agencies create at least 36.5 billion messages per year,[124] a number that most certainly has increased exponentially. More recently, a respondent to our online survey posited that about 90% of the business of the federal government was conducted by email.[125] And while electronic records include a variety of records (e.g., spreadsheets, maps, pictures), the widespread usage of email records makes them a top priority for agency record keeping policies.

Using a combination of FOIA requests and internet-based research from federal agency websites, CREW compiled the policies of the majority of larger, cabinet-level agencies in order to assess the sufficiency of current electronic record keeping policies. Generally speaking, agencies' electronic record keeping policies fall into four main groupings: (1) those that acknowledge DOD 5015.2, the current NARA-approved standard for electronic records management, and reflect this option; (2) those that recognize electronic record keeping as an option at all; (3) those that employ only a "print and save" or "print and file" technique; and (4) those that include pilot programs with the goal of implementing electronic record keeping in the

---

[120] 63 Fed. Reg. at 44,639.

[121] See Fed. R. Civ. P. 34(b)(ii).

[122] In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation, 2007 U.S. Dist. LEXIS 2650 (E.D.N.Y. Jan. 12, 2007); but see Kentucky Speedway, LLC v. National Association of Stock Car Auto Racing, Inc., 2006 U.S. Dist. LEXIS 92028 (Dec. 18, 2006) (Rule 34(b) does not require production of metadata absent a showing of a particularized need).

[123] Michigan First Credit Union v. Cumis Insurance Society, Inc., 2007 U.S. Dist. LEXIS 84842 (E. D. Mich. Nov. 16, 2007).

[124] See Baron, *E-Mail Metadata*.

[125] Citizens for Responsibility and Ethics in Washington and OpenTheGovernment.org Federal Records Officer Information Survey -- E-mail Records (responses collected March 4, 2008 to March 19, 2008 (unpublished survey) (hereinafter "Survey"), p. 39 (Exhibit 32).

future. Moreover, not all agencies have adopted agency-wide policies; in some agencies individual offices and components employ widely differing policies.

More generally, our research show that government policies vary widely, not only among agencies but also within them, at least in the justifications and explanations they offer for their policies. Some variation is expected given the leeway that agencies need to provide guidance on agency-specific documents and to work with varied computer systems. The amount of confusion within agencies and within the government as a whole, however should not be accepted. For example, when an agency that does not currently use an electronic system nevertheless provides guidance on its use, employees may be misled into thinking that Outlook or another email program is adequate for record keeping purposes, when it is not. This, coupled with the fact that some of the records policies apparently still in effect are quite dated, raises serious concerns about the level of importance and attention that federal agencies are giving to electronic records management.

Based on CREW's research it appears that overall, the print and save policy dominates the federal government. While some agencies have taken steps in the direction of managing records electronically, no agency from which we received responses has a well developed plan to move to full, agency-wide electronic records management. The technology for electronic records management exists and there is no justification for outdated and ineffective management of electronic records.

Reliance on employees in the first instance to determine what qualifies as record material will always leave room for mistakes, even with the most technologically sophisticated records management system. According to information management consultant J. Timothy Sprehe, there are few if any "quality assurance programs" set up to make sure employees are capturing proper records.[126] When coupled with the lack of records management training at agencies this leads to serious gaps in the net set up to capture federal records. Sprehe suggests automating many records functions to begin to solve this problem,[127] but others question whether full automation is even possible.[128] One thing is certain: as long as individual employees with little training and even less interest in records management serve as the determining point for what is and is not record material, records will be lost.

In order to properly focus employees on their record keeping obligations and to implement needed technology improvements senior agency management must be involved. Current trends show, however, that senior management is becoming less -- not more -- interested in records management. Research by the Information Technology Association of America found that 23% of senior technology managers at federal agencies now report to the chief financial

---

[126] Sprehe, *E-Mail Recovery Problems*.

[127] Id.

[128] Ben Bain, *Are We on the E-Record?*, Federal Computer Week, July 30, 2007 (Exhibit 33).

officer of their agency and not the agency head or secretary.[129] Many respondents to CREW's survey agreed that senior management lack the will and knowledge to improve records management

Finally and perhaps most notably, no agency we looked at used an agency-wide electronic record keeping system. Previously published reports document that most agencies do not use electronic systems for any records management.[130]

1. Policies That Acknowledge DOD 5015.2

Department of Energy

The Department of Energy created a standard in 2000, based on DOD 5015.2 STD, "as a recommended method for meeting the requirements and laws pertaining to records management."[131] The standard was called DOE-STD-4001-2000. There are no substantial differences between the DOD standard and the DOE standard.[132] When NARA officially endorsed version 2 of the Department of Defense's Electronic Records Management Software Application Design Criteria Standard, DOE cancelled DOE-STD-4001-2000 in favor of DOD 5015.2 STD.[133]

The Department of Energy requires that electronic records be "maintained in an approved electronic records management application meeting the requirements of DOE-STD-4001-2000."[134] It seems, however, that DOE had yet to implement an electronic records management policy as of 2006, because DOE Order 243.1 states that, "until an electronic records management system is available and implemented, electronic records will be printed and retained as paper files."[135]

Department of Education

---

[129] Miller, *Survey Shows CIOs Losing a Seat at the Table*.

