Record Keeping Requirements for State Departments of Transportation

DETAILS

59 pages | | PAPERBACK

ISBN 978-0-309-42987-0 | DOI 10.17226/22986

AUTHORS

October 2009

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

Subject Areas: IA Planning and Administration;
IC Transportation Law

Legal Research Digest 52

RECORD KEEPING REQUIREMENTS FOR STATE DEPARTMENTS OF TRANSPORTATION

This report was prepared under NCHRP Project 20-6, "Legal Problems Arising Out of Highway Programs," for which the Transportation Research Board is the agency coordinating the research. The report was prepared by Terri L. Parker, Regional Counsel, Missouri Department of Transportation. James B. McDaniel, TRB Counsel for Legal Research Projects, was the principal investigator and content editor.

CONTENTS

The Problem and Its Solution

State highway departments and transportation agencies have a continuing need to keep abreast of operating practices and legal elements of specific problems in highway law. This report is a new paper, which continues NCHRP's policy of keeping departments up-to-date on laws that will affect their operations.

Applications

In recent years, a series of issues have emerged confronting state departments of transportation (DOTs) with a broadening definition of "public record" and the necessity for a system for retaining, organizing, and avoiding the spoliation of evidence. Specific issues include creating records for administrative needs, collecting evidence in anticipation of litigation, escrowing documents, dealing with electronic documents/email, being aware of public records laws, and protecting all proprietary information.

This project previously published "Freedom of Information Acts, Federal Data Collections, and Disclosure Statutes Applicable to Highway Projects and the Discovery Process," Orrin F. Finch and Gary A. Geren, *NCHRP Legal Research Digest 33*, April 1995. There has been a great deal of change since the release of that report and emerging communication methods likewise present new problems for developing methods of data information collection, storage, and protection. Federal, state, and local government agency lawyers and administrative personnel; private contractors; and other transportation professionals will benefit from an awareness of pertinent legislation and regulations, cases, and best practices as guidance for maintaining records to fit their particular needs.

While the focus of this digest is on requirements applicable to state DOTs, federal statutes are discussed extensively because many are directly applicable to state governments in their capacity as grantees. Federal case law is discussed as well, as many of the documentation and retention issues confronting state courts have previously been comprehensively addressed by federal courts.

The material covered in this digest should be useful to attorneys, administrators, safety officials, freedom of information officers, risk management personnel, maintenance engineers, and legislators.

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

RECORD KEEPING REQUIREMENTS FOR STATE DEPARTMENTS OF TRANSPORTATION

By Terri L. Parker
Regional Counsel, Missouri Department of Transportation

I. INTRODUCTION

Transportation agencies continue to be challenged by new and emerging communication methods as they develop and improve their strategies for data collection and protection. To competently address related issues, counsel for transportation agencies should be familiar with pertinent legislation and regulations, as well as mandatory and best practices as guidance for maintaining records to fit their needs. Applicable law and regulations pertaining to keeping, releasing, and destroying records within transportation agencies are discussed in this digest. The reader should be aware that, while this digest discusses rules and cases generally, specific research must be done for individual jurisdictions. Several terms used in the recordkeeping industry are described briefly in this section. The reader should refer to these definitions as necessary to fully understand and appreciate these discussions.

Definitions

Electronic records are records stored in a form that only a computer can process. They may include numeric, graphic, or text information, which may be recorded on any medium capable of being read by a computer.

Electronic signatures have been incorporated as part of federal law as the Electronic Signature in Global and National Commerce Act (ESGNCA)[1] and The Uniform Electronic Transaction Act (UETA)[2] and many state laws. The intent of these laws is to place electronic documents and the use of electronic signatures on a par with traditional paper-based transactions and the use of manual signatures. These laws were intended to eliminate any concerns that electronic signatures are as enforceable as traditional signatures.

Metadata are data that describe other data. Metadata can provide such information as the author, the last date a document was printed, the date the file was created, the number of words in the document, and when and what changes were made to the document.

Records are defined as all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical forms or characteristics, created or received by an agency as evidence of its organization, functions, policies, decisions, procedures, or operations.[3] Courts have ruled that text messages, instant messages, and voice mail records are public records and are subject to the same disclosure laws that apply to e-mails and paper records.[4]

Records Management is defined as the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to the creation, use, maintenance, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the agency.

The remainder of this report is organized into three sections and a conclusion. Sections II, III, and IV are summarized below.

Section II: Record Retention provides the reader with current information about maintaining and releasing records. It outlines pertinent legislation as well as best practices relating to records retention policies and document management systems. This information should assist agencies in retaining and organizing data. One part of this section is devoted to creating records for administrative needs and the collection of evidence from claim to litigation.

Section III: Release of Stored Information—Litigation and Discovery discusses the release of electronically stored information (ESI) in the litigation context and some of the challenges implicit in working with electronic information. The chapter includes a best practices section.

Section IV: Open Records outlines the broadening definition of "public record" and explores court interpretation of public records laws more expansively. One section discusses trends in state and federal open records laws. Other sections are devoted to proprietary information in proposals and critical infrastructure protection acts that are being adopted around the country.

To collect current data for this report, a survey was sent to the transportation agencies of each of the 50 states, as well as Washington, D.C., and Puerto Rico, regarding their retention policies. Thirty-one responses were received. A copy of the Records Retention Survey is attached as Appendix A. Responses are compiled and summarized in Appendix B.

[1] Pub. L. No. 106-229, 114 Stat. 464 (2000), codified at 15 U.S.C. § 7001 *et seq*.

[2] Drafted by the National Conference of Commissioners of Uniform State Laws at its Annual Conference, July 23–30, 1999.

[3] This definition is found in the Federal Records Act in 44 U.S.C. § 3301.

[4] *See* Detroit Free Press v. City of Detroit, Case No. 08-100214 (Feb. 5, 2008).

II. RECORD RETENTION

A. Adoption of Records Retention Program

Record-keeping requirements are imposed by both federal and state laws. Federal agencies are required[5] by law to establish and maintain records retention policies. State governments are also required by law to manage and maintain their records. For a sample list of laws requiring state agencies to maintain these records, see Appendix B. Not only are the systems required by law, records management programs allow their users to manage organizational information so that it is timely, accurate, complete, cost-effective, accessible, and useable. The following have been asserted to be the most important operational reasons to set up a good records management program.[6]

- To control the creation and growth of records.
- To reduce operating costs.
- To improve efficiency and productivity.
- To assimilate new records management technologies.
- To ensure regulatory compliance.
- To minimize litigation risks.
- To safeguard vital information.
- To support better management decision making.
- To provide easy access to information.
- To preserve the corporate memory.
- To foster professionalism in running the business.

Federal agencies are required by statutory provisions[7] to establish and maintain records retention policies. The National Archives and Records Administration (NARA) implemented the federal records retention regulations beginning at 36 C.F.R. § 1234.2, relating to electronic records and e-mail. The basic requirements of 36 C.F.R. § 1234.10 are as follows:

1. The agency must establish an agency-wide program for the management of all records created, received, maintained, used, or stored on electronic media.
2. Electronic records must be integrated with other records and information resource management programs.
3. Adequate training must be provided to staff.
4. An approved records dispositions schedule must be developed.
5. Methods of implementing controls over information that is related to national security, classified, sensitive, and proprietary, and over records covered under the Privacy Act must be established.
6. The agency must ensure that contractors comply with record retention policies so that their records can be easily accessed.

Accessibility of Records

When developing a records retention policy or reviewing an existing policy, an agency should consider several federal laws. It may be necessary to provide records in Braille, via a closed-circuit magnification system, reading machines, or large print indexes so that individuals with disabilities can access public records.[8]

In 49 C.F.R. §§ 7.2 and 7.5 is set out the U.S. Department of Transportation's (USDOT) responsibility to provide more than mere traditional paper access to its records. "Reading room" records are available on the USDOT Web site and include the following types of information: how to make a Freedom of Information Act (FOIA) request; opinions made in the adjudication of any case; statements of policy, staff manuals, or instructions to staff; various publications and forms; and many links to other transportation Web sites.[9]

Similarly, when an agency designs an Internet Web site, it must consider accessibility issues. Any Web site user should have access to the information and experiences available online. Those users with visual, hearing, or other physical impairments may have difficulty accessing Web content.[10]

Staff should consult state and local law as well as their counsel when developing a records management program. Each jurisdiction has different legal requirements.

Records Retention Policies in Litigation

Two federal lawsuits form the basis for the theories behind many of the current record retention and e-mail policies. These cases dealt with e-mail record-keeping policy for the federal government, examining the entire life cycle of the document from creation to disposition.

The two cases are loosely based upon the same set of facts and parties. In 1985, electronic mail was widely available to federal staff using professional office system software, which allowed users to send electronic

[5] 44 U.S.C. §§ 3101–3107.

[6] (Adapted from TEN BUSINESS REASONS FOR RECORDS MANAGEMENT IN INFORMATION AND RECORDS MANAGEMENT: DOCUMENT-BASED INFORMATION SYSTEMS, 1995.)

[7] 44 U.S.C. §§ 3101–3107.

[8] *See* § 508 of the Rehabilitation Act of 1973, 29 U.S.C. § 794d. *See also* 36 C.F.R. pt. 1194, which states as follows:

> The purpose of this part is to implement section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

[9] *See*, *e.g.*, http://www.faa.gov/foia/electronic_reading_room/.

[10] There are commercial providers who can provide accessibility assistance to Web designers.

messages, transfer text documents, and share calendar information. Backup tapes of the stored information were made weekly.

In 1987, National Security Council (NSC) policy makers considered e-mail to be a communications medium that relayed material of little importance. According to the policy, if an official "record" was created by the use of e-mail, users were supposed to print the message and file it or reduce the contents of the e-mail to a written memo or letter and file the memo. Once the e-mail message was reduced to paper it could be deleted. However, the "print and file" policy conflicted with actual practice, and many e-mail messages that were true records were never printed.

In anticipation of the change of administration from President Ronald Reagan to President George H.W. Bush, NARA announced it would delete all the Reagan era e-mails. This announcement spurred a suit by public interest groups, *Armstrong v. Bush*.[11] Armstrong alleged that a substantial amount of information contained on the Professional Office System (PROFS) qualified as records that should be retained under federal law. The court was asked to enjoin disposal of the PROFS[12] information, to direct the President and the NSC to properly classify the information, and to subject the information to the "life cycle" contemplated by federal law. Plaintiffs also alleged that the Archivist "abdicated" his statutory responsibilities by failing to exercise proper oversight of the decisions of the President and the NSC with regard to the PROFS information and further requested that the Archivist be ordered "to carry out his duties under the laws and regulations he administers."[13]

The appellate court decided that the record-keeping policy allowed the impermissible destruction of federal records, that electronic versions of e-mail were "records," and that the paper printouts did not include all the significant material contained in the electronic records. The paper printouts did not have information such as directories, distribution lists, and receipts. The court directed the Archivist of the United States to develop new guidelines for managing e-mail. Once those guidelines were developed, they spurred the General Records Transmittal 20 lawsuit, *Public Citizen v. Carlin*.[14]

In *Carlin*, Plaintiffs challenged the guidelines developed by NSC after the court's ruling in *Armstrong*. Under the new guidelines, e-mail records were not stored in their original format but rather as records that were transferred to paper or microfilm. The government argued that the most important element of the policy was that electronic records were captured with transmission data, including the name of sender, addressee, and date the message was sent. The appellate court deferred to the Archivist's decision and ruled in favor of the government, ruling that the technology for managing electronic records electronically was not available.

The rulings in these cases brought electronics records issues to the attention of government officials and the rest of the nation, setting the framework for the government records retention policies of today.

Recent Developments

It is interesting to note that the National Security Archive filed a lawsuit in 2007 against the Executive Office, alleging that several million e-mail messages were improperly deleted from White House computer servers.[15] A magistrate ordered the White House to provide it with information about the backup media that it uses to preserve records. The litigation is ongoing at the time of the writing of this digest. As evidenced by newspaper headlines, presidential and public records are and continue to be important in the public's eyes.[16]

Federal agencies are required to identify important documents and devise a trustworthy means of storing the records so that they are easily accessible and the documents themselves are easy to authenticate. This is no easy task,[17] where it is estimated that NARA received one hundred million e-mails at the end of George W. Bush's presidential term. NARA is expected to receive over one billion e-mails in the next decade.

In *New Jersey Land Title Association v. State Records Committee, Division of Archives and Records Management*,[18] the title association requested the state archive division to keep records such as notices of settlement and *lis pendens* and federal tax liens beyond the scheduled retention period due to the agency's history of "inconsistencies, irregularities and unreasonable delays in filing, indexing and providing public access to certain land records."[19] The court noted that the State Records Committee conducted a survey of the retention practices for these types of records by the 21 county clerks and registrars of deeds and mortgages. The survey disclosed "a notable lack of uniformity among the counties regarding microfilming of the records: some doing all three series, others just two, and still others only one."[20] The court found that the State Records

[11] 721 F. Supp. 343 (D.D.C. 1989).

[12] An intercommunicative software system marketed by IBM. *See id*. at 345.

[13] *Id*. at 347.

[14] 184 F.3d 900, 337 U.S. App. D.C. 320 (C.A.D.C. 1999).

[15] Citizens for Responsibility and Ethics in Washington v. Executive Office of the President, No. 1:07-cv-01707-HHK (D.D.C. Filed Mar. 21, 2008).

[16] *See*, *e.g.*, *Records Request Seeks Insight, Clarity*, FAIRBANKS DAILY NEWS-MINER, July 19, 2008; Pete Yost, Lawsuit: White House Won't Release Visitor Records, Townhall.com, June 16, 2009; *[Pensylvania] Open Records Office Issues First "Final Determinations,"* HEADLINES & DEADLINES, Mar. 5, 2009, available at http://pna.informz.net/pna/archives/archive_258793.html.

[17] *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt*?, 13 RICH. J. L. & TECH. 10 (2007).

[18] 315 N.J. Super. 17, 716 A.2d 541 (1998).

[19] *Id*. at 20.

[20] *Id*. at 21.

Committee's decision to approve the destruction of the documents was arbitrary and capricious because the Committee ignored its own finding that longer retention of these records might be in the public interest without providing any rational basis for their destruction.

In *Hynix Semiconductor, Inc. v. Rambus, Inc*.,[21] the primary question before the court was whether Rambus adopted and implemented a document retention policy in advance of "reasonably foreseeable" litigation in order to destroy relevant information. The court found the word "reasonable" must be viewed from the perspective of a plaintiff, who is in control of when the litigation is to be commenced. In this case, Hynix argued that Rambus contemplated litigation at the time it began to formulate a litigation strategy and set up a document retention policy that would deliberately destroy certain documents. The court noted that "a legitimate consequence of a document retention policy is that relevant information may be kept out of the hands of adverse parties," citing *Arthur Andersen LLP v. United States,*[22] where the court commented that "[d]ocument retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business." The court observed that a document retention policy that is "adopted or utilized to justify the destruction of relevant evidence is not a valid document retention policy,"[23] but held that Rambus did not purposefully discard documents to defeat fair litigation practices.[24]

Practical Considerations

Once a records retention policy has been adopted, courts may treat the policy as a set of rules that govern the agency. It is therefore important to educate employees on how to comply with the policy and the fact that if the agency has adopted a policy, staff is expected to conform to it.

Survey Responses

Of the responses received, not one agency said their policy had been challenged in court. However, several states indicated that their policies were considered by the courts when evaluating claims. For example, in Missouri, a lawsuit was filed against Governor Blunt, alleging that his office failed to comply with state record-keeping policies when disposing of e-mail. In Arkansas, a construction claim was recently filed by a contractor in an administrative suit. One of the issues in that suit is whether the project design consultant properly kept and retained e-mail correspondence related to the project as part of the government project file.

[21] 591 F. Supp. 2d 1038 (N.D. Cal. 2006).

[22] 544 U.S. 696, 125 S. Ct. 2129, 2135, 161 L. Ed. 2d 1008 (2005).

[23] *See* Hynix, 591 F. Supp. 2d at 1060.

[24] *Id*. at 1069.

B. RECORDS RETENTION STANDARDS

The following are comprehensive practices of state and federal agencies and may be helpful when staff reviews current policies or contemplates new policies.

1. Developing a plan. The Texas Department of Information Resources published a paper titled "Data and Electronic Records Management Best Practices" in April 2006. The guidance in the paper is based upon the Texas Administrative Code.[25] In its entirety, the paper is an excellent resource for those developing a records retention plan. The following is a summary of some of the important points of the paper.

An effective records management program is based upon a comprehensive framework for data and electronic record-keeping. In order to develop a comprehensive record-keeping program, input regarding which documents should be kept and for how long should be obtained from several sources, including records and information management staff, custodians of the records, legal counsel, creators of records, and the managers of the business units.

Texas has 10 key principles, which form the basis of their record-keeping strategy:

1) Creating Data and Electronic Records. Data and electronic records are created as evidence of business activity. Staff ensures that the legal and business requirements to create data and electronic records have been identified. Further, they ensure that systems that manage electronic records have record-keeping capability and business information systems without record-keeping capability are not used to capture or manage electronic records. Staff ensures that electronic records are captured in record-keeping systems.