[130] See, e.g., *E-Government; Probes Highlight Problems with E-Mail Storage,* Technology Daily, May 3, 2007, PM Edition (Exhibit 34).

[131] U.S. Dep't. of Energy, DOE-STD-4001-2000 (2000) (Exhibit 35).

[132] Id.

[133] Memorandum from Sharon A. Evelin, Director, Records Management Division, IM-23 (Feb. 26, 2007) (Exhibit 36).

[134] U.S. Dep't. of Energy, DOE Order O 243.1, Records Management Program (2006) (Exhibit 37).

[135] Id.

By 2002, the Department of Education had acknowledged that email was the "ubiquitous" form of agency communications.[136]

In January 2007, in a departmental directive the Department of Education endorsed the use of "electronic recordkeeping systems meeting the requirements of DOD-5015.2-STD."[137] But documents released to CREW did not indicate that any such system was in use. Moreover, the same directive offers as an alternative policy that all electronic records, including email, "be printed and retained as paper files."[138]

Department of Commerce

The Department of Commerce (DOC) Record Management Policy encourages program offices to "convert to and rely on electronic records whenever feasible." The policy also states that "an electronic records management product used by a Federal agency must, at a minimum, meet the Department of Defense (DOD) 5015.2 Standard."[139] Nevertheless, a PowerPoint training program from DOC states that "electronic records may be stored in computer memory or on storage media,"[140] even though merely saving a record on a computer hard drive does not meet the DOD 5015.2 Standard.

2. Policies That Acknowledge Electronic Record Keeping

Department of Homeland Security

The Department of Homeland Security Records Management Handbook requires that email records be maintained by "printing the email message (with attachment) and filing, when paper files are used as the record keeping system." The handbook also allows for "filing email electronically, when an electronic recordkeeping system is used as the recordkeeping system."[141] Documents released to CREW did not indicate that any such electronic system is in use.

---

[136] U.S. Dep't. of Education, Departmental Directive OCIO:1-103, Departmental Records and Information Management Program (2002) (Exhibit 38).

[137] U.S. Dep't. of Education, Departmental Directive OM:6-103, Records and Information Management Program (2007) (Exhibit 39).

[138] Id.

[139] U.S. Dep't. of Commerce, Records Management Policy (2005) (Exhibit 40).

[140] *Department of Commerce Records Management Training*, U.S. Dep't of Commerce (undated), available at http://ocio.os.doc.gov/ITPolicyandPrograms/Records_Management/PROD01_002018 (Exhibit 41).

[141] U.S. Dep't. of Homeland Security, Records Management Handbook, 0550 Publication (2005) (Exhibit 42).

Department of Justice

The Department of Justice policy "governing the Department-wide Records Management Program . . ." states that "e-mail information that is record information must be retained in a record keeping system that meets ORMP [Office of Records Management Policy] criteria. If the e-mail system in use does not meet ORMP criteria for electronic recordkeeping, or has not been appraised as an electronic record keeping system by NARA . . . then employees and contractors must print the e-mail to paper, along with all contextual information, and file it in a paper recordkeeping system."[142]

The same policy also notes that "backup tapes are NOT recordkeeping systems of the Department of Justice."[143]

A Department of Justice memo dated November 26, 2003 refers to a system called "Enterprise Vault from KVS," which appears to be the most current reference.[144] Enterprise Vault appears to be only an e-mail archiving system[145] and it is not currently on the list of programs that have DOD 5015.2 certification.[146]

Department of Justice - Bureau of Alcohol, Tobacco and Firearms (ATF)

ATF policy states that "[b]ecause ATF does not have an electronic recordkeeping system, e-mail messages to be retained as Federal records must be printed and filed as part of each office's paper recordkeeping system . . ."[147]

Department of Justice - Tax Division

A Tax Division directive from 1996 states that "[t]o our knowledge, there is no commercially available computer software that provides a system of indexing electronic records that meets those [NARA's] proposed standards. Accordingly, until further notice, all e-mail

---

[142] U.S. Dep't. of Justice, Records Management, DOJ 2710.11 (2006) (Exhibit 43).

[143] Id. (emphasis in original).