2) Creating Information About Data and Electronic Records. Metadata about data and electronic records are captured and maintained. Staff develop policies and practices to ensure that standardized metadata are created and maintained to facilitate record keeping and disposition. The creation and capture of metadata occur as a normal part of business and record-keeping operations. Staff define metadata that need to be captured, ensure that the systems are capable of capturing metadata when data and records are created and during their management, and are responsible for accurately entering metadata and adhering to metadata standards. Classification tools must be developed to assist with titling, indexing, and retrieving data and electronic records.

3) Determining How Long to Keep Data and Electronic Records. Data and electronic records are to be retained and remain accessible until no longer required. Staff need to determine how long to keep data and electronic records to meet legal, business, and historical needs, based on the agency's approved records retention schedule. The agency should obtain data and records

[25] *See* 13 TAC 1 §§ 6.91–6.97 (Texas State Library and Archives Commission).

disposition authority through its approved records retention schedule, which identifies its business records in any format, including electronic. Staff ensure that the system is designed to allow the application of retention principles so that records that have met retention requirements can be identified and disposed of according to the retention schedule.

4) Storage Data. Electronic records data and electronic records should be stored in appropriate conditions so they will be accessible as long as they are needed. Staff should make sure records and data are stored on appropriate devices based on business need, preservation requirements, and costs. System backup tests must be performed, and integrity tests must be performed on storage devices. Media must be stored in conformance with standards accepted in the industry.

5) Security and authentication controls ensure that data and records are safe from intentional or unintentional damage or tampering. Security must be maintained according to the Department of Information's standards.[26] Procedures must be in place to identify and respond to incidents or attempted security breaches.

6) Business Continuity Planning for Data and Electronic Records. A business continuity plan must be developed for data and electronic records to prevent, prepare for, and recover from a disaster. Practices should be in place to minimize the risk of losing data and records if a disaster occurs. Vital data should be identified, and recovery and restoration procedures should be in place.

7) Data Preservation. The agency must have a strategy to make sure data are preserved and accessible for as long as required.

8) Access to Records. The agency must provide access to data and electronic records in accordance with state public disclosure laws. Mechanisms should be in place to supervise access to data and protect confidential information from unintended or unauthorized release.

9) Disposition of Records. Records are disposed of lawfully and according to policy. Disposition schedules should be in line with the agency policy and state law. Appropriate methods of destruction must be used.

10) Types of Records. Particular types of records such as instant messages; Web-based records, including data from the agency Web site; and records that are subject to online security processes must be managed appropriately.

Lastly and obviously, in order to have a successful program, senior management must commit resources to manage the records. [27]

2. Storage and maintenance of records. In Illinois, the Local Records Act [28] allows local government agencies to dispose of original records if the records are reproduced in a "durable medium that accurately and legibly reproduces the original records in all details" and the storage medium does not allow additions, deletions, or changes to the original document images. Digital records must be maintained in a trustworthy manner so that they are easily accessible. Any information that is a public record when originally produced in paper remains a public record when produced or maintained in a digital format and must be retained for as long as otherwise required by law. Disposing of records prematurely is a felony. Agencies should prepare documentation to explain how their systems and procedures ensure the authenticity and integrity of the document. The documentation should explain the technology that was used during the creation of the document, how the document enters the system, and the security measures that ensure that the document has not been altered. Word-processing software is constantly changing. Because of this, a document that was created on a common software 10 years ago may no longer be accessible, either due to a failure to keep the software updated or because the storage medium may deteriorate. The Illinois State Archivist suggests that digital records with a retention value of more than 10 years be backed up on microfilm or paper. Digital information should be stored off-site in a controlled atmosphere. Maintaining constant temperature and humidity is important for long-term preservation. Agencies should ensure that the digitizing system they select is usable for many years. The agency should be aware of and plan for the cost of hardware, software, employee training, scanning current and future files, and converting old records.[29]

Survey Results

The states that responded to the survey indicated that they currently use a mix of paper copies, microfilm, and scanning to servers to retain documents (see Appendix B). Minnesota is perhaps the most innovative, using paper, microfilm, digital copies, x-rays, and video to store documents. Recently, during a records collection project, they transcribed 10-year-old dictating tapes and took photographs of a plan that was 50 ft long. Vermont uses the following storage methods: microfilm, microfiche, paper, Mylar, blueprints, photos, carbon copies, digital images, OnBase software, COLD technology (Computer Output to Laser Disk–Reports), video logs, CADD software, PrintRoom for Plans, databases, accounting programs, CDs, DVDs, removable disk drives, flash drives, optical drives, and biometric drives.

Many states are either required by law to maintain the old systems for ease in accessing old records or to migrate old records into the new systems. Examples of these requirements include the following: In Wisconsin, agencies are required to retain old document storage

[26] 1 TAC 10 § 202.

[27] http://www.dir.state.tx.us/education/index.htm, last visited Apr. 4, 2009.

[28] 50 ILL. COMP. STAT. 205.

[29] Illinois Records Management Bulletin, *Guidelines for Electronic Records*, Apr. 2001, http://www.sos.state.il.us/departments/archives/records_management/electrecs.pdf.

systems so that old documents can be retrieved upon request.[30] The Texas Maintenance of Electronic Records Storage Media regulation requires the migration strategy for upgrading equipment as technology evolves to be documented and to include 1) periodically recopying to the same electronic media as required, and/or transferring of data from an obsolete technology to a supportable technology; and 2) providing backward system compatibility to the data in the old system, and/or converting data to media that the system upgrade and/or replacement can support.[31]

3. Calendars. The Environmental Protection Agency (EPA) established a protocol for senior officials' calendars. Those calendars are permanent government records under EPA's Record Schedule and must be preserved as permanent records. Staff members are required to make their electronic calendar their "official" calendar to avoid having to make copies of personal planners. Staff need to ensure that "substantive" calendar information for the time period is captured in the senior official's record-keeping system.[32]

Substantive calendar information includes information relating to official EPA activities, when the information has not been incorporated into memoranda, reports, correspondence, or other records included in the official files. Employees are required to print a copy of the calendar weekly and place it in their record-keeping system. At the end of each calendar year, the file is closed, maintained for 5 additional years, and then transferred to the National Archives.

4. E-mail. New Jersey developed its own "Guidelines and Best Practices for Managing Electronic Mail."[33] The guidelines are considered best practices for all state and local government agencies and are summarized below. The policy is intended to assist state employees in complying with New Jersey's Open Public Records Act,[34] as well as to promote best practices to facilitate the effective capture, management, and retention of electronic messages as public records. The guidelines contain the following directives:

Electronic mail is often used as a substitute for the telephone and to transmit information that in years past would have been transmitted via interoffice memo or the United States Postal Service. Government agencies must make their employees aware that e-mail messages, like paper records, must be retained and destroyed according to established records management procedures. Many states still do not include "e-mail" as a component of their record-keeping system for public records act purposes. However, e-mails are considered government records and must be treated as any other government records would be treated. An e-mail is a "record" if it serves to document the organization, functions, policies, decisions, procedures, or other activities. All e-mail messages that meet the criteria of the definition of a government record must be available to the public upon request unless they fall under the exceptions contained in the act or are otherwise exempt.

The schedule for retention and disposition of e-mail messages must be related to the information they contain or the purpose they serve. For instance, if the record will only be needed for a short period of time, a schedule may be set up to keep the record on site for a year, then to have it transferred to storage or destroyed.

Backing up all of the messages onto tapes or other media or purging all messages after a set amount of time is not an appropriate strategy for managing e-mail.

Management of E-mail

Record Copy. Messages are often widely distributed, but only one copy of the document should be retained. For example, a document outlining the current overtime policy of a department does not need to be retained by each person in the department. The logical person to retain that document is the one that created it. Generally, the person who sends the message and the primary recipient ("to," not "cc") should maintain the record copy of the message. Prompt deletions of duplicate copies of e-mails make the system easier to manage and reduce storage space.

Filing. Nontransitory messages should be filed in a way that enhances their accessibility. E-mail systems should be set up in a way that makes this easy. In addition to the "New" and "Sent" mail functions, other folders may be set up. New and sent mail should be transferred to folders that are set up by category. Additionally, provision should be made for storage of these documents on a long term basis. Employees should be responsible for classifying their messages according to content, the agencies' folder structure, and the records policy.

If messages are sent to a distribution list such as "Design Staff," a list of members of that distribution list must be kept as long as the message itself is kept. Descriptive subject lines should be used. For instance, "January 31 Traffic Meeting Minutes" is preferable to "Meeting Minutes."

Storage. Three types of systems may be used.

1) The online storage system is simply the storage of electronic information in the system that is being used by the agency. The e-mail message can be recalled at any time for reference or response. The cost and effect of storage on the system must be considered.

---

[30] WIS. ADMIN. CODE §§ 16.61, 16.661, 16.662.

[31] 13 TEX. ADMIN. CODE § 7.76.

[32] *See*, *e.g.*, Lisa P. Jackson, EPA Administrator, Memo to EPA Employees, Transparency in EPA's Operations (Apr. 23, 2009), available at http://epa.gov.administrator/operationsmemo.html (last visited June 16, 2009).

[33] State of New Jersey Circular Letter 03-10-ST: Managing Electronic Mail: Guidelines and Best Practices, http://www.state.nj.us/state/darm/links/pdf/circular-letter-03-10-st.pdf.

[34] N.J. Pub. L. 2001, c.404; the New Jersey Open Public Records Act (OPRA) Central is available at http://www.state.nj.us/opra.

2) Near-line storage is the storage of messages and other information in an electronic record-keeping system. The message, metadata, and attachments are removed from the online system and stored in electronic format. The files should be stored in a format that is compatible with the agency operations and filed according to the agency practices and that can be retrieved and referenced electronically. A filing system that is consistent with established practices should be used. These records may need to be protected from alteration.

3) Offline storage is the storage of data outside of an electronic environment, such as printing an e-mail to paper for storage in a paper file. It also includes storage on magnetic tape or optical disk. Messages may not be searchable or retrievable in electronic form.

Archiving of E-mail. Messages that need to be kept permanently should be removed from the electronic system and stored. Agencies must be aware of the potential for degradation of records if stored in an electronic format.[35]

Admissibility in Court. Courts require assurance that the systems in which records are retained are reliable. The reliability of the process or system used to produce the records determines their admissibility.

5. Electronic Records as Evidence. Part of the State of California Guidelines on Electronic Records includes a discussion on "electronic records as evidence," which is summarized here. Electronic records as a group are a much newer medium than paper or microfilm. If a person wants to introduce a record of a public agency into evidence, he or she must satisfy the court that the document is authentic and trustworthy. Electronic records are vulnerable to changes, and additional efforts must be taken to assure the court of their trustworthiness.

The content of a record may change if the equipment is not working properly. Because of this, an organization may be required to present evidence that the equipment was working properly on the day the computer record was prepared. The organization may also be required to prove that its system is free of errors in programs. This could be done using a witness familiar with the operation of the system. The organization may have to present the specific version of a computer program.

Retention schedules are considered evidence of the official retention period and specified disposal time. Although an approved records retention schedule for a requested record does not guarantee the court's acceptance of it, the fact that a record is scheduled for retention helps the agency meet the requirement of a record being created as a "regular practice" of the agency. Courts also acknowledge that records are disposed under an approved records policy. Courts have imposed penalties on entities that failed to have current records retention schedules or failed to follow established procedures to manage and safeguard records. If records are willfully withheld or the entity cannot demonstrate a good faith effort to find them, criminal sanctions could be imposed.[36]

C. Disposal of Records

In the states that have a retention policy, it is usually a crime to destroy records without lawful authority. No records should be destroyed while they still have historical or administrative value, but records should be destroyed when the cost to maintain them exceeds their usefulness to the organization. That determination is ultimately the responsibility of the state archivist or other authority responsible for determining the retention schedule.

An approved retention schedule is continuing authority to destroy records at the end of their scheduled retention period. With an approved schedule, an agency may destroy records at the end of their scheduled retention period.

Staff should remember that schedules do not replace good judgment. Records required for legal or audit purposes beyond the scheduled retention period must be maintained in an appropriate format until cleared for destruction by the appropriate authority.

Only confidential or otherwise protected documents should be destroyed using specialized equipment or methods due to their expense. Most paper documents can be recycled or disposed of using any method that actually destroys the documents.

D. Electronic Signatures

Electronic signatures have been incorporated into federal law under the ESGNCA[37] and UETA.[38] Most states have adopted a version of UETA.[39] An electronic signature is defined as "an electric sound, symbol or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record."[40] If used, electronic records must satisfy any formal requirements, such as notices, disclosures, or completeness of terms. For example, if the parties' e-mails show an agreement on the sale of widgets, a "quantity" term must be included in order to create a valid contract. Electronic records and signatures laws and acts satisfy the requirements under existing law, such as the statutes of fraud that require documents be signed in writing.

[35] New Jersey storage standards are set forth in N.J. ADMIN.CODE 15:3–6.

[36] *See* http://www.documents.dgs.ca.gov/osp/recs/erm-s4.pdf, last visited Apr. 4, 2009.

[37] 15 U.S.C. § 7001 *et seq*.

[38] The Uniform Electronic Transactions Act was completed by the Uniform Law Commissioners of the National Conference of Commissioners on Uniform State Laws in 1999, available at http://www.nccusl.org.

[39] *See*, *e.g*., Michigan Uniform Electronic Transactions Act, MICH. COMP. LAWS 450.831_450.849.

[40] *Id*.

The purpose of these types of laws is to place electronic documents and the use of electronic signatures on a par with traditional paper-based transactions and the use of manual signatures. They are intended to eliminate any doubt about the enforceability of electronic transactions and remove barriers to their use in the business, public, and government sectors.

One specific type of electronic signature is called a digital signature.[41] This term is used to denote the use of encryption technology that is used to enable a computer user to transmit a secure communication over the Internet or through any other open or closed network with a signature that has the same legal force and effect as a traditional handwritten signature on paper. The security features of a digital signature allow networked communications to be authenticated, confidential, and nonrepudiable.

In the workplace, managers should understand the risks and benefits associated with electronic signatures. They need to be able to identify the precautions that need to be put in place to prevent fraud and reduce the significant liabilities that can be associated with the uninformed use of electronic signatures. Managers must be able to make judgments about when the use of electronic signatures makes business sense.

The California UETA[42] recognizes and authorizes the conduct of business, public, and governmental affairs using electronic means. It applies to all the electronic records and signatures related to a transaction, and covers e-mails, reports, memoranda, accounting records, and any other electronic documents prepared in connection with a transaction.

Some of the most significant provisions of the California UETA are:

1. A record or signature may not be denied legal effect or enforceability only because it is in electronic form.
2. A contract may not be denied legal effect or enforceability only because an electronic record was used in its formation.
3. If a law requires a record to be in writing, an electronic record satisfies the law.
4. If a law requires a signature, an electronic signature satisfies the law.

Essentially, the UETA applies to transactions that the parties have agreed to conduct electronically. Under most circumstances, electronic records and electronic signatures may be used in place of traditional paper-based and handwritten methods.

E. Creating Records for Administrative Needs

This section will provide a general overview of types of records that should be collected and kept to prepare for litigation, historical, and business purposes in the human resources, construction, real estate, and personal injury litigation areas. The reader is cautioned to do his or her own research for a particular jurisdiction.

1. Human Resources

The chart in Appendix D is an analysis of personnel-related documents and the federal laws that are applicable to these types of documents. While every effort has been made to ensure that the laws cited herein are up to date, this publication is not a substitute for individual research in a particular jurisdiction.[43]

Performance Issues.—The agency should retain annual reviews, documentation of counseling sessions, and written warnings for at least 3 years. Before disposing of records of this type, counsel, the records retention policy, or human resources staff should be consulted. This retention period is dependent on internal policy as well as state law.

Discrimination Suits.—If a lawsuit of this nature is anticipated, any pre-suit materials should be gathered from the supervisor in preparation for claims, termination hearings, and the like. That information will typically be collected and retained by the human resources staff. Employee complaints and grievances should be documented in the same manner. Again, consultation with the human resources department is important to properly document files.

2. Construction Claims

Because a contractor may have as long as 10 years to bring a claim against a government agency, it is important to document events, conversations, and disputes before important information is lost or forgotten. A list of documents that an agency will likely collect during the course of a construction project and a suggested retention time can be found in Appendix E.[44] While every effort is made to ensure that reasonable retention periods are recommended, the reader should consult with counsel before determining a retention period for most documents.

3. Property Acquisition

Land is acquired for purposes of building or maintaining highways or for maintenance or administrative functions. A recommended chart for the retention of documents can be found in Appendix F.

4. Personal Injury Claim Through Litigation

Often a transportation agency or municipality can be sued if an injury or death occurs as a result of a "dan-

[41] *See* David P. Vandagriff, *In re Technology: Who's Been Reading Your Email? Two Easy-to-Use Tools Can Protect Privacy, Integrity of Documents*, 81 A.B.A.J. 98 (May 1995).

[42] *See* CAL. CIV. CODE §§ 1633.1–1633.17.

[43] *See* http://www.mnwfc.org/winona/record_retention_requirements1.htm, last visited Apr. 5, 2009.

[44] *See* Michigan Department of Transportation's June 2, 2008, memo entitled, Retention and Disposal of Construction Project Records, available at http://www.michigan.gov/documents/mdot_construction_record_requirements_109208_7.pdf.

gerous condition" of public property or, in some cases, if an employee operates a state vehicle negligently. It is important to gather information at or near the time of the crash or injury to document the condition of a road, a vehicle, or a construction zone before the evidence changes or is lost entirely.