[144] Memorandum from Paul R. Corts, Assistant Attorney General for Administration, (Nov. 26, 2003) (Exhibit 44).

[145] *Symantec Enterprise Vault Placed in Leaders Quadrant in Latest Magic Quadrant for E-mail Archiving*, available at http://www.symantec.com/about/news/release/article.jsp?prid=20070601_01 (Exhibit 45).

[146] See DOD Compliant Product Register.

[147] U.S. Dep't. of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, Electronic Mail (E-Mail) Records, AFT O 1342.1 (2004) (Exhibit 46).

messages that constitute federal records must be printed on paper, annotated, and stored in an existing system of records . . ."[148] Given that the Tax Division has never released any updated policy or directive, we assume the 1996 directive is still in force.

Department of Justice - Criminal Division

A document from 2002 mentions that new "automatic purge" software for emails "does not free the user of his responsibility to save (Print or Archive) e-mail records designated as 'official records.'"[149] There is no further explanation of what "Print or Archive" actually means in practice. The policy also states that the only "viable solution" for avoiding the loss of official email messages and documents is that be "printed out and retained in hard copy."[150] The document goes on to speculate that one day there might be a requirement to save official records in electronic format, but there is no indication that the Criminal Division has yet implemented such a requirement.

Department of Health and Human Services (HHS)

HHS policy clearly states in HHS-2007-0004 that within each HHS office, electronic records -- including email -- should be maintained in an "enterprise-wide electronic content management system with record keeping functionality . . ." If such a system is not available electronics records should be printed and filed in a paper record keeping system.[151]

HHS - Health Resources and Services Administration (HRSA)

HRSA follows the same guidelines for record keeping as HHS.[152]

HHS - Food and Drug Administration (FDA)

The FDA provided CREW with a copy of an HHS record keeping policy that has since been made obsolete by HHS-2007-0004, cited above.

HHS - Administration for Children and Families (ACF)

---

[148] U.S. Dep't. of Justice, Tax Division, Tax Division Directive No. 106, Retention of E-Mail Messages That Constitute Federal Records (1996) (Exhibit 47).

[149] U.S. Dep't. of Justice, Criminal Division, E-Mail Retention Guide, Attachment to 80-4 (2002) (Exhibit 48).

[150] Id.

[151] U.S. Dep't. of Health and Human Services, HHS Policy for Records Management, HHS-2007-0004 (2008) (Exhibit 49).

[152] Letter from Mona Finch, Freedom of Information Officer, to Anne Weismann, Citizens for Responsibility and Ethics in Washington (July 24, 2007) (Exhibit 50).

In its Standard Operating Procedure for Records Management, the Administration for Children and Families states that "[a]ll ACF staff must be able to identify those electronic mail messages the are Federal records and must be aware of the record keeping requirements that apply to electronic mail."[153] The policy does not, however, explain what an employee is to do with an email that is a federal record once it has been identified.

HHS - Agency for Healthcare Research and Quality (AHRQ)

The AHRQ provided CREW with a copy of an HHS record keeping policy that has since been made obsolete by HHS-2007-0004, cited above.

HHS - National Institute of Health (NIH)

Section 1743 of the NIH National Library of Medicine Manual requires that when emails are federal records "the e-mail must be printed out and filed with related records in the official files of the employee's organization."[154]

In contrast, section 1742 of the NIH Policy Manual regarding the "Transfer, Withdrawal and Destruction of Records at the Washington National Records Center" states that "[p]ermanent electronic records must be either on open-reel magnetic tape on tape cartridges."[155] It is unclear whether email, which is an electronic record, is covered by this policy given the agency-wide practice of printing out emails, thereby converting them to paper records.

Department of Labor (DOL)

Under a 1996 DOL memo, email messages that were federal records were to be printed and filed in an appropriate record keeping system.[156]

A 2004 memo from the Solicitor of Labor reiterates the policy that "once an e-mail is determined to be a federal record . . . it must be printed out and filed in an appropriate file system." The memo also notes that the email program Outlook "does not allow records to be

---

[153] U.S. Dep't. of Health and Human Services, Administration for Children and Families, Standard Operating Procedure for Records Management (2005) (Exhibit 51).

[154] U.S. Dep't. of Health and Human Services, National Institute of Health, National Library of Medicine, NLM Manual, 1743 Keeping and Destroying Records (2006) (Exhibit 52).

[155] U.S. Dep't. of Health and Human Services, National Institute of Health, NIH Manual, 1742 Transfer, Withdrawal and Destruction of Records at the Washington National Records Center (2004) (Exhibit 53).