When should information about an accident be gathered? The Missouri Department of Transportation (MoDOT) requires staff to inspect and photograph the sites of all serious and fatal accidents that occur on state highways. The risk management staff receives daily crash information from the highway patrol's database. Employees are trained to visit the scene, document the road conditions by taking photographs, and inspect for "dangerous conditions." These photographs are many times never used, but when litigation occurs, the state's photos are typically the photos taken closest in time to the crash and can be very useful.

Risk management and legal staff evaluate the accidents on a case-by-case basis. If it seems almost certain that litigation will occur, such as when a highly publicized accident occurs, additional steps may be taken. Sometimes an independent accident reconstructionist will be retained immediately so that accurate measurements of sign spacing and skid or scuff marks will be preserved or so that speeds of vehicles can be determined. Witness statements may be taken if witnesses can be located through information on the police report or through other means.

If a crash occurs in a maintenance work zone or construction zone, onsite staff document the warning signs and other warning devices such as changeable message boards and arrow boards and take statements from workers on the scene. Most state vehicles are equipped with disposable cameras, and most shops are equipped with digital cameras. It is also prudent to gather construction plans, work orders, traffic control plans, and any other paper documents that outline the traffic control that was required or planned for the job. Employees are also encouraged to document property damage repair costs, including materials and staff time.

Protection of Information.—Although the terms "work product" and "attorney client privileged" are at times used interchangeably, the two doctrines are separate. If a relevant matter is privileged, it has complete immunity from discovery. A few recent cases in this area are discussed in this section; however, the reader is warned to carefully research the jurisdiction in question before asserting either of these privileges.

The work product rule is a qualified immunity from discovery that may be overcome by a proper showing. However, in ordering discovery of trial preparation materials where this showing has been made, a court should always protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of the party concerning the litigation.[45]

The *Brown v. Katz*[46] court discussed Indiana Trial Rule 26(B)(3), which defines the work product privilege. It provides that a party may obtain discovery of documents and tangible things otherwise discoverable and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative only upon a showing that the party seeking discovery 1) has a substantial need for the materials in the preparation of his or her case, and 2) is unable without undue hardship to obtain the substantial equivalent of the materials by other means. The court noted that a document is gathered in anticipation of litigation if it can be said that the document was prepared or obtained because of the prospect of litigation.

Products of investigation are "work product" because their subject matter relates to the preparation, strategy, and appraisal of the strengths and weaknesses of an action or to the activities of the attorneys involved. The *Brown* court cited *Howard v. Dravet*[47] for the proposition that a claim of work product privilege must be asserted "on a document-by-document basis."

In *Brown*, the court discussed the statutory source of the attorney-client privilege, which is found in Indiana Code Section 34-46-3-1. It reads "except as otherwise provided by statute, the following persons shall not be required to testify regarding the following communications…[a]ttorneys, as to confidential communications made to them in the course of their professional business, and as to advice given in such cases." The attorney-client privilege protects against judicially-compelled disclosure of confidential information. The court noted that the harm that is intended to be prevented by the law is not the manner in which the confidence is revealed, but the revelation itself.

Asserting the Privilege.—When a party withholds information that would otherwise be discoverable under the rules of civil procedure by claiming that it is privileged or subject to protection as trial preparation material, that party must describe the type and nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection. This is usually done by producing a privilege log that sets out the type of documents or materials that are protected.

The written statement of a witness, whether prepared by the witness and later delivered to an attorney or drafted by the attorney and adopted by the witness, is not properly considered work product of an attorney, because it records the mental impressions and observations of the witness himself or herself and not those of the attorney. What a witness knows is not the work of counsel.

In some jurisdictions, where the work product doctrine is concerned, protection under the state Public Records Act applies to materials created in anticipation

[45] *See* B*rown v. Katz*, 868 N.E.2d 1159 (Ind. Ct. App. 2007).

[46] *Id.*

[47] 813 N.E.2d 1217, 1222 (Ind. Ct. App. 2004).

of litigation, even after that litigation has terminated. In *Soter v. Cowles Pub. Co.,*[48] documents that were created by or gathered by members of a school district's legal team in anticipation of a potential wrongful death claim against the district by the parents of a student with a peanut allergy to whom the district served a peanut butter cookie were found to be "work product" for purposes of the exemption under the Public Records Act. The court determined those documents were materials that would not be discoverable in the context of a controversy under the civil rules of pretrial discovery. The court also found that an attorney or legal team's notes regarding witness interviews were "highly protected" opinion work product, for the purposes of the civil rule that codified the work product doctrine.

Practical Considerations

In Missouri, staff are instructed to write their incident narratives to the attention of their counsel, rather than their supervisor, so that there will be no doubt later on that the statement was taken in anticipation of litigation. A form has been developed that assists employees in writing their statement. The form organizes the statement in a "who, what, when, where, why and how" format so that all the basic information will be gathered (attached as Appendix H).

III. RELEASE OF ELECTRONICALLY STORED INFORMATION—LITIGATION AND DISCOVERY

This section discusses the federal rules of civil procedure relating to ESI in the discovery and litigation contexts and provides an outline for best practices in discovery.[49]

Digital documents are very different from their paper counterparts. Electronic data can change when moved, copied, or opened. When data change, they become different, discoverable data that look almost exactly like the other data. For that reason, it is important to understand the complexity of an electronic records request and the dangers in failing to respond appropriately when undertaking a response to the request.

Federal Rules 26, 33, 34, 37(f), and 45 were modified in 2006 to include references to ESI. The updates had several purposes. The new rules amended existing rules to include provisions that acknowledged that ESI is widely used and discoverable, required parties to discuss ESI discovery issues early in the litigation, and theoretically reduced the cost of ESI discovery by creating a presumption that ESI that is not reasonably accessible because of excess cost or burden is not discoverable.

The federal courts must both enforce the parties' duties to find and preserve ESI and attempt to minimize discovery costs. "The tension between these competing interests has been exacerbated by the information technology revolution. Courts are now facing the challenge of overseeing discovery at a time when potential access to electronically stored information is virtually limitless, and when the costs and burdens associated with full discovery could be more outcome-determinative, as a practical matter, than the facts and substantive law."[50] Federal Rule of Civil Procedure 26(b)(2)(B) gives the courts the tools to balance these competing interests.

A. Federal Rule 26

Federal Rule 26(b)2(B) limits the release of ESI. "A party need not provide…if not reasonably accessible because of undue burden or costs." The notes from the rules define "reasonably accessible" data as data that are used in the ordinary course of business or available with little time or expense. "Unreasonably accessible" data are defined as data on systems that are no longer used, deleted data, and data from disaster recovery tapes that are not searchable.

When answering discovery requests, parties must identify information by category or type if it contains potentially responsive materials that are not being searched or produced. The responding party is required to preserve the information even if it is not searching or producing the materials, so that it is available if a court later orders it to be produced.

1. Reasonable Accessibility

The court in *Zubulake v. UBS Warburg*[51] broke electronic data down into the following five categories, listed in order of most accessible to least accessible: 1) active online data, such as hard drives; 2) near-line data such as robotic storage devices like optical disks; 3) offline storage/archives, which are removable optical disks or magnetic tape media that can be labeled and stored in a shelf or rack; 4) backup tapes such as tape recorders that read data from and write it onto a tape; and 5) erased, fragmented, or damaged data that can only be accessed after significant processing.

While the court considered the first three categories of data noted in *Zubulake* "accessible" and the last two categories "inaccessible," it is certainly possible that changes in technology could make previously inaccessible data less expensive and easier to access.

In reviewing a discovery request to determine whether information requested is accessible or inaccessible, the court may also consider the specificity of the request; the quantity of information available from other and more easily accessed sources; the failure to produce relevant information that seems likely to have existed but is no longer available on more easily ac-

[48] 162 Wash. 2d 716, 174 P.3d 60 (Wash. 2007).

[49] *See also The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production*, http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf.

[50] Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614 (D. Colo. 2007).

[51] 217 F.R.D. 309, 311 (S.D.N.Y. 2003).

cessed sources; the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; predictions as to the importance and usefulness of the further information; the importance of the issues at stake in the litigation; and the parties' resources. [52]

The courts may set out specific e-discovery guidelines. In *O'Bar v. Lowe's Home Centers,*[53] the district court *sua sponte* ordered discovery guidelines, requiring the parties to identify ESI that was or was not reasonably accessible without undue burden or cost, the identity of the sources of information and the reason for the party's contention that the ESI was or was not reasonably accessible without undue burden or cost, the methods of storing and retrieving that ESI, and the anticipated costs and efforts involved in retrieving that ESI. The court set out lengthy guidelines for the parties and directed them to follow the "Suggested Protocol for Discovery of Electronically Stored Information" as set forth by the United States District Court for the District of Maryland. The Maryland protocol can be found as Appendix G.

2. Undue Burden

In *Equal Employment Opportunity Commission v. Boeing Company,*[54] the court addressed an e-discovery dispute, analyzing plaintiff's request to discover "[a]ll bases for Boeing's position that retrieval of e-mails" responsive to its requests for production of documents would cost at least $55,000. Plaintiff argued that the information requested was relevant to its claims and therefore discoverable pursuant to Rule 26(b)(1), Federal Rules of Civil Procedure, because "it will allow the EEOC to determine whether Boeing has any basis for its cost assertions and whether any asserted basis are legitimate." The court concluded that defendant made the showing, pursuant to Rule 26[(b)(2)(B)], that "the information sought is not reasonably accessible because of undue burden or costs," and that plaintiff did not show good cause to justify the expense of the proposed discovery for purposes of Rule 26(b)(2)(B).

3. Payment to Retrieve Inaccessible Data

In *Semsroth v. City of Wichita*,[55] female officers of the city police department filed suit alleging sexual harassment, hostile work environment, gender discrimination, and violations of their equal protection and due process rights. Plaintiffs requested e-mails that had been deleted in compliance with the records retention policy. Plaintiffs argued that a search of current active files would be inadequate because there was no way to obtain information regarding the past deleted e-mails. The backup tapes that were requested were the only source of information regarding the e-mails that were in existence on July 23, 2004. The parties disagreed on who should pay to retrieve the documents. The city kept backup tapes for disaster recovery purposes only, and not to retrieve information. To conduct a word search of the e-mails contained on a given backup tape, the city would have to restore the backup tape to an e-mail server. Despite the hardware's availability, the labor costs to retrieve the information were substantial. The court noted that where the storage media is reasonably related to the purposes for which the information is retained, it will not automatically require that party to bear the costs of retrieving the information. The court decided that the scope of the search of the e-mails should be limited in two respects: the court limited the search by allowing plaintiffs' access to only one backup tape for the date in question and further pared down the search by ordering fewer terms to be searched.

Another case of interest is *AAB Joint Venture v. United States.*[56] This construction litigation was based upon plaintiff's claim that site conditions were different than contemplated by the original design plans. Gaps in available government e-mails prompted the court to order defendant United States to restore 25 percent of the e-mail backup tapes in the time period requested by the plaintiff. Plaintiff then had the opportunity to review the responsive material to determine if it contained relevant evidence and if additional restoration of backup tapes was warranted. This approach allowed the court to do a benefit-burden analysis before making the determination of whether to require costshifting or costsharing.

In *Disability Rights Council of Greater Washington v. Washington Metro Area Transit Authority* (WMATA),[57] plaintiffs claimed WMATA failed to provide adequate paratransit services through the MetroAccess program. They further claimed that the service provided was materially inferior to the Metrorail and Metrobus services available to people without disabilities. Plaintiffs requested that the court order WMATA to produce backup tapes of electronic documents that were written and received since the filing of the lawsuit. WMATA had a policy of deleting all e-mails after 60 days. Even though the lawsuit was filed on March 25, 2004, WMATA did not stop its e-mail system from obliterating the older e-mails until, at the earliest, June 2006. As a result, with the exception of three individuals, all possibly relevant and discoverable emails had been purged every 60 days for a period of 3 years. The court ordered the transit authority to produce the documents and shoulder the cost.

---

[52] George B. Murr, *Federal Rule of Civil Procedure 26(b)(2)(B) and "Reasonable Accessibility": The Federal Courts' Experience in the Rule's First Year*, RECORDS RETENTION REPORT, Dec. 2007, *available at* http://www.bmpllp.com/publications/articles.php?action=display_publication&publication_id=106.

[53] 2007 U.S. Dist. LEXIS 39205 (W.D.N.C. May 2, 2007).

[54] 2007 U.S. Dist. LEXIS 29107 (D. Ariz. Apr. 18, 2007).

[55] 239 F.R.D. 630 (D. Kan. 2006).

[56] 75 Fed. Cl. 432 (Fed. Cl. Ct. 2007).

[57] 2007 WL 1585452 (D.D.C. June 1, 2007).

4. Mistakenly Producing Privileged Information

Rule 26(B)(5) protects information that was not found during the review prior to production that is later determined to be privileged. The producing party may designate material as "privileged" after it is produced.

Courts require counsel to be quite technologically sophisticated in responding to discovery requests. In *Victor Stanley v. Creative Pipe*,[58] plaintiff requested a ruling that 165 electronic documents inadvertently produced by defendants were not privileged because their production occurred under circumstances that waived any privilege or protected status. The parties had agreed to a joint protocol to search and retrieve relevant ESI responsive to plaintiff's requests. The protocol contained detailed search and information retrieval instructions, including nearly five pages of keyword/phrase search terms aimed at locating responsive ESI. During the review process, potentially privileged documents were overlooked and produced to plaintiff. The court noted that:

> [I]t is universally acknowledged that keyword searches are useful tools for search and retrieval of ESI, [however] all keyword searches are not created equal; and there is a growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches for privilege review…common sense suggests that even a properly designed and executed keyword search may prove to be over-inclusive or under-inclusive, resulting in the identification of documents as privileged which are not, and non-privileged which, in fact, are. [59]

In *Corvello v. New England Gas Co.*,[60] the Rhode Island Department of Environmental Management (RIDEM) sought a protective order and the return of allegedly privileged documents that it claimed to have inadvertently produced in response to a subpoena *duces tecum* issued by New England Gas Company, Inc. (NE Gas). NE Gas contended that the documents were not privileged and that, even if they were, any privilege was waived by RIDEM's failure to properly assert the privilege and by RIDEM's failure to take timely corrective action after learning of the disclosure. The motion for a protective order was denied and information that may have otherwise been protected was ordered to be disclosed.

Federal Rule of Evidence 502 was recently enacted to address the challenges associated with electronic discovery. The rule enables litigants to exchange materials without waiving privilege or work product protection. It is intended to reduce the burdens associated with e-discovery (and the often massive exchange of materials in electronic format), provide clear guidance to courts and parties on waiver of attorney-client privilege and work product protection, avoid the broad waiver of privilege and work product protection by the disclosure of materials in discovery, and protect parties that enter into nonwaiver agreements. However, exactly how Rule 502 will operate is open to debate, as the courts at the time of this writing have not had an opportunity to interpret or apply it.

B. Federal Rule 33

Federal Rule 33(d) states that if the answer to an interrogatory can be determined by providing business records rather than answering the interrogatory, the answering party may produce the records. The answering party may produce records either electronically (stored on disk or CD) or hard copy. The responding party may only substitute access to the records for the actual records if the burden of deriving the answer will be the same for both parties. The recipient must be able to locate and identify information as readily as the answering party.

In *Jackson v. City of San Antonio*,[61] the court considered a dispute over the Fair Labor Standards Act[62] records. Plaintiffs objected to defendants' production of computerized pay and time records in response to several of their interrogatories and production requests as being an unauthorized "data dump." Plaintiffs complained that counsel failed to include necessary field descriptors on their response. Plaintiffs argued that without the field descriptors, the records were unhelpful, unusable, and nonresponsive. Defendants responded that because the business records contained the information plaintiffs requested and because the burden of culling out the requested information was no greater for plaintiffs than it would be for defendants, the rules allowed defendants to respond by producing their business records. Defendants also explained that because plaintiffs had not identified the particular work weeks for which each claimed entitlement to Fair Labor Standards Act overtime wages, they were unable to identify the particular records for particular weeks for which they sought an offset or credit. The court found that the computerized records were an adequate response to these discovery requests.

C. Federal Rule 34

Federal Rule 34 states that production of ESI encompasses more than simply documents. Any party may serve another party with a request to produce any designated documents or ESI, including writings, drawings, graphs, charts, photographs, sound records, or images. The response must be reasonably usable.

Production of Metadata

In *Aguilar v. Immigration and Customs Enforcement Division of U.S. Department of Homeland Security*,[63] the plaintiffs in a civil rights class action claimed that

[58] 250 F.R.D. 251 (D. Md. 2008).

[59] *Id.* at 257.

[60] 243 F.R.D. 28 (D.R.I. 2007).

[61] 2006 WL 487862 (W.D. Tex. Jan. 2006).

[62] The Fair Labor Standards Act of 1938, Pub. L. No. 75-718, 52 Stat. 1060 (June 25, 1938 (codified at 29 U.S.C., ch. 8)).