[156] Memorandum from Shirley A. Malia, Director, Information Technology Center (March 28, 1996) (Exhibit 54).

managed in a way that meets the requirements of the FRA."[157]

A Frequently Asked Questions (FAQs) document, attached to a 2006 DOL memo, complicates the policy further. This document explains that there are "two ways to save Federal Records: (1) Print and save the email message and corresponding attachment(s) into a manual filing system or; (2) Click and save the email message and corresponding attachment(s) into your Agency's electronic record keeping system." The document encourages the reader to ask the Agency's records manager for guidance on identifying the system. It is unclear from the document if any such system exists at DOL.[158]

DOL requires that permanent electronic records be on "open reel magnetic tapes, tape cartridge or CDROM's,"[159] but does not address specifically the status of email as either a paper or electronic record.

DOL - Occupational Safety and Health Administration (OSHA)

According to an OSHA FAQ document from 2006, there is no current DOL-wide record keeping system and employees should therefore either "print and save" or "click and save." Again, no electronic records keeping system is identified, although the document does say that "DOL is in the beginning stages of developing a Document Management/Records Management application."[160] No documents about this program were released to CREW.

Department of Housing and Urban Development (HUD)

Documents released by HUD did not outline how federal e-mail records should be maintained. On its website, HUD provides a link to General Records Schedule 20 on electronic records (created by NARA). Under GRS 20, "e-mail must be saved to an electronic record keeping system, paper, or microform for record keeping purposes" [161]

In a Strategic Plan released by HUD's chief information officer, the agency set a goal to

---

[157] Memorandum from Howard M. Radzely, Solicitor of Labor, (July 8, 1004) (Exhibit 55).

[158] Memorandum from Patrick Pizzella, Assistant Secretary for Administration and Management, Chief Information Officer (December 1, 2006) (Exhibit 56).

[159] U.S. Dep't. of Labor, Manual Series, DLMS 1 - Records Management, Departmental, Chapter 400 - Records Management Program (2005) (Exhibit 57).

[160] "OSHA Records Management Briefing" (Presentation Handout) (Nov. 15, 2006) (Exhibit 58).

[161] *GRS Transmittal No. 20. National Archives and Records Administration, General Records Schedules*, (Feb. 27, 2008), available at http://www.archives.gov/records-mgmt/ardor/grs20.html (Exhibit 59).

"Define E-Government strategies and focus in support of Vision 2010 to include Enterprise Records Management (ERM) and other appropriate initiatives" by FY 2007.[162] HUD's Strategic Portfolio Review FY2008 also mentions records management, and states that "[t]he Electronic Document and Records Management Enterprise Service enables HUD to effectively manage all of its documents and records in a consistent, legal, and logical manner, from creation to disposition, using a common set of tools, standards and policies."[163] No other documents released by HUD in response to CREW's FOIA requests or available on HUD's website mention an "Electronic Document and Records Management Enterprise Service."

HUD has posted an "Exhibit 300 Business Case" on its website that also relates to records management. This document describes a "HUD Electronic Records System (HERS),"[164] but it is unclear how or if this relates to records management.

Department of Agriculture

Department of Agriculture policy dictates that the print and file approach be taken when an email and its attachments are determined to be federal records if a paper system is used.[165] The policy also provides that employees must use an electronic system if one is available and specifies that backup tapes are not adequate for this purpose.[166] The agency's records management policy available on its website makes no mention of any electronic record keeping system currently in use.[167]

3. Policies That Include Only "Print And File"

Department of Interior

---

[162] U.S. Dep't. of Housing and Urban Development, Strategic Plan, Vision 2010, The Office of the Chief Information Officer (2007) (Exhibit 60).

[163] U.S. Dep't. of Housing and Urban Development, Strategic Portfolio Review FY2008 (2007) (Exhibit 61).

[164] U.S. Dep't. of Housing and Urban Development, HUD Electronic Records System, Exhibit 300: Capital Asset Plan and Business Case Summary, (2007) (Exhibit 62).

[165] U.S. Dep't of Agriculture, Office of the Chief Information Officer, *Records Management, DR 3080-001,* available at http://www.ocio.usda.gov/records/doc/DR3080-001.html (Exhibit 63).

[166] Id. According to a source at the Department of Agriculture that we spoke with, who requested anonymity, the agency is experimenting with two different DOD 5015.2-certified electronic records programs, one of which may be implemented throughout the agency. We have not yet seen any documentation of either program.

[167] Id.

The Department of Interior (DOI) presents a unique case in records management mainly because of the long running Cobell civil suit against DOI.[168] Court orders in that case have mandated a variety of record policies at DOI, including that all records related to the case be preserved in paper format. This policy has proved costly and burdensome to the agency.[169] In addition, in 2001 as a sanction for its failure to live up to its e-discovery obligations, the Cobell court ordered that DOI be disconnected from the internet. This left some DOI programs without email accounts through at least December 2007.[170]

The Department of Interior published a pamphlet entitled "Managing Electronic Mail" with guidance on identifying email records, managing email and employee responsibilities. The pamphlet states that when an email is determined to be a record, the employee is required to "print a hard copy of the record, including attachments and transition information, and file it in the official filing system."[171]

4. Pilot Programs

Environmental Protection Agency - Office of Environmental Information

In 2003, the Environmental Protection Agency (EPA) announced the results of a pilot program to select an enterprise-wide Electronic Records and Document Management System (ERDMS). The agency's effort was headed by the Office of Environmental Information and resulted in the selection of a commercial off-the-shelf (COTS) solution.[172] EPA's process was chronicled in a series of "Recommended Practice" documents later produced by NARA to show other agencies how to select a system.[173] It is unclear, however, if EPA ever implemented the program because current records management policy at the agency provides for printing and

---

[168] See Cobell v. Kempthorne, 96-1285 (D.D.C.).

[169] E-mail from Brian McCauley, Bureau Records Officer, Capital Planning and Information Policy Branch Minerals Management Service/Department of Interior, to Ginny Morgan, MMS FOIA/Privacy Officer (Jan. 25, 2008 12:53 PM) (hereinafter "McCauley Email") (Exhibit 64).

[170] Ben Bain, *Hot or Not: Congress Failed to Make a Mark,* Federal Computer Week, December 17, 2007. (Exhibit 65).

[171] *Managing Electronic Mail*, On the Record with the Department of Interior Records management Program (undated), available at http://www.doi.gov/ocio/records/brochure.html (Exhibit 66).

[172] Memorandum from Mark Luttner, Office of Information Collection (OIC), and Mark Day, Office of Technology Operations and Planning (OTOP) (August 15, 2003) (Exhibit 67).

[173] National Archives and Records Administration, E-Gov Electronic Records Management Initiative, Recommended Practice: Evaluating Commercial Off-the-Shelf (COTS) Electronic Records Management (ERM) Applications (2005) (Exhibit 68).

saving e-mail records when an electronic system is not available.[174]

HHS - Centers for Disease Control - Office of Health and Safety

The Centers for Disease Control (CDC) called the need for electronic record keeping systems in the federal government "imperative" and said that "printing and storage of [electronic] documents is no longer a viable option." To that end the CDC states that it is testing (as of 2005) an electronic system in its Office of Heath and Safety.[175]

DOI - Mineral Management Service - Mineral Revenue Management

According to a records officer at the Mineral Management Service, the agency's Mineral Revenue Management program has undertaken a pilot program to find an electronic solution to its records management issues. To that end, the program is testing a software program that is compliant with DOD 5015.2 standard.[176]

TESTING AGENCY ELECTRONIC RECORDS PRACTICES

Agency electronic record keeping policies tell only half of the story; still missing are the actual agency practices in managing email records. To test the efficacy of agency email policies, CREW submitted a series of FOIA requests to seven agencies for specific email records pertaining to discrete, agency-specific policies, programs or actions. We selected the subjects for the requests based on press releases on agency websites within the last three years, paying careful attention to subjects of limited scope so as not to unnecessarily overwhelm FOIA offices. At the same time, we sought subjects that were sufficiently large and important that it was likely the subject agency created at least some emails that could be considered federal records. CREW requested the records in either paper or electronic form. Although the test sample is very limited, the results were consistent with CREW's experience as a frequent FOIA requester of email and other electronic records. Agencies responding to the hundreds of FOIA requests CREW has filed since its inception have provided copies of emails almost exclusively in paper form and many agencies consistently have produced no emails whatsoever.

To date five of the seven agencies have responded.[177] All responding agencies provided records only in paper form. A summary of their responses follows.

---

[174] Environmental Protection Agency, Records Management Policy, Records Management (2006) (Exhibit 69).

[175] U.S. Dep't of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, General Administration, Records Management, CDC-GA-2005-07 (2005) (Exhibit 70).

[176] See McCauley Email.

[177] The Department of Justice and HHS have not yet responded.

1. Department of Labor

CREW originally sought emails related to the Department of Labor's October 19, 2005 award of $125 million to 70 community colleges competing for the President's Community-Based Job Training Grants. Specifically, CREW sought copies of email records related to the disbursement of Community-Based Job Training grant monies to selected community colleges.[178] After discussions with a DOL FOIA officer, CREW agreed to limit the request to 12 specific community colleges.

DOL responded within 30 days with 28 responsive documents, including emails and attachments from November 2005 to January 2007 dealing with the disbursement of grant money.

All emails provided were branded with the date and time they were sent, attachments were enclosed and the full names of senders and recipients (excluding redactions) were clear on each e-mail.