[63] 2008 WL 5062700 (S.D.N.Y. Nov. 2008).

armed immigration officers had entered and searched homes of Latinos without obtaining a search warrant or consent. Production of documents with metadata included was not a subject at the parties' Federal Rule of Civil Procedure 26(f) discovery conference or in plaintiffs' first request for production of documents. Later, plaintiffs requested e-mail and electronic documents in Tagged Image File Format (TIFF) with corresponding metadata fields and production of spreadsheets and databases in native format. The court granted plaintiffs' motion to compel the production of metadata for any Word™ or PowerPoint™ documents only as long as plaintiffs were willing to bear the cost of a second production.

Similarly, in *Autotech Techs Ltd. Partnership v. AutomationDirect.com, Inc.*,[64] defendant sought the production of a document with metadata. However, plaintiff had already produced the document in both portable document format (PDF) on a CD and paper format, and had provided a "Document Modification History" showing a chronological list of all changes made since the document was created. Defendant wanted the electronic version of the document and wanted to know when the document was created, when it was modified, and when it was designated "confidential." Defendant argued that the document had to be produced with metadata since the metadata existed in its "native format" on a computer at Autotech's offices in Iowa. The court considered whether either the PDF file or the hard copy was a reasonably usable form under Federal Rule of Civil Procedure 34(b)(2)(E). Defendant argued that the production was not usable because it did not contain things that metadata would contain, like the history of the document. However, the court noted that the paper copy of the document included a nine-page history of the changes made to the document from its creation on February 9, 2000, to March 2, 2007. Further, the court pointed out that defendant had not specified that it wanted metadata to be produced, and that there was no mention of metadata in earlier motions to compel. It commented "it seems a little late to ask for metadata after documents responsive to a request have been produced in both paper and electronic format. " The court cited *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery*[65] with approval.

D. Federal Rule 37

Federal Rule 37 deals with the parties' failure to provide information. The courts recognize that some information will be lost during the regular operation of a computer system. Sanctions will not be imposed for the loss of ESI during routine and good faith operations of the computer system. However, a litigant cannot exploit a routine operation by allowing a system to continue destroying information that it is required to preserve.

1. Sanctions

The courts are harsh when dealing with parties who have intentionally destroyed electronic evidence. In *Kucala Enterprises Ltd. v. Auto Wax Co., Inc.,*[66] the court addressed plaintiff's use of a computer program titled "Evidence Eliminator" before a deposition. Defendant Auto Wax argued that Kucala's use of the Evidence Eliminator program on two computers, throwing away an older computer, and otherwise destroying discoverable information and documents severely prejudiced Auto Wax in that it could not discover evidence to successfully defend itself in the underlying action. The court ruled that Kucala flagrantly disregarded a court order requiring him to allow inspection of his computer and further commented on his "utter lack of respect" for the litigation process. The court found that Kucala's actions were unreasonable, and that he was at fault for not preserving evidence in his control, which he had a duty to maintain. The court recommended Kucala's suit be dismissed and some of defendant's attorneys fees reimbursed.

In *Munshani v. Signal Lake Venture Fund II,*[67] the court appointed a computer forensics expert to determine whether a certain e-mail purportedly sent by defendant Hemant Trivedi to plaintiff Suni Munshani was authentic. The expert concluded that the message was not authentic. The expert established that Munshani took the header from another e-mail sent to him by Trivedi, altered the substance of that e-mail, and then provided the altered e-mail in response to discovery and swore that it was authentic in affidavits to the court. Plaintiff's lawsuit was dismissed, and the plaintiff was ordered to reimburse the defendants for their costs.

Spoliation of Evidence.—"Spoliation" has been defined as "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[68] In *Zubalake v. UBS Warburg LLC*,[69] the court held that plaintiff must establish three things to obtain spoliation sanctions: the party having control over the evidence had the obligation to preserve it at the time it was destroyed, the records were destroyed with a "culpable" state of mind, and the destroyed evidence was relevant to the parties' claim such that a reasonable trier of fact could find it supported the claim.

Stevenson v. Union Pacific Railroad[70] involved a wrongful death and personal injury claim due to a railroad crossing accident. The plaintiffs filed a motion for sanctions because Union Pacific destroyed both a voice

[64] 248 F.R.D. 556 (N.D. Ill. 2008).

[65] The Sedona Conference Working Group Series, July 2005 version.

[66] 56 Fed. R. Serv. 3d 487 (N.D. Ill. 2003).

[67] 2001 WL 1526954 (Mass. Super. Ct. Oct. 9, 2001).

[68] *See* West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999).

[69] 229 F.R.D. 422 (S.D.N.Y. 2004).

[70] 354 F.3d 739 C.A. 8 (8th Cir. 2004).

tape of conversations between the train crew and dispatch at the time of the accident and track maintenance records from before the accident. Union Pacific argued that sanctions were not justified because it destroyed the documents in good faith pursuant to its routine document retention policies.

The district court applied the following test in analyzing the case: 1) whether the record retention policy was reasonable considering the facts and circumstances surrounding those documents, 2) whether lawsuits or complaints had been filed frequently concerning the type of records at issue, and 3) whether the document retention policy was instituted in bad faith.

The appellate court found that the district court's bad faith determination was supported by Union Pacific's destruction of the voice tape pursuant to its routine policy when Union Pacific knew that the tapes would be important to any litigation over an accident that resulted in serious injury or death and knew that litigation is frequent when there has been an accident involving a death or serious injury. The court noted that the tape was the only recording of the conversations at the time of the accident, and a tape such as that would always be highly relevant to potential litigation over the accident. The court also considered evidence that Union Pacific was careful to preserve a voice tape in other cases where the tape proved to be beneficial to Union Pacific. The court found that the pre-litigation destruction of the voice tape in this combination of circumstances, even though done pursuant to a routine retention policy, created a sufficiently strong inference of an intention to destroy it for the purpose of suppressing evidence of the facts surrounding the operation of the train at the time of the accident and imposed sanctions against the railroad.

In *United Medical Supply Co. v. United States of America*,[71] the federal government was sanctioned when it failed to follow its own document retention policy and destroyed relevant documents in a suit against it for recovery of lost profits and payments. The court prohibited the government from cross-examining contractor's expert regarding gaps in the record created by government's spoliation and from adducing its own expert testimony construing the same gaps. The government was further sanctioned by the court's requirement for it to reimburse the contractor for any additional discovery-related costs, including attorney's fees that were incurred after discovery began. The court pointed out that it was "[M]ost disturbing [that] some of these documents were destroyed even after the court conducted its first spoliation hearing." Even though defendant apologized for what it claimed was the "negligence" of some of its employees and for making repeated misstatements to the court as to the steps that were being taken to prevent spoliation, the government also told the court that it should not—or could not—impose spoliation sanctions because the defendant did not proceed in bad faith. The court commented that "[w]hile defendant may be wrong in asserting that it acted in good faith, it most certainly is wrong in thinking that it can recklessly disregard its obligations to preserve evidence without legal consequence."

2. Litigation Hold

The duty to preserve documents begins when the "litigant knows or should know the evidence is relevant to imminent or ongoing litigation."[72] The court in *Toussie v. County of Suffolk*[73] considered the county's failure to initially perform a diligent search for e-mails responsive to plaintiff's request. The county advised the court that to perform the search requested by plaintiffs, it would be necessary to restore 470 backup tapes, which required a new system to be purchased at a cost of approximately $934,000. The county estimated that the search would then take 960 man-hours to complete. The court found that once the duty to preserve attaches, a litigant is expected, at a minimum, to "suspend its routine document and record destruction policy and to place a litigation hold" and ruled against the county.[74]

Practical Considerations—Implementing Litigation Hold.—When it is apparent that a lawsuit is going to ensue, the obligation to preserve any and all related information should be communicated throughout the agency. Every employee that may be affected by the lawsuit should be made aware of the situation and educated on the type of information that would logically apply to a litigation preservation order. Counsel should create a procedure by which staff can adhere to the obligation without interfering too much with day-to-day work. If it is too early to set up a procedure, counsel can specify temporary actions that people can take and simply identify a time period when a more formal plan will be put in place.

Practical Considerations—Responding to an E-Records Request.—Counsel is ethically obligated to be familiar enough with his or her client's computer systems and their inner workings to engage in electronic discovery. Counsel has to have a basic understanding of the computer system's capabilities and the way the agency's system retains, stores, and destroys information. It is important to know the agency's policy regarding e-mail and other document retention methods. Before attempting to respond to an e-records request, counsel must consult with the information systems department to learn the important areas of the computer systems operations and how those systems interact with each other. Locations to become familiar with are centralized e-mail systems, database tracking systems, accounting and financial systems, and backup and dis-

[71] 77 Fed. Cl. 257 (2007).

[72] United States *ex rel*. Koch v. Koch Indust., 197 F.R.D. 463 (N.D. Okla. 1998).

[73] 2007 WL 4565160 (E.D.N.Y. Dec. 2007).

[74] *See also* Doe v. Norwalk Cmty. Coll., 2007 WL 2066496 (D. Conn. July 16, 2007), where the court held that a party needs to act affirmatively to prevent its computer system from destroying information even if such destruction would occur in the regular course of business.

aster recovery systems. Counsel should find out where backup data are stored and whether they can be retrieved, if necessary.

Supporting systems could also contain valuable stored information. Fax servers sometimes save copies of all transmissions in and out of an organization. Safety systems, such as antivirus applications, may log files that pass through the networks, and other systems, such as computer servers, may store Internet traffic and e-mail forwarding information. It may also be necessary to retrieve documents from employees' home computers or zip drives if employees work from home or transport data from work to home or vice versa.

As information is collected, a list should be made of every employee who provides information responsive to the request. The list should identify information that each user has access to in addition to physical locations that may collect or store information. These data can be collected in a chart format that is similar to that used for collecting medical records in a personal injury lawsuit.

Determining what information is relevant to the case is the responsibility of the producing party, although in situations that may be contested it is important to save information that may turn out to be relevant to avoid spoliation accusations. Obligations to preserve and capture information should be identified early on in the process and defined to limit the scope of the search to relevant information and also to avoid excessive costs.

After relevant information has been identified and located, it must be collected. Computer staff, under the guidance of counsel, should create exact copies of stored information. When preserving electronic files, it is important to remember that copying information for the purpose of responding to a discovery request may change the original data.

According to Federal Rule of Civil Procedure 30(b)(6), a party responding to a discovery request must designate a person who can help the requesting party understand where information is stored. That person must be made available for deposition. It is important to remember that the method of data collection is discoverable.

Before the data are prepared for review by counsel, every document should be accessed and metadata extracted. Each piece of information should be saved in a central database for sorting, searching, and use in the review process later on. Every document should be inspected for privileged information, trade secrets, and relevancy. There are many computer applications available that allow for easy importing and accessing of information. The format in which the information is released to the opposing party should be agreed upon prior to the release of the information.[75]

[75] Some of the material in this section was taken from an article written by Paul J. Neale, Jr., American Law Institute-American Bar Association, appearing in *Electronic Records Management and Digital Discovery*, 2005.

IV. OPEN RECORDS

Government should be transparent, and its records should be open and readily accessible to the public. This theme is repeated again and again in the headlines and echoed in judicial opinions. However, the courts, the legislature, and the public still recognize that some information should be exempt from disclosure and kept from the public eye. This section will discuss trends in federal and state open record laws as they relate to transportation issues.

A. The Freedom of Information Act[76]

Essentially the Freedom of Information Act (FOIA) requires the release of all nonexempt public records. The exemptions are set out below.

Exemption 1—Classified Matters of National Defense or Foreign Policy. This exemption protects national security information concerning the national defense or foreign policy, provided that it has been properly classified in accordance with the substantive and procedural requirements of an executive order.

Exemption 2—Internal Personnel Rules and Practices. This exemption protects mandatory disclosure records "related solely to the internal personnel rules and practices of an agency."

Exemption 3—Information Specifically Exempted by Other Statutes. This exemption incorporates the disclosure prohibitions that are contained in various other federal statutes.

Exemption 4—Trade Secrets, Commercial, or Financial Information. This exemption protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."

Exemption 5—Privileged Interagency or Intra-Agency Memoranda or Letters. This exemption protects "inter-agency or intra-agency memorandums of letters which would not be available by law to a party…in litigation with the agency." It has been construed to exempt those documents that are normally privileged in the civil discovery context.

Exemption 6—Personal Information Affecting an Individual's Privacy. This exemption permits the government to withhold all information about individuals in personnel and medical files and similar files when the disclosure of such information would constitute a clearly unwarranted invasion of personal privacy. This exemption is not to be used to withhold information a person requests about himself or herself.

Exemption 7—Investigatory Records Compiled for Law Enforcement Purposes.

Exemption 8—Records of Financial Institutions. This exemption covers matters that are contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.

[76] 5 U.S.C. 552, current through 111 Pub. L. No. 25 (2009).

Exemption 9—Geographical and Geophysical Information Concerning Wells. This exemption covers geological and geophysical information and data, including maps, concerning wells.

The USDOT implemented FOIA through 49 C.F.R. Section 7. The regulation is comprehensive and a good resource for an agency that is establishing or considering changes to their open records policy.

The FOIA exemptions and exclusions discussed in this section are national security in the context of national infrastructure security, trade secrets, and commercial information and material that is protected by other federal laws. Several other laws as they relate to transportation issues are discussed. There are many other resources that discuss all of the FOIA exemptions. This publication simply attempts to discuss the exemptions applicable to transportation agencies.[77] The following is a discussion of trends that have been noted in recent FOIA decisions.

1. FOIA Exemption 1—National Security

Several courts have considered the national security exemption as it relates to the protection of information outlined in the Homeland Security Act of 2002[78] and the Critical Infrastructure Act.[79] In *Coastal Delivery Corp. v. United States Customs Service*,[80] a trucking company involved in a tort claim requested information about the number of inspections performed on goods at a Southern California seaport. The customs service refused to release the information, claiming that its release would allow terrorists to more easily avoid detection when smuggling items into American ports. The court agreed, reasoning that even if the information about the particular port in this case might not prove damaging, if the government were forced to release information about all of its ports, it would allow terrorists to determine which ports were the most lightly inspected and, therefore, the easiest in which to carry out illegal activities.

Similarly, in *Judicial Watch v. Department of Transportation,*[81] the D.C. District Court allowed the USDOT to withhold the locations of warehouses where explosive detection devices made for use by the Transportation Security Administration were maintained before being sent to airports. The court accepted the argument that disclosure of the locations of these warehouses would place national security at risk.

Similarly, in *Living Rivers, Inc. v. United States Bureau of Reclamation*,[82] a Utah federal district court held that inundation maps prepared by the U.S. Bureau of Reclamation for the areas below the dams were exempt from disclosure. Terrorists could use the maps to estimate the extent of flooding that would be caused by attacking individual features of the dam and to compare the amount of flooding and damage that would result from attacking one dam as compared to attacking another dam.

2. FOIA Exemption 3—Information Protected by Specific Legislation

a. The Homeland Security and Critical Infrastructure Acts.—The Homeland Security[83] and Critical Infrastructure Acts[84] were enacted in response to the events of September 11, 2001. The Critical Infrastructure Information Act of 2002[85] is part of the broader Homeland Security Act (the Act). Several parts of the two acts are pertinent to transportation agencies. The Act specifically exempts sensitive information from release under the FOIA.

> Critical infrastructure information, including the identity of the submitting person or entity, that is voluntarily submitted to a covered federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement…shall be exempt from disclosure under [the Freedom of Information Act].[86]

Within the Act, the term "critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[87] The Act then provides a list of "covered agencies" that includes federal, state, and local agencies. The law requires the voluntary provider of written material to mark sensitive material with a statement reading, "This information is voluntarily submitted to the federal government in expectation of protection from disclosure under the provisions of the Critical Infrastructure Information Security Act of 2001."[88]

The House Government Reform Committee amended the original language of the Act to provide that voluntarily submitted critical infrastructure information "will

[77] *See* ORRIN F. FINCH & GARY A. GEREN, FREEDOM OF INFORMATION ACT, FEDERAL DATA COLLECTIONS AND DISCLOSURE STATUTES APPLICABLE TO HIGHWAY PROJECTS AND THE DISCOVERY PROCESS (NCHRP Legal Research Digest 33, 1995). The text of the Federal Freedom of Information Act can be found at 5 U.S.C. § 152.

[78] Pub. L. No. 107-296, 116 Stat. 2135, codified at 6 U.S.C. § 101 *et seq*.

[79] The Critical Infrastructure Information Act of 2002 (CIIA), codified at 6 U.S.C. §§ 131–34, was passed on Nov. 25, 2002, as subtitle B of Title II of the Homeland Security Act, §§ 211–15.

[80] 272 F. Supp. 2d 958 (C.D. Cal. 2003).

[81] 2005 WL 1606915 (D.D.C. 2005).

[82] 272 F. Supp. 2d 1313 (D. Utah 2003).

[83] Pub. L. No. 107-296, 116 Stat. 2135, 6 U.S.C §§ 101 *et seq*.

[84] Pub. L. No. 107-56, 115 Stat. 400, 42 U.S.C. § 5195c.

[85] 6 U.S.C. §§ 131–34.

[86] 6 U.S.C. § 133(a)(1) and (1)(A).

[87] *See* 6 U.S.C. § 101(4), referencing 42 U.S.C. § 5195c.

[88] 6 U.S.C. § 133(a)(2)(A).

not be subject to agency rules or judicial doctrine regarding ex-parte communications, nor used directly in civil actions if that information is submitted in good faith." Further, the Committee stated that "disclosure of information under this section does not constitute waiver of legal privilege or protection, such as trade secret protection."[89] The Homeland Security Act requires federal officials who "advise, alert, [or] warn" of critical infrastructure threats to withhold any voluntarily submitted critical infrastructure information as well as "information that is proprietary, business sensitive, or otherwise not appropriately in the public domain."[90] Officials who hold sensitive information gathered by others must treat that information as sensitive.

At the time of this writing, there is little case law interpreting either of the two acts. In *Tombs v. Brick Township Municipal Utilities Authority,*[91] appellant requested access to a topographic map in digital format from the Brick Township Municipal Utilities Authority (BTMUA). The geographic information system (GIS) data included maps and information on treatment facilities, information systems, and distribution lines of BTMUA that could not be separated from the software program used to access and manipulate the data. BTMUA's Executive Director denied the request, claiming the information sought was proprietary, subject to alteration, and concerned the township's "critical infrastructure" or "assets" in need of protection under New Jersey's Domestic Security Preparedness Act. BTMUA offered to provide appellant with paper copies of maps of the Brick Township for $5. BTMUA submitted an application for protection of the map to the Department of Homeland Security (DHS). DHS granted protected critical infrastructure information status to the material, declaring that it would be "handled and safeguarded as required by the CII[A] [Critical Infrastructure Information Act of 2002[92]] and 6 C.F.R. § 29"[93] and that the material "shall not be made available pursuant to any State or local law requiring disclosure of records or information." On appeal, the court protected the information.

Survey Results—Critical Infrastructure Policies

One of the questions posed was whether a request for building layout plans, computer programs, computer coding information, bridge inspections, or other structural information was treated differently than other requests for public records. Agencies were asked whether they had adopted a specific critical infrastructure policy.

The transportation agencies in Alabama, Connecticut, Kentucky, Hawaii, Maryland, Michigan, Nevada, and Oklahoma review records requests in light of and in conjunction with their public records acts. New York law[94] exempts records that, if disclosed, would endanger the life or safety of any persons or jeopardize an agency's capability to guarantee the security of its information technology assets.

North Carolina, Maryland, and Utah responded that their laws specifically stated that the definition of public record "shall not" include public security plans, detailed plans and drawings of buildings, risk assessments, and emergency procedures. North Carolina law[95] protects emergency response plans and sensitive security information. Hawaii's response indicated that, while they do not have a specific critical infrastructure policy, requests are scrutinized and screened for security purposes. Alabama responded that they consider public records requests in conjunction with the Anti-Terrorism and Homeland Security Acts.

Arkansas, Virginia, and Minnesota indicated that their security or critical infrastructure policy could not be released due to its content. Two states, Mississippi and Oklahoma, responded that requests for sensitive information were not treated any differently than other requests.

Missouri, as have some other states, has developed its own version of the Federal Critical Infrastructure Information Policy. The text of the policy acknowledges that the Missouri Open Records law[96]requires governmental agencies to conduct business in a manner open and accessible to all citizens. The policy provides guidelines for the protection of "sensitive" information, which is defined as "information that if released would threaten public safety." Examples include building structural or security plans, transportation security plans, cyber security plans, computer and network documentation, bridge plans, or any other document or specific program related to security systems and structural plans of the transportation system. Sensitive information is to be stored in a secure place with limited access. Certain staff members must determine whether an item is sensitive and therefore exempt from disclosure.

A process similar to the sunshine law request process was set up to process requests for sensitive information. If a request for information is denied, a letter is sent to the requestor explaining that disclosure of the information would impair MoDOT's ability to protect the security or safety of travelers or the transportation system infrastructure. If MoDOT receives sensitive security information from other agencies, that information is protected in the same manner as MoDOT's own information.

b. Federal Hazard Elimination Program.—Accident and safety data collected by public agencies may be pro-

[89] *See* Tech Law Journal Daily E-Mail Alert 4470, July 16, 2002, available at http://www.techlawjournal.com/alert/2002/07/16.asp; 6 U.S.C. § 133 (a)(B) and (C).

[90] 6 U.S.C. § 133(g)(2).

[91] 2006 WL 3511459 (N.J. Super. A.D. 2006) (unpublished opinion).

[92] 6 U.S.C. § 131 *et seq*.

[93] Public disclosure laws, 6 C.F.R. § 29.8(g) and (j).

[94] 21 N.Y. COMP. CODES R. & REGS. § 1500.8.

[95] N.C. GEN. STAT. 132-1.6

[96] MO. REV. STAT. ch. 610.

tected by 23 U.S.C. § 409 and 23 U.S.C § 152. [97] The Federal Hazard Elimination Program, § 152, was codified in the 1970s. The program provided state and local governments with funding to improve "dangerous" sections of roads. To be eligible to receive federal funding, states were required to evaluate their roads to identify hazardous locations and assign priorities for the correction of those locations. After this program was introduced, state and local governments articulated their concerns about liability risks for accidents that took place at the identified locations where improvements had not yet occurred. In response to this concern, Congress adopted 23 U.S.C. § 409, which is set out below:

> Notwithstanding any other provision of law, reports, surveys, schedules, lists, or data compiled or collected for the purpose of identifying, evaluating, or planning the safety enhancement of potential accident sites, hazardous roadway conditions, or railway-highway crossings, of this title or for the purpose of developing any highway safety construction improvement project which may be implemented utilizing Federal-aid highway funds shall not be subject to discovery or admitted into evidence in a Federal or State court proceeding or considered for other purposes in any action for damages arising from any occurrence at a location mentioned or addressed in such reports, surveys, schedules, lists, or data.

Similarly, 23 U.S.C. § 402 provisions for discovery purposes exclude crash records maintained in a state data system if the system is established using federal funds. Language in the Safe, Accountable, Flexible, Efficient, Transportation Equity Act: A Legacy for Users (SAFETEA-LU) makes it clear that the § 409 exclusion extends to safety records that are required by federal law to be maintained.[98]

There was a great deal of controversy about the utility of 23 U.S.C. § 409 until 2003, when the U.S. Supreme Court decided *Pierce County, Washington v. Guillen*.[99] The Court considered a discovery request by the Guillens, who were plaintiffs in a wrongful death lawsuit. The Guillens requested that the county provide them with copies of documents that showed the accident history of the intersection where the fatal accident occurred. That request was denied by the county because accident reports "compiled or collected" for 23 U.S.C. § 152 purposes were protected by federal law. An appeal followed and the case was eventually heard by the U.S. Supreme Court. The Court found that as long as accident reports were obtained for § 152 purposes, they were protected from discovery. The Court emphasized that any information collected for the purpose of identifying, evaluating, or planning a safety enhancement *shall not* be subject to discovery or entered into evidence.

More recently, in *Long v. State ex rel. Dept. of Transp. and Development,*[100] letters between the mayor and Louisiana Department of Transportation and Development (DOTD) about a plan to signalize a railroad crossing using funds available through a federal safety program, and concerning the mayor's commitment to maintain both pavement striping and signs, were found to be protected from discovery and inadmissible pursuant to 23 U.S.C. § 409. The court found that the letters were information that was necessary for the commencement of the upgrade for this roadway/railroad crossing, and therefore, the letters were prepared for the purpose of the federal safety program.

The courts will not protect the information if it is not going to be used in litigation. In *Telegram Publishing Co. v. Kansas Department of Transportation,*[101] a newspaper reporter made a request for the department's railroad safety data and hazard rating system. That request was denied based upon § 409. Summary judgment was granted in favor of Telegram Publishing, and it was awarded attorneys' fees. The appellate court found *Pierce County* irrelevant because Telegram was not seeking information for litigation purposes. The court went on to say that § 409 "contains no prohibitions against disclosure upon a request by a newspaper reporter, as in the case at hand." The court in *Newsday, Inc. v. State of New York Dept. of Transp.*[102] had a similar holding.

Another related issue is whether previous disclosure of the information sought in litigation prevents the agency from claiming the exemption or privilege when the information is later requested in litigation. In *Robertson v. Union Pacific R. Co.,*[103] the parent of a young man who was injured in an automobile-train collision brought a negligence action against the railroad, alleging that the intersection was dangerous and the railroad had prior notice of that fact. Appellants attempted to introduce a newspaper article at trial to show notice to the railroad of the danger of the crossing. The article was written using data compiled by the Arkansas Highway Department. The railroad argued that the district court properly excluded the newspaper article from evidence, because "[t]o allow the introduction of the data through the newspaper article would circumvent the purpose of the statute." Appellants were not allowed to introduce evidence of otherwise inadmissible data simply because it was reported by an indirect, secondary source. The court of appeals held that the newspaper article that identified the crossing at which this collision occurred as the most hazardous railroad crossing in the state was not admissible; the instruction to the parent's expert witness to disregard any information compiled or utilized by the highway department in

[97] *See also* ORRIN F. FINCH & GARY A. GEREN, FREEDOM OF INFORMATION ACT, FEDERAL DATA COLLECTIONS AND DISCLOSURE STATUTES APPLICABLE TO HIGHWAY PROJECTS AND THE DISCOVERY PROCESS (NCHRP Legal Research Digest 33, 1995); *Validity, Construction, and Operation of Evidentiary Privilege of 23 U.S.C.A. § 409*, 181 A.L.R. FED. 147 (2002).

[98] *See* § 1401(g)(4) of SAFETEA-LU at 119 Stat. 1225.

[99] 537 U.S. 129, 123 S. Ct. 720, 154 L. Ed. 2d 610 (2003).

[100] 916 So. 2d 87 (La. 2005).

[101] 275 Kan. 779, 69 P.3d 578 (Kan. 2003).

[102] 1 Misc. 3d 321, 765 N.Y.S.2d 758 (N.Y. Sup. 2003).

[103] 954 F.2d 1433 (8th Cir. 1992).

formulating his opinion was not an abuse of discretion; and evidence that flashing lights at the crossing had failed on two separate occasions following the collision was irrelevant.

The court in *Coastal Delivery Corporation v. United States Customs Service*[104] dealt with the waiver issue in the FOIA context. In this case, plaintiff trucking company requested that the Customs Service release information regarding the number of examinations performed on merchandise arriving into the Los Angeles/Long Beach seaport. The Customs Service argued that the information was protected under FOIA exemptions because terrorists and others could use the information to discover the rate of inspection and then direct their containers containing contraband to vulnerable ports. Plaintiff argued that defendant had disclosed these types of numbers before, and therefore defendant should be required to disclose the requested information to plaintiff at this time. The court found that because Customs did not disclose the exact information requested, only similar information, that "for Customs to have waived its right to argue exemptions, it must have disclosed the exact information at issue," citing with approval *Mobil Oil Corp. v. United States Environmental Protection Agency*[105] and protecting the information.

Practical Considerations

Discovery.—While it is typically acknowledged by plaintiffs' attorneys that accident reports and accident study information may be protected by federal law, it is often necessary to prove this to the court. Plaintiffs may argue that any exemption or privilege should be construed narrowly and that the burden of proof is on the proponent of the exemption or privilege to prove that the information should be protected.[106] The court must have sufficient information to enable it to determine that the information should be protected from discovery. It is helpful for the agency that wishes to protect the information to have an employee execute an affidavit that sets forth that the data were collected for purposes consistent with the Hazard Elimination Act.[107] Typically a privilege log, which sets out document names and a brief description of the document, is provided to the court and to opposing counsel. An *en camera* review of the documents can be requested by either party.

Open Records Responses.—It is important to note that objective records that contain verifiable facts are much more useful to the agency than records that contain opinions, feelings, and other subjective information. For instance, an "incident response" employee who did not witness an accident should not speculate in his report how an accident occurred. He should merely record the facts about the incident that he is able to observe.

It could be (and has been) argued that open records requests made by counsel prior to the filing of a lawsuit can be denied if litigation is pending. The definition of "pending" must be decided on a case-by-case basis and based upon a careful rule of applicable state open records law. Stamping information that is released with a "subject to 23 U.S.C. 409" message may alleviate the problem of that information being used in discovery or being admitted into evidence if counsel determines that the information must be released pursuant to a public records request.

c. The Americans With Disabilities Act of 1990.—The Americans with Disabilities Act of 1990 as amended (ADA)[108] and the Family and Medical Leave Act of 1993 (FMLA)[109] restrict the use of, and access to, employee medical files and require that the files be retained for specific periods of time. Both the ADA and the FMLA allow information to be released as needed to supervisors and managers regarding work restrictions or needed accommodations. [110]

d. Health Insurance Portability and Accountability Act.—The Health Insurance Portability and Accountability Act (HIPAA)[111] states that individually identifiable health information should not be disclosed without the permission of the patient. This law is important to transportation agencies in the context of employee litigation and advice to staff generally. If the legal department or human resources department receives a request for a former or current employee's medical information, a release with the employee's signature should be obtained prior to the disclosure of the information. In addition, HIPAA requires "covered entities," such as health care providers and group health plans (including the employers that provide the plan), to ensure the privacy of certain "protected health information," which may include some medical records related to group health plans.

e. Drivers Privacy Protection Act.—The Drivers Privacy Protection Act [112] regulates the disclosure of personal information contained in the records of state motor vehicle departments. State motor vehicle departments require drivers and automobile owners to provide personal information, which may include a person's name, address, telephone number, vehicle description, Social Security number, medical information, and photograph, as a condition of obtaining a driver's license or registering a vehicle. Prior to the enactment of this law, many states sold that information to individu-

[104] 272 F. Supp. 2d 958 (C.D. Cal. 2003).

[105] 879 F.2d 698, 701 (9th Cir. 1989).

[106] *See* State *ex rel.* Dixon v. Darnold, 939 S.W.2d 66 (Mo. App. 1997).

[107] A sample affidavit is attached to the end of this section as App. H.

[108] 101 P.L. No. 336, 104 Stat. 327, 42 U.S.C. §§ 12101–12213, 29 C.F.R. § 1602.14.

[109] 103 P.L. No. 3, 107 Stat. 6, 29 U.S.C. § 2601.

[110] *See* App. D for a chart detailing the lengths of time certain information should be kept.

[111] 42 U.S.C. § 1320.

[112] 103 P.L. No. 322, 108 Stat. 1796, 18 U.S.C. §§ 2721–2725.

als or businesses, generating significant revenue for the state. The data had the potential to fall into the wrong hands, and in at least one case, the release of data resulted in the murder of a woman.

South Carolina sued to block enforcement of the Act in *Reno v. Condon*.[113] The Supreme Court held that it was appropriate to regulate the personal information found on license applications and that Congress had the authority to enact the Drivers Privacy Protection Act because the Act regulated the states as owners of motor vehicle databases that are used in interstate commerce. The Court found that the regulation, which permitted disclosure of the personal information in limited situations for any "state-authorized public purpose" relating to the operation of a motor vehicle or public safety, was constitutional.

f. The Uniform Relocation Assistance and Real Property Assistance Program.—The Uniform Relocation Assistance and Real Property Assistance Program[114] provides that an agency should maintain adequate records of acquisition and displacement activities in sufficient detail to demonstrate that it complied with the law. The regulation goes on to state, "[r]ecords maintained by an agency in accordance with this part are confidential regarding their use as public information, unless applicable law provides otherwise."

The court in *City of Reno v. Reno Gazette–Journal*[115] dealt with the regulation when addressing a sunshine law request from a newspaper. The city was asked to provide appraisal values for the parcels of property it was acquiring as part of a public works project. The request included the amount of compensation that was offered to the property owners, a breakdown of any costs in the budget, and the names and addresses of property or lease owners with a list of appraisal values and relocation payments. The city denied the request on the basis that the records were confidential under federal and state law. The newspaper prevailed in the lower court and the city appealed to the Nevada Supreme Court. The court found that the records were protected under federal law, reasoning that a specific provision takes precedence over a general provision and since the federal law specifically deemed the records to be closed, the general language of the sunshine law did not control on this issue. Similar reasoning was followed in a Kentucky Attorney General Opinion.[116]

3. Trade Secrets

Trade secrets are discussed in 18 U.S.C. § 1905. The FOIA does not apply to trade secrets and commercial or financial information obtained from a person if it is privileged or confidential. The term "trade secret" (as defined by 18 U.S.C. § 1905) is a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that is the end product of either innovation or substantial effort. The "commercial" aspect of the exemption is not confined to records that reveal basic commercial operations or relate to income-producing aspects of a business, but may apply when the provider of the information has a commercial interest in information submitted to the agency. Information does not need to relate to business entities to constitute financial information; protected information may be personal financial information.[117]

a. Proprietary Information Held by State Departments of Transportation.—State transportation agencies often deal with trade secrets in the context of proprietary information contained in bid documentation and contracts. The USDOT has a process to notify people or businesses who have submitted confidential information when that information is requested. Bid solicitations notify all potential bidders that they should mark confidential information as confidential. If the USDOT receives a FOIA request for records that include confidential information and staff believe the information should be released under FOIA, the office will notify the information submitter in writing that the information has been requested. USDOT will, to the extent permitted by law, consider a submitter's objections and grounds for nondisclosure before determining whether to disclose business information. The submitter may object to the disclosure of the information. If a decision is made to disclose the material, the submitter will be provided notice of that decision so that judicial remedies can be pursued. The submitter in that case must file a "reverse FOIA" action, asking that the information be protected and not released to the public. The government assumes no liability for the disclosure of information that was not appropriately designated.[118]

In *Center for Auto Safety v. National Highway Traffic Safety Admin.*,[119] the National Highway Traffic Safety Administration (NHTSA) issued an Information Request to nine airbag manufacturers and importers seeking information on airbag systems used in 1990–1998. The Center for Auto Safety sought access to the information pursuant to FOIA. NHTSA released some of the information to the Center, but claimed that the remaining submissions were protected from disclosure under Exemption 4 of FOIA, which excludes "trade secrets and commercial or financial information obtained from a person and privileged or confidential" from disclosure. The court found that information submitted by airbag manufacturers to NHTSA about the performance of airbags should be released because information addressing the physical and performance characteristics of airbags, not how the airbags were manufactured, did not qualify as trade secret information for purpose of the FOIA exemption.