2. Department of Agriculture (USDA)

Through its FOIA of the Department of Agriculture, CREW requested emails dating from May 1, 2006 to October 1, 2006, related to USDA's transition to "ongoing bovine spongiform encephalopathy (BSE) surveillance" as announced on July 20, 2006.[179] This program was administered by the Animal and Plan Health Inspection Service (APHIS) and followed standards and gridlines established by APHIS with Veterinary Services (VS) and the National Surveillance Unit (NSU).[180] Organizationally, NSU is a unit of VS,[181] which in turn is an operational program unit of APHIS under the jurisdiction of the Office of the Undersecretary for Marketing and Regulatory Programs (MRP).

As of publication date, CREW had received responses from two departments of USDA. The Office of the Undersecretary for Marketing and Regulatory Programs (MRP), which has jurisdiction over all sub-units related to the creation of the BSE plan, did not locate any

---

[178] *2005 Highlights*, available at http://www.dol.gov/dol/highlights/highlights-2005.htm (Exhibit 71).

[179] *USDA Announces New BSE Surveillance Program*, available at http://www.usda.gov/wps/portal/usdahome?contentidonly=true&contentid=2006/07/0255.xml (Exhibit 72).

[180] *Bovine Spongiform Encephalopathy (BSE) Ongoing Surveillance Plan*, available at http://www.aphis.usda.gov/newsroom/hot_issues/bse/downloads/BSE_ongoing_surv_plan_final_71406%20.pdf (Exhibit 73).

[181] *About the National Surveillance Unit*, available at http://www.aphis.usda.gov/vs/ceah/ncahs/nsu/about.htm (Exhibit 74).

responsive records.[182] It is unclear whether APHIS, VS, NSU and MRP did not create any email records or whether the FOIA officer was simply unable to locate email records.

The other responding department, the Office of General Counsel, released 20 pages of documents, including four pages of heavily redacted emails. One of the emails originated in APHIS,[183] raising the question why USDA's Office of General Counsel considered the document to be a record worthy of preservation, while another department either did not regard the email as record material or was unable to locate it. The Office of General Counsel also released several other non-email documents related to the program.

3. Department of Interior

From the Department of Interior CREW sought emails pertaining to the agency's November 10, 2005 announcement that it would not recognize the St. Francis/Sokoki Band of Abenaki located in and around Swanton, Vermont as an Indian Tribe.[184] CREW limited the time-frame of the request to between August 1, 2005 and December 1, 2005. As of our publication date Interior had produced two releases, both from the Office of the Secretary. The first contained five documents totaling 26 pages and included memos but no emails. The second consisted of 12 pages, all of which are either emails or attachments.

In light of the Cobell court orders it is impossible to know if the volume of emails the Department of Interior produced in response to our FOIA request is limited because the relevant offices did not have email access during the relevant time period, or because the agency lacks the ability to perform an effective and comprehensive search for email records.

4. Department of Commerce

From the Department of Commerce CREW requested emails sent or received by agency employees or officials from July 1, 2006 to December 1, 2006, related to DOC's stated "efforts to strengthen U.S. competitiveness in the world travel and tourism market."[185] The agency publicized this plan in a press release dated September 5, 2006.

---

[182] Letter from Rita Morgan, USDA Freedom of Information Officer, Administration to William C. Holmes, CREW (March 13, 2008) (Exhibit 75).

[183] Email from Laird Draves, APHIS, to Mark Garrett (office unknown) (Aug. 1, 2006) (Exhibit 76).

[184] *Associate Deputy Secretary Declines to Acknowledge St. Francis/Sokoki Band of Abenaki as an Indian Tribe*, available at http://www.doi.gov/news/05_News_Releases/051115a.htm (Exhibit 77).

[185] *U.S. Travel and Tourism Advisory Board Recommends New National Strategy to Attract International Visitors,* available at http://www.commerce.gov/NewsRoom/PressReleases_FactSheets/DEV01_005353 (Exhibit 78).

In response, DOC released dozens of emails and related attachments. The documents were well laid out and contained all relevant transmission data. Attachments were stapled to the corresponding email, which aided in the usefulness of the FOIA release.