[113] 528 U.S. 141, 120 S. Ct. 666, 145 L. Ed. 2d 587 (2000).

[114] 49 C.F.R. § 24.9(b).

[115] 119 Nev. 55, 63 P.3d 1147 (2003).

[116] *See* Ky. Op. Att'y Gen. 05-ORD-128, 2005 WL 3844502.

[117] CJS Records § 138.

[118] *See* 49 C.F.R. § 7.17, Consultation with submitters of commercial and financial information.

[119] 244 F.3d 144, 345 U.S. App. D.C. 248 (D.C. Cir. 2001).

Practical Concerns

Because of the potential liability connected with the unauthorized release of proprietary or confidential information protected by state trade secrets acts, the agency must set up a procedure that requires those submitting sensitive or otherwise potentially protected information to clearly identify the information as a "trade secret." Care must be taken to ensure that appropriate safeguards are in place to keep the information confidential once it has been determined that it should be confidential. The agency's open records policy should reflect that confidential or proprietary information will not be released. Staff must be trained to ensure compliance with the policy as the agency may have liability if the information is accidentally released.

Survey Results—Confidential Information

Agencies were asked how they processed "proprietary" or other information contained in bid documents or other confidential information that the submitter might reasonably believe would be protected from disclosure.

Missouri's law protects information contained in a bid until the bids are opened and read, at which point they become public record. North Carolina's law[120] protects such information if it is a "trade secret" as defined by state law, if the information is the property of a "private person" as defined by state law, and if the information was furnished in connection with a bid, proposal, or the like, and the information is designated when submitted as confidential information.

In Hawaii, confidential information stored in the document management system is kept in a secure folder with limited access. Similarly, in Alabama, proprietary and confidential information is maintained only in paper form and is kept under lock until destroyed under the records retention policy.

Montana responded that its constitution requires that the records in a state agency's possession be provided to the public and that confidential information under almost all circumstances must be provided upon request. They also noted, however, that if they receive a request for information that could be considered confidential, such as bid information, they notify the submitting party so that the submitter could litigate the issue if it chose to do so.

Similarly, Wisconsin responded that it requires that confidential information be designated as "confidential" upon submission, and if it receives a request for the information, it notifies the bidder to allow the bidder to handle the litigation if it so chooses. Vermont uses the following method: Bid proposals are regulated as restricted or confidential records. The only individuals who can access these records are those who have been granted access by the Vermont Agency of Transportation (VTrans) Public Records Officer in writing. This information is provided to the records center, and only individuals included on this list are allowed to request or view these records. Restricted or confidential information is removed from the paper proposals prior to public viewing, and only authorized personnel are allowed to view the data.

b. Public-Private Partnerships.—Many public agencies are forming "public-private partnerships" (PPPs). Typically the PPPs involve a state or municipal highway department or bridge or transit authority that owns and operates highway and transit facilities. The private partners are professional service companies, contractors, and financial entities pursuing business with owner-operators. Until recently, private-sector participation was limited to planning, design, or construction contracts on a fee schedule based on the public agency's specifications.

Expanding the private sector's role allows public agencies to tap private sector technical, management, and financial information. The private partner can expand its business opportunities in return for assuming the new or expanded responsibilities and risks. Public agencies must be able to protect the confidential or proprietary information that is contained within the communications from the private companies.

Confidential information is one of the components addressed by the Federal Highway Administration's PPP model legislation. This document suggests that the agency inform the submitter, prior to the submission, that it may request an opinion from the agency as to whether the information it plans to submit will be subject to the state's open records act and therefore subject to release. The submitter then has an opportunity to object to the release of any information it identifies as confidential or proprietary if it is requested under the state's open records act. If the state determines the information should remain confidential, it will not be released if requested.[121]

Practical Concerns.—Agencies that contract with private firms to provide government services should address public records compliance issues. Contracts with the firms should contain indemnification and hold-harmless clauses to protect the agency in case the contractor's failure to produce such records results in liability under the public records law.

B. TRENDS IN PUBLIC RECORDS LAWS

The reader should be aware that generally the intent of public records laws is to be expansive, and the exceptions are narrowly construed by the courts. The reader should carefully research case law for the specific jurisdiction.

Who Is Subject to Public Records Law?

In *Central Atlantic Progress v. Baker*,[122] the Atlanta Chamber of Commerce refused to allow inspection of the bids for the Nascar Hall of Fame and the 2009 Super Bowl by the *Atlanta Journal–Constitution*. The at-

[120] N.C. GEN. STAT. § 132-1.2.

[121] *See* http://www.fhwa.dot.gov/ppp/pdf/legis_model.pdf, last visited Apr. 4, 2009.

[122] 278 Ga. App. 733, 629 S.E.2d 840 (Ga. App. 2006).

torney general issued an opinion stating that, in light of the significant involvement of public officials, public employees, public resources, and public funds in the matters, the bids were subject to the Georgia Open Records Act[123] and should be disclosed. On appeal, the court agreed with the attorney general's opinion.

Similarly, the court in *News Journal Corp. v. Memorial Hospital-West Valencia*[124] found that contractors' records are public records when the contractor is relieving the government from the operation of a governmental function such as operating a jail or hospital or providing fire protection.

Personal E-mails as Public Records

In *Griffis v. Pinal County*,[125] a former county manager who was being investigated for misuse of public funds filed an action against the county trying to block the release of personal e-mail messages he had sent or received while he was the county manager. The court found that the definition of public records is not unlimited, as the law requires public officials to make and maintain records "reasonably necessary to provide knowledge of all activities they undertake in the furtherance of their duties" and, further, that the definition does not encompass documents of a purely private or personal nature. Because the "nature and purpose" of the document determine its status, the mere possession of a document by a public officer or agency does not by itself make that document a public record under public records law, nor does expenditure of public funds in creating the document.

Personal e-mails sent or received by government employees may be public records, and therefore open to inspection, but to be considered an "official record" the record must have some relation to the official duties of the public officer that holds it. In *State v. Clearwater*,[126] the court rejected the argument that placement of e-mails on the state's computer system automatically makes them public records. Similarly, in *Denver Publishing v. Board of County Commissioners*,[127] the court found that for an e-mail to be a public record, the content of the e-mail must reveal a "demonstrable connection" to the employee's performance of public functions or a connection to the receipt or expenditure of public funds. The court stated that it was important to weigh open access to government records against the protection of individual privacy.

In a slightly different context, in *Tiberino v. Spokane County*,[128] Ms. Tiberino's employment as a secretary for the Spokane County Prosecutor's Office was terminated based on her unsatisfactory work performance, including her use of e-mail for personal matters. Ms. Tiberino threatened the county with a lawsuit for wrongful termination. In response to the threat, the county printed all e-mails Ms. Tiberino had sent or received from her work computer. The county received requests for those records from Cowles Publishing Company and Spokane Television, Inc. The court found that the fact that Ms. Tiberino sent 467 personal e-mails over a 40 working-day time frame was of significance in her termination action and the public had a legitimate interest in having that information. However, the court found that what she said in those e-mails was of no public significance, that the public had no legitimate concern requiring release of the e-mails, and that the e-mails should be exempt from disclosure.

1. Withholding Documents Based Upon Attorney–Client Privilege

Courts generally hold that government agencies are allowed to consult with counsel outside of the hearing of the media or other interested parties. In *Roberts v. City of Palmdale*,[129] the court applied the attorney-client privilege to the California Public Records Act,[130] noting that a city council needs the freedom to confer with its attorneys confidentially to obtain adequate advice. Similarly, in *Tennessean v. Tennessee Department of Personnel*,[131] a newspaper requested harassment investigation files from a state agency. The agency withheld some documents based upon attorney-client privilege. On appeal, the court reasoned that if the purpose of the document was to provide legal advice or prepare for litigation then the privilege applies, however, if the purpose of the document was to enforce the antidiscrimination policy or comply with the state's legal duty to investigate, the documents were not privileged.

In the case of *Springfield Terminal Ry. Co. v. Department of Transp.*,[132] documents authored by the department of transportation's chief counsel and outside counsel that contained advice about the mechanics of and possible outcomes of future eminent domain litigation were not public records and therefore not subject to disclosure under Maine's Freedom of Access Act, because the documents were privileged under the work-product doctrine.

2. Trade Secrets and Proprietary Information

In *Cubic Transp. Systems, Inc. v. Miami-Dade County,*[133] Cubic brought a suit against the county for the protection of its "trade secrets" after submitting bid information for the county's consideration. The court found that Cubic failed to protect its trade secrets from the effect of the Public Records Act when it did not mark the documents as "confidential," and continued to supply the county with documents without asserting a

[123] GA. CODE ANN. § 50-18-70 *et seq*. (2006).

[124] 695 So. 2d 418 (Fla. App. 5 Dist. 1997).

[125] 215 Ariz. 1, 156 P.3d 418 (2007).

[126] 863 So .2d 149,151 (Fla. 2003).

[127] 121 P.3d 190, 199 (Colo. 2005).

[128] 103 Wash. App. 680, 13 P.3d 1104, 1108 (Wash. App. 2000).

[129] 20 Cal. Rptr. 2d 330, 853 P.2d 496 (1993).

[130] CAL. GOV'T CODE § 6250 *et seq*. (1993).

[131] 2007 WL 1241337 (Tenn. App. 2007).

[132] 2000 Me. 126, 754 A.2d 353 (2000).

[133] 899 So. 2d 453 (Fla. 2005).

post-delivery claim of confidentiality. The court cited *Sepro Corp. v. Florida Department of Environmental Protection*[134] for the proposition that

> [T]he trade secret owner who fails to label a trade secret as such, or otherwise to specify in writing upon delivery to a state agency that information which it contends is confidential and exempt under the public records law is not to be disclosed, has not taken measures or made efforts that are reasonable under the circumstances to maintain the information's secrecy.

The order compelling production of the documents was affirmed.

In *California First Amendment Coalition v. County of Santa Clara and Peter Kutras*,[135] a case decided in superior court, the county argued that the GIS base map was proprietary information and should not be released in response to a public information request. GIS technology provides a 3-D display, on maps, of information in an easy-to-use database. The court rejected the county's arguments that it could withhold the GIS base-map files because of their status as computer software and because the files allegedly contain "trade secrets" protected from disclosure under state and federal law. The superior court concluded the base map consisted of data, not software, and found that the county, by selling the base map to private entities, had waived any trade secret protection to which the records otherwise might be entitled. The court found that federal copyright protection did not permit the county to deny a valid request under California's Public Records Act. The court also rejected the county's attempt to avoid releasing the records by getting them designated "Critical Infrastructure Information" by DHS. The court noted that this designation was sought only after the plaintiff filed suit, and despite the county's past sales of the GIS base map to 15 purchasers, 5 of them private companies.

In the case of *Douglas Asphalt v. E.R. Snell Contractor*,[136] the Georgia Department of Transportation held the bid records of 11 asphalt contractors, and received a request from Douglas Asphalt to review those records. The contractors joined together and claimed the state's records contained trade secrets. The court agreed and noted that the asphalt industry is highly competitive and that because materials make up the largest part of the costs, companies spend a lot of time and money perfecting the formulas to reduce their costs. The court was concerned that competitors could derive the mix designs from reviewing the requested information.

In *Springfield Terminal Ry. Co. v. Agency of Transp.*,[137] VTrans issued a request for proposals, seeking a rail freight operator to provide freight service. The proposal request required that each bidding operator submit detailed information regarding corporate finances, in addition to a general technical proposal. In response to the VTrans request, three freight operators submitted proposals containing the required financial information. The financial information included balance sheets, income statements, profit and loss statements, statements of retained earnings, statements of cash flows, and freight and passenger flow projections. Springfield Terminal Railway (STR) also submitted a proposal, but omitted the required financial information. Later, STR submitted a request to inspect or copy public records relating to the selection, solicitation, and recruitment of entities to operate the rail line. VTrans produced some of the requested documents, but withheld the financial documents, claiming them as exempt under Vermont's Public Records Act.[138] VTrans also withheld information, including the names of current and potential shippers, stockholder information, and employee information. The court found that the data contained in the bidders' proposals could be used to give STR a detailed account of confidential, sensitive data and vitiate the competitive advantage held by the bidders and ruled that VTrans did not have to release the documents.

3. Information Protected From Disclosure Due to Security Concerns

In *Northwest Gas Ass'n v. Washington Utilities and Transp. Comm'n,*[139] several pipeline companies brought an action against the Washington Utilities and Transportation Commission, trying to enjoin the disclosure of a detailed map and pipeline data in response to newspapers' public records act request. Several newspapers intervened. The pipeline companies asked the trial court to enjoin the commission from disclosing the data under Revised Code of Washington 42.56.540, which protects public records from disclosure when "examination would clearly not be in the public interest and would substantially and irreparably damage vital government functions." The companies submitted more than 20 declarations from Northwest Gas Association members and other industry representatives. These declarations asserted that 1) the companies' natural gas pipeline system "constitutes part of the critical energy infrastructure" of the state and of the northwest region of the United States, and 2) "[t]he incapacity or destruction of the regional gas pipeline system would have potentially catastrophic consequences for economic security and public safety." The newspapers could not refute these assertions. Because the pipelines raised serious issues of proprietary interests, public safety, and national security, the court decided that the information should not be released.

4. Personnel Records

In *Herald Co. v. City of Bay City*,[140] the court held that Bay City violated the state FOIA when it did not

[134] 839 So. 2d 781, 784 (Fla. 1st Dist. 2003).

[135] Case No. 1-06-CV-072630 (May 2006).

[136] 282 Ga. App. 546, 639 S.E.2d 372 (2006).

[137] 174 Vt. 341, 816 A.2d 448 (2002).

[138] VT. STAT. ANN. tit. 1, § 317(c)(9) (2002).

[139] 141 Wash. App. 98, 168 P.3d 443 (2007).

[140] 463 Mich. 111, 614 N.W.2d 873 (2000).

disclose its records concerning the final candidates for fire chief. The city argued that "private details" of the applicants' lives would be revealed if they released the records, but the Michigan Supreme Court found that the records were protected only if they revealed intimate or embarrassing details about an individual's private life.

In the case of *In Re Wick Communications Co. v. Montrose County Board of County Commissioners,*[141] while a termination hearing was pending, the *Montrose Daily Press* requested photocopies of "any and all pages from the diary…discussed and used during a public grievance" for a former Montrose employee. Faced with the decision of disclosing the entire contents of his personal diary or risking citations for contempt and prosecution, the city manager petitioned the court for relief. The court found that in cases where it is unclear whether the custodian of the record holds the record in an individual or official capacity, and thus whether the record is private or public, the requesting party must make a threshold showing that the document is likely a public record. The court found that Colorado's law did not apply to a private diary and the diary did not have to be produced.

5. When Agency Fails to Follow Its Own Policy

The court in *Gumina v. City of Sterling*[142] evaluated a claim by a terminated city employee who sought the minutes from two city council executive sessions in which her employment was discussed. The court held that the city council's failure to comply strictly with requirements for executive sessions rendered meetings open such that recorded minutes were open to the public.

An open records request for the investigation of the rape and murder of a 14-year-old child was denied due to the "pending investigation" exemption to the public records law. However, the county failed to respond to the request in 3 days, which was required by state law. Because of the county's failure to respond to the request in a timely manner, the court reversed an earlier ruling in favor of the county and ruled that the Public Records Act had been violated.[143]

6. Payment of Redaction Fees

The court in *Data Tree v. Meek* [144] considered Data Tree's request to obtain bulk records of 20 separate microfilm rolls to collect real estate information. The county said the redaction fees would be $22,000 because social security numbers, birthdates, and other confidential information would have to be redacted. The court decided that the costs of producing records and redaction should be borne by the requester.

7. Requested Information Release Format

49 C.F.R. § 7.14(5) states as follows: The request should state the format (e.g., paper, microfiche, computer diskette, etc.) in which the information is sought, if the requestor has a preference. Several states have similar legislation. Mississippi's Section 225-61-10 (2) states that "[a] public body shall provide a copy of a record in the format requested if the public body maintains the record in that format…."

In *Wiredata v. Village of Sussex*,[145] a request was made to the city for property assessment data in a specific format that would have required the contractor to provide access to the database. The format had been created and maintained by a contractor in the contractor's own database. The city's response was provided in PDF format. The requestor filed an appeal, claiming that the contractor should have allowed direct access to the computer database. The court disagreed, commenting that the risks of confidential information being compromised and damage to the database outweighed the requestor's right to the information in a particular format.

In *State ex rel. Milwaukee Police Ass'n v. Jones*, the police chief's production of an analog recording of a digitally-recorded 911 call was an insufficient response under the Wisconsin Public Records Act when the requester sought access to the actual recording for the purpose of examining the record and making a digital copy. Wisconsin's statute, Section 19.36(4), allows a requester the right to inspect and make a copy of a record and further provides that "the material used as input for a computer program or *the material produced as a product of the computer program is subject to the right of examination and copying.*" The court reasoned that the statute allows for exactly what the police association had requested—access to the source "material" and the opportunity for "examination and copying." Finding in the requestor's favor, the court stated that a "potent open records law must remain open to technological advances." [146]

8. Using Public Records Acts as a Discovery Tool

California law[147] exempts "[r]ecords pertaining to pending litigation to which the public agency is a party…until the pending litigation or claim has been finally adjudicated or otherwise settled." The California Public Records Act's[148] pending-litigation exemption protects attorney-client privileged information and attorney work product, as well as any other work product related to pending litigation. [149] In C*ounty of Los Ange-*

[141] 81 P.3d 360 (Colo. 2003).

[142] 119 P.3d 527 (Colo. App. 2005).

[143] Athens Newspapers v. Unified Gov't of Athens, 284 Ga. 192, 663 S.E.2d 248 (2008).

[144] 279 Kan. 445, 109 P.3d 1226 (Kan. 2005).

[145] 310 Wis. 2d 397, 751 N.W.2d 736 (2008).

[146] State *ex rel.* Milwaukee Police Ass'n v. Jones, 237 Wis. 2d 840, 615 N.W.2d 190 (2007).

[147] CAL. GOV'T CODE § 6254.

[148] CAL. GOV'T CODE §§ 6250 *et seq*.

[149] *See* Bd. of Trustees of Cal. State Univ. v. Superior Court, 132 Cal. App. 4th 889, 34 Cal. Rptr. 3d 82 (2005).

les v. Superior Court,[150] the court held that the California Public Records Act's pending-litigation exemption confers a broad exemption from disclosure on public agencies by protecting its work product generated in anticipation of litigation. The court emphasized that a document is protected from disclosure under the Public Records Act's pending-litigation exemption only if the document was specifically prepared for use in litigation.

The following cases, found in various jurisdictions, provide insight on this issue.

In W*esco, Inc. v. Sorrell*,[151] gas station owners were defendants in criminal and civil cases where violations of environmental laws were alleged at their different facilities. The defendants tried to obtain the state's documents under the state's Access to Public Records Act[152] after they had been denied discovery of those documents in the pending criminal and civil cases. The state Supreme Court held that documents were relevant to the government's pending cases against the gas station owners, and thus exempt from disclosure under the state's Access to Public Records Act.

In *Hangartner v. City of Seattle*,[153] requests were filed for documents related to a monorail project under the state Public Disclosure Act.[154] The requests were denied based on the "records relevant to a controversy" exception to the public records law. The court found that the phrase "relevant to a controversy" means "completed, existing, or reasonably anticipated litigation," and that the city failed to establish that there was any threat or reasonable anticipation of litigation concerning the enactment of legislation relating to the monorail, but only a "litigation-charged atmosphere."

In *Soter v. Cowles Pub. Co*.,[155] the court found that materials that would not be discoverable under the civil rules of pretrial discovery were also exempt from disclosure under the Public Records Act.[156] The protection of the documents was triggered prior to the initiation of litigation and extended beyond the official termination of litigation. Courts do not distinguish between completed and pending cases in applying the exemption under the Public Record Acts for records that would not be discoverable under the civil rules of pretrial discovery. This is because the possibility of disclosure, even disclosure after termination of the lawsuit, could cause witnesses to hesitate to reveal details to the attorneys, and it might cause attorneys to hesitate to reduce their thoughts or understanding of the facts to writing.

The court in *American Civil Liberties Union of Delaware v. Danber*[157] dealt with the "potential litigation" exemption to the public records law. The American Civil Liberties Union (ACLU) made a FOIA request to the Department of Corrections (DOC) for information regarding the delivery of health care services within Delaware's prison facilities. The DOC invoked FOIA's potential-litigation exemption based on "correspondence from the ACLU, some addressed to inmates in the custody of the DOC, that suggest that the ACLU may be contemplating litigation against the DOC based on alleged inadequate medical care at DOC facilities." The court noted that "[i]n our litigious society, a governmental agency always faces some threat of suit. To construe the term 'potential litigation' to include an unrealized or idle threat of litigation would seriously undermine the purpose of [FOIA]." The court adopted the Delaware Attorney General's two-pronged test to determine if the "potential litigation" exception would justify a refusal to supply information in response to a FOIA request: 1) litigation must be likely or reasonably foreseeable; and 2) there must be a "clear nexus" between the requested documents and the subject matter of the litigation. The court commented that the test "strikes a balance between the need to construe the exceptions to FOIA narrowly and the need to give effect to the actual words of the statute which provide for the exception" and allowed the information to be withheld.

In *Kentucky Lottery Corporation v. Stewart*,[158] a state agency denied an open records request because the documents requested were related to a matter in litigation. The court stated that the "litigation exemption" did not terminate a person's right to use an open records request in litigation and further commented that an open records request should not be evaluated based on who is requesting the documents.

The state Office of Risk Management was ordered to allow public access to documents involving dental malpractice claims that it had settled in *Times Picayune Publishing Corp. v. Board of Supervisors of Louisiana State University*.[159] The documents requested were copies of settlement checks and related settlement material. The records request was denied because the risk management office was involved with other similar claims and stated that their claims file was still open. The court found that since the earlier claims were settled, they were not pending and therefore were subject to disclosure, even though the claims had been consolidated for discovery purposes.

Different state court decisions result in similar outcomes when a litigant asserts a public records act as a discovery tool. Variances among decisions depend upon the facts and nature of each case.

9. Exemption of Records Regarding the Future Purchase of Real Estate

State FOIAs generally require public agencies to keep the content of real estate appraisals, engineering or feasibility estimates, and evaluations relative to property acquisitions confidential until the property is

[150] 82 Cal. App. 4th 819, 98 Cal. Rptr. 2d 564 (2000).

[151] 177 Vt. 287, 865 A.2d 350 (2004).

[152] 1 VT. STAT. ANN. § 315.

[153] 151 Wash. 2d 439, 90 P.3d 26 (2004).

[154] *See* WASH. REV. CODE § 42.17.310(1)(j).

[155] 162 Wash. 2d 716, 174 P.3d 60 (Wash. 2007).

[156] WASH. REV. CODE § 42.56 *et seq*.

[157] 2007 WL 901592 (Del. Super. 2007).

[158] 41 S.W.3d 860 (Ky. App. 2001).

[159] 845 So. 2d 599 (La. Ct. App. 2003).

acquired or related transactions are terminated or abandoned.

In *Heidemheimer v. Texas Department of Transportation*,[160] after the state planned and announced a highway project, the applicant requested that the department produce parcel numbers and names and addresses of parcel owners for property it planned to acquire. The department refused to provide them, relying on Texas Government Code Section 552.105(2), which provides that "[i]nformation is excepted from the requirements of Section 552.021 if it is information relating to…appraisals or purchase price of real or personal property for a public purpose prior to the formal award of contracts for the property." The court found that the records did not have to be released because their release could affect negotiations by inflating sale prices. However, in *Coleman v. Boston Redevelopment Authority*,[161] the plaintiff property owner requested appraisals for real estate that the agency intended to acquire. The agency produced some documents in response to the request, but not the appraisals. The court ruled that the appraisals were protected until a final agreement was reached, any litigation relative to the appraisal was terminated, or the time to begin an action expired. The court ordered the appraisal to be released because the tract in question had already been settled.

10. Attorney's Fees

A prevailing party in public records disclosure litigation may be awarded attorneys fees.

In *Specht v. Finnegan*,[162] an appellate court affirmed the trial court's order of attorney's fees and costs due to the agency's repeated violations of Ohio's public record and open meetings laws. The township failed to deliver records in a timely manner, overcharged for records, and locked the doors to the township hall during "public" meetings. The court allowed a $500 fine for each violation and $16,000 in attorney's fees.

In *Burlington Free Press v. University of Vermont*,[163] the newspaper made a request for documents held by the university after its investigation of allegations of hazing by a fraternity. Some of the documents requested under the public records act were released, and some were withheld. The trial court refused to award attorney's fees even after the documents were ordered to be released. The Vermont Supreme Court held that attorney's fees were not appropriate, and the newspaper's legal fees were simply a cost of doing business.

In *Olibas v. Honorable Sheriff Gomez*,[164] Olibas, a bail bondsman, requested data from the office of Sheriff Gomez, who responded by providing the information he requested, but refused to compile information in response to the request or to create records in response to the request. Olibas filed a legal action against Sheriff Gomez. The court found that Olibas' petition was groundless and in bad faith and awarded the sheriff $4,800 in attorney's fees.

Practical Concerns

Thirty of the 31 states that responded to the survey had a public records request review process in place, even if the process was as simple as sending the requests through the legal office. Many states have a list of documents that can be released without an official public records request.

V. CONCLUSION

State public disclosure laws require maintenance of appropriate records. The nature of the record and the extent of the record keeping will vary depending on the purpose and technical operation of the federal or state agency. The process of record keeping involves an understanding of the legal requirements and the context in which the records are kept. Considerations such as which staff division is responsible for the records, maintenance, content of the records, privacy, and security are all important factors. Special consideration must be given to evolving obligations and restrictions associated with electronic records.

This report has touched upon many of the legal variables associated with record keeping, with the purpose of affording a basis for further examination for practical application.

[160] 2003 WL 124248 (Tex. 2003).

[161] 61 Mass. App. Ct. 239, 809 N.E.2d 538 (Mass. App. Ct. 2004).

[162] 149 Ohio App. 3d 201, 776 N.E.2d 564 (2002).

[163] 172 Vt. 303, 779 A.2d 60 (Vt. 2001).

[164] 242 S.W.3d 527 (Tex. App. 2007).

APPENDIX A: RECORDS RETENTION SURVEY

The purpose of this questionnaire is to gather information regarding public record policies in your state for the preparation of an article for the Transportation Research Board.

1. Does your agency have a records retention policy that pertains to the entire agency? Do any of your departments or divisions (right of way, construction, maintenance, environmental, legal) have their own policy? Please provide a copy.

2. Are you required by any statute, regulation or internal policy to retain particular records? If so could you identify and attach the statute, policy or regulation?

3. Has your agency's records retention policy been challenged in court? If so what type of challenge was made, i.e., was the allegation that the policy was not comprehensive enough or that it was not followed? What were the results of the challenge?

4. Are you aware of any pending legal challenges of your records retention policy? Are you aware of any legal challenges for your failure to have such a policy or comply with the existing policies?

5. What methods are you using to retain documents? For example, storage of paper documents, microfilm, or scanning and saving to a central computer database. Have you experienced any problems retrieving and authenticating these documents once they are stored? Are you required by law to maintain old systems so that your older documents can be easily retrieved? If you are not required by law do you maintain old systems for ease of retrieval in new systems?

6. How do you handle "proprietary" or other information contained in bid proposals or other confidential information that the submitter may reasonably believe would be protected from disclosure?

7. If you receive a request for building layout plans, computer programs, computer coding information, bridge inspections or other structural information, is this request treated differently than other requests for public records? Have you adopted a specific critical infrastructure policy? If so would you please attach a copy to your response?

8. Does your agency have a policy advising staff how to handle public records requests? If so would you please attach a copy of the policy to your response?

APPENDIX B: RESPONSES TO RECORDS RETENTION SURVEY

1) Does your agency have a records retention policy that pertains to the entire agency? Do any of your departments or divisions (right of way, construction, maintenance, environmental, legal) have their own policy? Please provide a copy.			
State	**Yes**	**No**	**Response**
Alabama	Yes		Overall policy for agency approved by director and state records commission. Divisions also have their own records schedule.
Alaska	Yes		State has a records retention policy; Divisions have individual schedules.
Arizona	Yes		Arizona Department of Transportation has a retention policy that includes schedules for individual divisions.
Arkansas	Yes		Agency has a policy, divisions do not have their own individual policies.
Connecticut	Yes		DOT has several retention schedules depending on unit.
Georgia	Yes		http://sos.georgia.gov/archives/who_are_we/rims/default htm
Hawaii	Yes		State general retention schedule; some departments have forms for records that are unique to their departments.
Kansas	Yes		http://www.kshs.org/government/records/stategovt/browseretentionschedules.php
Kentucky	Yes		http://www.kdla.ky.gov/recmanagement/schedules/Transportation.pdf
Maryland	Yes		DOT has a policy, and individual offices have individual policies.
Michigan	Yes		Both agency and individual divisions have policies.
Minnesota	Yes		The agency's schedule includes both general retention items that all offices and districts share and items specific to the business functions.
Mississippi	Yes		In the process of revising
Missouri	Yes		State has rules regarding records management: 15 CSR 30-45.010, RSMo. 109.200-109.310, Missouri General Retention and Disposition Schedule.
Montana	Yes		
Nebraska			Copies of current Department of Roads schedules can be found at http://www.sos.state.ne.us/records.
Nevada	Yes		
New Hampshire	Yes		Each bureau has its own retention guidelines.
New Jersey	Yes		NJDOT has a Records Retention Schedule for the entire Department.
New York	Yes		NYSDOT has its own policy.
North Carolina	Yes		
Ohio	Yes		See link http://apps.ohio.gov/rims/General/General.asp. ODOT uses the general schedules, as well as schedules specific to ODOT. See the following link for those schedules: http://apps.das.ohio.gov/rims/Search/SearchResult.asp?Order=s.ScheduleD&hPubsearchNav=PublicResponse&btnSearch=Search&optActGen=Active&txtSerAuthNo
Oklahoma	Yes		
Oregon	Yes		
Tennessee	Yes		Department has records retention schedule.

Texas	Yes		
Utah	Yes		Utah follows State Records Committee General Retention Schedule.
Vermont	Yes		
Virginia	Yes		Department Policy Memo re records retention, separate policy for e-mail retention.
Washington	Yes		General records retention schedule, currently updating agency unique schedules.
Wisconsin	Yes		DOT and individual departments have policies.

2) Are you required by any statute, regulation or internal policy to retain particular records? If so could you identify and attach the statute, policy or regulation?			
State	**Yes**	**No**	**Response**
Alabama			Ala. 41-13-21, DOT has established comprehensive internal policy.
Alaska			http://www.archives.state.ak.us/records_management
Arizona			Ariz. Rev. Stat. 41.1347 establishes records retention requirements.
Arkansas			Ark. Code Ann. 25-18-601-605, Ark. Code Ann. 19-4-1108.
Connecticut			General statute 11-8 controls policies.
Hawaii			Hawaii Revised Statutes, 94-3.
Kansas			Kan. Stat. Ann. 45-401.
Kentucky			See Ky. Rev. Stat. Ann. 171.410 through Ky. Rev. Stat. Ann. 171.740. These statutes may be accessed online at the following address: http://www.lrc.ky.gov/KRS/171-00/CHAPTER.HTM
Maryland			State Gov't Article 10-631 to 10-634, Md. Code Regs. 14-18.02.
Michigan			Public Act 504 of 1988, Section 18.1285 *et seq*.
Minnesota			Minnesota Statutes, Chapter 13, Data Practices Act, Chapter 138, Preservation and Disposal of Public Records.
Mississippi			
Missouri			Mo. Rev. Stat. 109.200–109.310, 15 CSR 30–45.010.
Montana	Yes		
Nebraska			Nebraska Records Management Act, 84-1201.
Nevada			No response
New Hampshire			Chapter 5, Archives and Records Management.
New Jersey			Some records are required to be kept according to state law; those items are reflected in the NJDOT retention schedule.
New York			Art and Cultural Affairs Law, Section 57.05 Department of Education has jurisdiction over all NY State records.
North Carolina			General Statute 132.
Ohio			
Oklahoma			
Oregon			Or. Rev. Stat. 192 and Or. Admin. R. 166.
Tennessee	Yes		
Texas			Chapter 441.183, Tex. Admin. Code Title 13, Chapter 6.
Utah	Yes		
Vermont			Attached.
Virginia			46.2-878 requires written copies of traffic engineering investigations for speed limits to be effective; 46.2-11.4 requires records to be kept of all highways in which speed has been reduced—several schedules approved by Library of Virginia.

Washington			Wash. Rev. Code 40.14 general retention schedule covers all state agencies.
Wisconsin			Wisc. State 16.61, Admin. Code 12.

3) Has your agency's records retention policy been challenged in court? If so what type of challenge was made, i.e., was the allegation that the policy was not comprehensive enough or that it was not followed? What were the results of the challenge?