5. Department of Education

Originally, CREW sought emails and attachments related to the Department of Education's June 2006 Gulf Coast Reading Initiative. Education, however, denied CREW's request for a fee waiver -- the same waiver that CREW had requested and received for all other FOIA requests used in this report. In the absence of a fee waiver, Education estimated that searching for responsive documents would involve 40 hours of labor spread out over workers at three different pay grades at a total of at least $2,111.83.[186]

Regardless of Education's reasons for denying the waiver, this response is a firm indictment of the agency's email record keeping practices. If Education were using a modern electronic record keeping program, the agency would be able to conduct a thorough search on this topic in much less time and at a significantly reduced cost.[187]

CREW SURVEY RESULTS

To gain a more complete understanding of current email record keeping practices in the federal government CREW, along with OpenTheGovernment.org, created and submitted a survey to over 400 records managers from 230 agencies and agency components. We selected records managers rather than other agency officials on the assumption they would have the best working knowledge of records practices in their agencies and because we had access to their email addresses. The survey was not designed to generate statistically valid results or to single out any particular agency or records manager, but instead to serve as an anecdotal framework for understanding how federal agencies actually handle their email records.

We received 87 complete or partial responses over a three-week period. Unless otherwise noted, there are at least 50 responses to any particular question discussed here.[188] The survey confirms what our research into agency policy had shown, namely that the most popular method of email records management is to print email records and file them with paper records. Results also confirm what agency policies submitted in response to CREW's FOIA requests hinted at -- some agencies have multiple policies governing email records or no policy at all. As

---

[186] Letter from Delores J. Barber, FOIA Public Liaison, OM/RIMS, Dep't of Education, to William C. Holmes, Citizens for Responsibility and Ethics in Washington, (Feb. 29, 2008) (Exhibit 79).

[187] CREW has had numerous other problems with Education and its failure properly maintain email records as the Federal Records Act requires.

[188] The entire survey is available as Exhibit 32 minus redactions to protect the anonymity of respondents.

one records manager stated in response to the question of how emails are preserved at their agency, "we have not gotten to that phase of records management."[189]

Only six survey respondents said that their agency exclusively used some type of electronic system to manage its email records. Of those six respondents, four identified specific product names -- all different -- and four responded that their agencies used products that were purchased off-the-shelf, demonstrating that some agencies are taking advantage of products already available to the government.[190]

Only two respondents claimed the email records management system used by their agencies was DOD 5015.2 compliant, while three respondents were completely unfamiliar with this standard. From this it appears that since endorsing the DOD standard in 2003, NARA has not made agencies sufficiently aware of this technology and the products that meet DOD specifications and are available to solve the agencies' record management issues.

The Survey responses also confirm that agencies are far more able to search for emails in electronic systems than for emails stored in paper systems. Five individuals, representing 83% of respondents who use an electronic system to manage their emails, said their systems were searchable for email records. By contrast, of those using paper or some other system, 61% (or 35 of the 57 respondents in this category) found it difficult to impossible to search for and find specific email records.[191]

Survey respondents most often identified lack of training as the biggest impediment to preserving agency email records; 52% of respondents found it to be among the biggest problems with records management in their agencies. Contributing to this problem is both a lack of employee interest in training and a lack of time for training.[192] A common theme, reflected in the third most popular answer choice, is that "training is not an agency priority."[193] Some agencies do not have, or the records managers do not know if they have, training policies in place.

For those agencies that have training policies, the most common method is an individual training session with an employee.[194] Other methods include handing out materials to employees, classes for groups of employees, or online or computer training.[195]

---

[189] See Survey at p. 18.

[190] Id. at pp. 17, 24, 25, 26.

[191] Id. at pp. 22, 29.

[192] Id. at pp. 16, 29, 30.

[193] Survey at p. 30.

[194] Id. at p. 31.

[195] Id.

Training issues extend beyond teaching employees how particular record keeping systems work. Federal employees appear to lack an understanding of the most basic concepts such as the definition of records and employee responsibilities for agency records. "[D]efinitions of what constitutes a record differs among employees," reports one respondent. "Sometimes co-workers may make a wrong judgement call regarding whether or not a particular email is a record that should be retained."[196] Another responded that "determining which e-mails are official records" is the biggest problem with their agency email records management.[197]

The survey exposes a potential legal pitfall in the lack of concern for metadata. As the Armstrong case made clear,[198] metadata -- which includes the name of senders and recipients including those carbon copied (cced), date of email transmission, and, if requested, time and date of receipt acknowledgment -- must be retained with its associated email records. Yet in CREW's survey only 74% of respondents said that the most basic information, the time and date of the e-mail and full names of the sender and recipients, is saved. "No guarantees," wrote one respondent.[199] Other potentially important metadata fared even worse. Only 68% of respondents retain attachments to emails, while only 56% retain the names of those cced on emails.[200]

Survey responses reveal that lack of compliance and lack of penalties for non-compliance are also major problems. "I do know that less than 80% of the agency complies," commented one respondent.[201] Overall, 30% of respondents do not think their co-workers comply with email record policies while 26% do not know if co-workers comply. 34% of respondents are not aware of any monitoring of employee record keeping practices, and 56% said there was no penalty for non-compliance (at least on the agency level).[202]

Respondents also identified lack of support from upper management as a key problem. As one record manager wrote, "management verbalizes about how important recordkeeping is but does nothing to implement or fund."[203] "Until managers understand why records management is important it will never get attention," stated another respondent.[204] "Management

---

[196] Id. at p. 33.

[197] Survey at p. 16.

[198] Armstrong v, Executive Office of the President, 810 F.Supp. at 341.

[199] Survey at p. 20.

[200] Id.

[201] Id. at p. 32.

[202] Id. at p. 35.

[203] Survey at p. 37.

[204] Id. at p. 39.

does not even realize that there is a problem or appear to care," wrote yet another.[205] One records manager wrote, "no monitoring, no training, no penalties, no requirements for training. Agency records experts are ignored if they raise issues, it's a mess."[206]

Our admittedly unscientific survey reveals a number of major problems. First, agencies have inconsistent policies, as evidenced by the fact that so many respondents use multiple techniques to preserve email records at their agencies. Second, agencies have been slow to move towards electronic record systems. Third, agencies are not complying with their legal obligation to preserve metadata. Fourth, agencies lack training and compliance monitoring, two problems that would be easily cured by reforming agency policy and increased NARA involvement. Fifth, senior agency officials do not recognize the serious problems with their agencies' electronic records management and have yet to take steps to correct those problems. This concern is magnified by the fact that, as one record manager noted, "nearly 90% of the business within a federal agency is accomplished through e-mail. If these records are not properly managed, that means 90% of the records are not properly managed."[207]

RECOMMENDATIONS

Effective solutions to the government-wide breakdown in electronic record keeping compliance will require legislative changes, a more active role by NARA and a larger percentage of agency budgets dedicated to technology improvements. More specifically, based on our findings we recommend the following:

1. Amend the Federal Records Act

Congress should amend the FRA to require that all agencies within the federal government implement electronic record keeping by a date certain that recognizes the readily available technology. Only through a statutory directive is there hope of reversing the technology backslide that has occurred within the federal government.

Congress should also amend the FRA to require NARA to conduct annual audits based on bench marks NARA establishes that address such issues as training, education and compliance. Each agency should be required to submit annual audits to NARA certified by the agency head. Only by requiring agency heads to play a direct and specific role will agencies give electronic record keeping the priority it deserves. Recognizing that NARA does not have the resources to audit every agency, Congress should require NARA to conduct yearly audits of select agencies based on their audit submissions.

The FRA should also be amended to add additional penalties for noncompliance directed

---

[205] Id. at p. 30.

[206] Id. at p. 34.

[207] Survey at p. 39.

at both the agency and individual agency employees. As outlined in our report, the private sector is subject to rigorous penalties for noncompliance with record keeping obligations, which may account for its greater degree of compliance in comparison to the federal government.

2. NARA Must Take A More Active Role

The FRA mandates that NARA assist agencies in implementing record keeping standards. NARA, however, has interpreted its responsibilities very narrowly as limited to providing guidance. While we believe the current statute clearly mandates more, to the extent there is any lack of clarity the FRA should be amended to compel NARA to take an active role in ensuring government-wide compliance with record keeping obligations.

Specifically, NARA must conduct meaningful oversight that includes monitoring of agency compliance and working more directly with agencies to ensure the implementation of effective electronic record keeping. NARA should set bench marks that each agency must meet, including for the full implementation of electronic record keeping and continued compliance with record keeping requirements.

3. Each Agency Must Take A More Active Role

Agencies must, of course, share in the responsibility for complying with their record keeping obligations. Toward that end, each agency should designate an individual responsible for electronic records management within the agency. This designee should serve as the contact point both internally, within the government and externally with Congress and the public. Establishing effective training and employee education should be included within this individual's responsibilities together with monitoring internally the agency's compliance with electronic record keeping requirements.

4. Adequately Fund Agency Electronic Record Keeping

The long-term benefits that agencies will realize once they implement agency-wide electronic record keeping will more than offset the short-term costs attendant to a conversion from a paper to an electronic system. FOIA compliance alone will be exponentially easier and more cost-effective if agencies can use the superior search capabilities of electronically-stored records and produce records in electronic formats. Litigation costs will also be reduced, along with agencies' potential exposure to costly litigation sanctions for failing to meet discovery obligations. As the private-sector experience makes clear, electronic record keeping is the most efficient and effective way for a large organization to manage its records.

Congress must make electronic record keeping a priority when appropriating agency funds. Agencies must make electronic record keeping a priority by requesting the full funding that they need to make the conversion from a paper to an electronic system. And NARA must add its voice to the need for more agency funding.

EXHIBITS

To view all the exhibits cited in this report, please visit www.citizensforethics.org