State	Yes	No	Response
Alabama		No	
Alaska		No	
Arizona		No	
Arkansas		No	
Connecticut		No	
Hawaii		No	
Kansas		No	
Kentucky		No	
Maryland		No	
Michigan		No	
Minnesota		No	
Mississippi		No	
Missouri	Yes		Matt Blunt [Governors Office] was sued for not retaining e-mails per approved records retention schedule
Montana		No	
Nebraska		No	
Nevada		No	
New Hampshire		No	
New Jersey		No	
New York		No	
North Carolina		No	
Ohio		No	
Oklahoma		No	
Oregon		No	
Tennessee		No	
Texas		No	
Utah		No	
Vermont		No	
Virginia		No	
Washington		No	
Wisconsin		No	

4) Are you aware of any pending legal challenges of your records retention policy? Are you aware of any legal challenges for your failure to have such a policy or comply with the existing policies?			
State	**Yes**	**No**	**Response**
Alabama		No	
Arkansas	Yes		Construction claim before an administrative body was filed by contractor in 2008; claim is still pending. Claimant raised the issue of whether Arkansas project design consultant properly kept and retained e-mail correspondence related to the project as part of their file.
Alaska		No	
Arizona		No	
Connecticut		No	
Hawaii		No	
Kentucky		No	
Kansas		No	
Maryland		No	
Minnesota		No	
Mississippi		No	
Michigan		No	
Missouri		No	
Montana		No	
Nebaska		No	
New Hampshire		No	
Nevada		No	
North Carolina		No	
New Jersey		No	
New York		No	
Ohio		No	
Oklahoma		No	
Oregon		No	
Tennessee		No	
Texas		No	
Utah		No	
Vermont		No	
Virginia		No	
Washington		No	
Wisconsin		No	

5) What methods are you using to retain documents? For example, storage of paper documents, microfilm, or scanning and saving to a central computer database. Have you experienced any problems retrieving and authenticating these documents once they are stored? Are you required by law to maintain old systems so that your older documents can be easily retrieved? If you are not required by law, do you maintain old systems for ease of retrieval in new systems?

State	Yes	No	Response
Alabama	Yes		Paper stored with their offices then destroyed consistent with retention policy. Final engineering drawings are scanned and digitally stored. Problems are inadequate indexing during scanning that was done by a consultant. Now staff does it and problem has been eliminated. Do not have to maintain old systems but have converted microfilmed documents to digital.
Alaska	Yes		Uses traditional storage methods.
Arizona			No response.
Arkansas	Yes		Documents are retained by traditional paper storage, microfilm, and scanning.
Connecticut	Yes		Varies by type of record.
Hawaii	Yes		Uses traditional methods—some problems with old microfilm, hard to read.
Kansas	Yes		Several mediums are used depending on the information, source, and user. Procedures must be approved through Electronic Records Committee.
Kentucky	Yes		Currently use traditional storage of paper documents and microfilm. Looking into the process of scanning and saving documents to CD or DVD. No problems with retrieving stored documents, short of occasionally finding that something had been misfiled. Not required by law to maintain old computer systems, but most older systems are maintained in order to be able to obtain historical data.
Maryland	Yes		Paper, CDs, storage online; law requires information to be usable.
Michigan	Yes		Uses many different systems; no problems in retrieving or authenticating; maintains old systems to be able to transition to new systems.
Minnesota	Yes		Many formats are used including paper, microfilm, digital, x-rays, video, databases—agency attempts to migrate media and data and to stay current with technology. The agency is not required by law to maintain old systems. Metadata are retained with documents stored in document management system.
Mississippi	Yes		Mississippi uses all traditional methods.
Missouri	Yes		Paper, scanning, microfilming. Experienced no problems authenticating. Understand that law implicitly requires reasonable efforts to retain data.
Montana	Yes		Uses all traditional methods; sometimes has difficulties in locating records due to nonstandardized naming protocol; paper copies easier to find because easier to locate offices that should have them.
Nebraska			The State Records Center provides scanning and microfilming services.
Nevada	Yes		Permanent storage is microfilm and/or paper. Plans, policies,

			and procedures for scanning and retaining electronic files, as working files only, are being developed.
New Hampshire	Yes		Paper documents moved to archives facility that has fire prevention system to protect and reduce water damage. Facility responsible for maintaining, retrieving, delivering, and tracking all items. Problems have been that old and new systems are not always compatible. Storage and scanning ensures document's retrieval.
New Jersey	Yes		Uses all traditional types; now must be saved in "eye-readable" format like microfilm—also must have methods in place for updating systems as new processes come online. N.J. Admin. Code 15:3 *et seq*.
New York	Yes		All traditional storage methods used, no special problems. NY regulations require state agencies to maintain a practical method of records retrieval of electronic records—NYCRR, regulation 188.20 relates to retention and preservation of electronic records.
North Carolina	Yes		Maintains old systems to the extent necessary to enable retrieval.
Oregon	Yes		Uses traditional methods; starting an Electronic Content Management program; custodians must make sure records can be read.
Texas	Yes		Uses traditional methods of storing paper, scanning and microfilming documents. 13 TAC section 6.94 requires agencies to take measures to preserve the accessibility and readability of e-records through retention of the required technology or copying or migrating to replacement technologies.
Utah	Yes		Paper, microfilm, scanning. Agency not required by law to maintain old system; however, some systems are maintained to ensure retrieval of documents.
Vermont	Yes		Microfilm, microfiche, paper, Mylar, blueprints, photos, carbon copies, digital images, ONBase, COLD Technology (Computer Output to Laser Disk–Reports), video logs, CADD, Digital Print Room for plans. Cross Sections, various maps, financial records in databases, accounting programs, CDs, DVDs, removable disk drives, flash drives, optical drives, biometric drives. VTrans has been electronically storing documents since 1995. Experienced very minimal problems, and those were successfully corrected by our Information Technology Unit. Where information was not migrated to newer technology, we must maintain the ability to reproduce the documents.
Virginia	Yes		Paper, microfilm, saving to computer, scanning; no problems authenticating once stored; 42.1-85 requires all state agencies ensure records are preserved, maintained, accessible throughout their life cycle, including converting and migrating records.
Washington	Yes		Traditional storage of paper, using microfilm and scanning. Maintain old systems to ensure easy retrieval of information.
Wisconsin	Yes		Uses traditional methods; problems retrieving have been experienced; required by law to maintain old systems.

6) How do you handle "proprietary" or other information contained in bid proposals or other confidential information that the submitter may reasonably believe would be protected from disclosure?	
State	**Response**
Alabama	Proprietary and confidential bidding information is maintained in paper format and kept under lock until destroyed consistent with records retention system.
Alaska	Alaska Statute 36.30.230.
Arizona	No response.
Arkansas	Bid tabulation not released to public until bid is awarded. Bid estimates are not open for public review pursuant to Ark. 25-19-105(b)(9)(A).
Connecticut	1-210(b)(24) protected until contract executed; proprietary protected under 1-210(b)(5).
Hawaii	Confidential documents kept in a secure folder with limited access.
Kansas	Open records act exempts from disclosure plans, designs, drawings, or specifications which are prepared by a person other than an employee of a public agency or records which are the property of a private person.
Kentucky	When proprietary information is archived, this portion is filled out with the proper authority cited. This gives notice to archive personnel that the records contained within that shipment are not to be accessed by the public, or by any unauthorized Cabinet personnel. The Open Records Act contains provisions that protect any proprietary information from public disclosure. Personnel are required to fill out a transmittal form to accompany each shipment to the archives. This transmittal has a field asking "Is access to these records restricted? If yes, cite authority."
Maryland	No response.
Michigan	Uses FOIA exemptions when applicable.
Minnesota	Data practices act—chapter 13 of Minnesota Statutes—addresses proprietary information. Some aspects of the bidding process are considered not public for periods of time.
Mississippi	Statute 25-61-9 protects trade secrets/confidential commercial information.
Missouri	Open Records Act, Missouri Uniform Trade Secrets Act.
Montana	Montana's constitution says all records in agency's possession are public records—no submitter can claim reasonable belief that document would not be provided if requested; however, if a contractor requests a document that might be confidential, such as another contractor's bid, MDT notifies the submitting party in writing of the request before releasing the documents in case a party would want to file a legal action to prevent MDT from providing it.
Nebraska	Protects proprietary information.
Nevada	Records are screened for proprietary information before any public release.
New Hampshire	Bid proposals, once opened, are available for public disclosure, barring financial and other information outlined in attached policy.
New Jersey	Addressed in public records law and N.J. Admin. Code 16:1A-1.8, NJDOT regulation.
New York	Exempts documents that if disclosed would impair contract awards or collective bargaining negotiations or trade secrets.
North Carolina	N.C. Gen. Stat. 132-1.2 protected if meets statutory criteria—if designated as confidential or trade secret at the time of disclosure.
Ohio	Sealed bids are exempt from open records law; bidder qualifications are exempt; trade secrets are exempt.

Oklahoma	Not disclosed.
Oregon	Internal review policy.
Texas	Security procedures are in place for offices responsible for handling or processing that information.
Utah	Policy covers.
Vermont	Bid proposals are regulated as Restricted/Confidential records. The only individuals that can access these records are those who have been granted access by the VTrans Public Records Officer in writing. This information is provided to the Records Center, and only individuals included on this list are allowed to request or view these records. VTrans employees possess a photo ID that includes their photo, signature, agency, division, work address, job title, birthdate, employee ID#, and date of issue. Restricted/confidential information is removed from the paper proposals prior to public viewing. Only authorized personnel are allowed to view this data. Bids that are submitted electronically are sent to an offsite high security SSL server, where all data is highly encrypted and requires a key for access. The server and a contractor's document are only accessible by that contractor via a key for uploading the bid proposal and by contract administration personnel responsible for processing the bid submission.
Virginia	2.2-3705.6 contains exclusions from FOIA for proprietary and trade secrets, redacted if otherwise subject to disclosure.
Washington	RCW 42.56 State Public Records Act stipulates what is exempt.
Wisconsin	Proprietary or trade secret must be identified by vendor/bidder. If it is requested, they notify the vendor/bidder of the request; if they want to fight it, they have to handle the litigation.

7) If you receive a request for building layout plans, computer programs, computer coding information, bridge inspections or other structural information, is this request treated differently than other requests for public records? Have you adopted a specific critical infrastructure policy? If so would you please attach a copy to your response?

State	Response
Alaska	Refer to FOIA.
Arizona	Federal Homeland Security Act, A.R.S. 39-121 *et seq*.
Arkansas	Records containing measures, procedures, instructions, or related data of a computer/computer system/network, including telecommunication networks, applications, passwords, PINS, etc. are not subject to release pursuant to Ark. Code Ann. 25-19-105(b)(11). Critical information policy not subject to public release. Personnel have made a list of infrastructure and structures plans that are not released to public in accordance with 6 U.S.C. 131, 132 and 133, 23 U.S.C. 40, and Ark. Code Ann. 25-19-105(a)(1)(A).
Connecticut	Exemptions in FOIA that cover some of these subjects.
Hawaii	Requests for plans are scrutinized and screened for security purposes—with other state and, if applicable, federal agencies; no specific critical infrastructure policy.
Kansas	Complies with open records act—turn over records not exempt—one exemption is for software programs for electronic data processing.
Kentucky	Documents of this nature are excepted from disclosure pursuant to Ky. Rev. Stat. 61.878(1)(m). This statute may be accessed online at the following address: http://www.lrc.ky.gov/KRS/061-00/878.PDF.
Maryland	State law 10-618 permits denial of that information. Department has a Critical Infrastructure Plan.
Michigan	All requests are handled through FOIA process, dependent on statutory ex-

	emptions.
Minnesota	Agency has identified critical infrastructures; certain data on those structures are nonpublic—security policy is classified as security information under Minnesota Gov't Data Practices Act 13.37 1(a).
Mississippi	Request not treated differently.
Missouri	MoDOT Critical Infrastructure Information Policy.
Nebraska	Reviewed on a case-by-case basis.
Nevada	Records are screened before any public release.
New Hampshire	Handled on case-by-case basis, no specific policy other than right-to-know law and its limitations.
New Jersey	Based on public records act, N.J. Admin. Code 16:1A-1.8, and NJDOT regulation regarding release of records, N.J. Admin. Code 16:1A-1.8.
New York	Exempts records which if disclosed would endanger the life or safety of any persons or jeopardize an agency's capacity to guarantee the security of its information technology assets.
North Carolina	NCGS 132-1.6 regarding protection of emergency response plans and sensitive security information
Ohio	Any security records are protected from disclosure, trade secrets are exempt, no specific infrastructure policy.
Oklahoma	Handled mostly just like any other request.
Oregon	No specific critical infrastructure policy.
Texas	Has policy on access to critical infrastructure information.
Utah	Administrative Rule 63G-2-106.
Vermont	Act 110: An act relating to access to Public Records yes: http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=01&Chapter=005&Section=00317.
Virginia	2.2-3705.2 exclusions from FOIA if disclosure would jeopardize the security of any government facility, structure, persons using that facility; critical infrastructure policy is not available for release.
Washington	Wash. Rev. Code 42.56 State Public Records Act stipulates what is exempt.
Wisconsin	Federal law 42 U.S.C. 5195c, 6 C.F.R. part 2. Department has a critical infrastructure policy.

8) Does your agency have a policy advising staff how to handle public records requests? If so would you please attach a copy of the policy to your response?

State	Yes	No	Response
Alabama			Records management policy provides all requests go through legal department; Section 36-12-40 requires operational records to be open to public inspection.
Alaska		No	
Arizona	Yes		
Arkansas			Requests are sent to legal department to ensure compliance with all appropriate laws.
Connecticut	Yes		Currently in revision.
Georgia			Ga. Code Ann. 50-18-70.
Hawaii			Uniform information practices act for handling public records requests; guidelines for personal information records.
Kansas	Yes		Kan. State Ann. 75-3501-3520.
Kentucky			The Kentucky Attorney General has prepared an outline concerning Open Records and Open Meetings to educate public employees and assist with the proper handling of public records requests. This outline may be accessed at the follow-

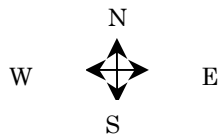
			ing address: http://ag.ky.gov/civil/outline.htm.
Maryland	Yes		
Michigan			FOIA Act, Section 15.231.
Minnesota			No policy regarding records requests, but staff are trained to assist with requests.
Mississippi	Yes		
Missouri	Yes		
Montana			
Nebraska	Yes		Yes; no copy available at this time.
Nevada			Informal policy—requests usually go through legal department.
New Hampshire			NH DOT Right to Know Policy 103.
New Jersey			N.J. Admin. Code regulation 47:1A-1.1.
New York			New York has internal policy advising staff on processing requests for department records.
North Carolina			In development.
Ohio	Yes		
Oregon	Yes		
Texas	Yes		
Utah	Yes		
Vermont			DPM concerning compliance with FOIA requests; also has staff tracker to assist in processing requests.
Virginia	Yes		
Washington	Yes		
Wisconsin	Yes		

APPENDIX C: EMPLOYEE WITNESS STATEMENT

Date of Event: _____ Time of Event: _____
Employee Name: _____ Job Title: _____
Route: _____ At or Near intersection: _____
County: _____ Direction: _____
Construction work: *Yes No* If yes, who was the contractor and foreman: _____
Type of Work Being Performed: _____
Weather Condition: _____
Pavement Conditions: _____
Did any MoDOT employee witness the event? *Yes No* If so, whom: _____
Did any MoDOT employee take pictures? *Yes No* If so, whom: _____
Was Traffic Control in Place? *Yes No*
If Yes, what traffic control was in place: _____

Supervisor/Crew Leader, below provide a Detailed Diagram of the traffic control that is noted above:

(use another piece of paper if necessary)



APPENDIX D: DOCUMENTS RELATED TO RECRUITMENT[165]

Type of Record	Retention Period	Statute
Job orders submitted by the employer to employment agencies, or labor organizations for recruitment of employees	1 year from date of personnel action	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Job advertisements and notices to public or to employees regarding job openings, training programs, promotions, and opportunities for overtime	1 year from date of personnel action	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Criteria for selection for apprenticeship programs in recognized trade or craft; chronological list of all applicants' names, addresses, dates of application, sex, minority group class (race or national origin); and any test papers or interview records on which hiring decisions were made	1) 2 years or period of chosen applicant's apprenticeship, whichever is longer; or 2) 1 year from date of report	42 U.S.C. § 2000e8c; 29 C.F.R. § 1602 (Title VII of the Civil Rights Act of 1964)

Documents Related to Employee Selection

Type of Records	Retention Period	Statute
Written training agreements, summaries of applicants' qualifications, job criteria, interview records, and identification of minority and female applicants	Duration of training program plus 3 years	29 U.S.C. § 206(d)(1); 29 U.S.C. § 211; 29 C.F.R. § 516.5 (Fair Labor Standards Act (FLSA) and National Labor Relations Act)
Test appearances and results from employment test	1 year from date of personnel action	29 U.S.C. § 626;29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Results in physical examinations	1 year from date of personnel action	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Promotion, demotion, transfer, selection for training, layoff, recall, or discharge	1 year from date of personnel action	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Hiring documents, including job applications, resumes, job inquiries, and records of refusals to hire	1 year from date of personnel action	29 U.S.C. § 62; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Application forms and other preemployment records of applicants for temporary positions	1 year after personnel action	29 U.S.C. § 626; 29 C.F.R. § 1627.3 9 (Age Discrimination in Employment Act)
All personnel or employment records, including application forms, resumes, other hiring records; records regarding promotion, demo-	1 year from date records made or personnel action taken, whichever is later	42 U.S.C. § 2000e8c; 29 C.F.R. § 1602.14 (Title VII of the Civil Rights Act of 1964)

[165] *See* http://www.mnwfc.org/winona/record_retention_requirements1.htm, last visited Apr. 5, 2009.

tion, transfer, layoff, discharge, pay rates, or other compensation terms		
INS form I-9 Employment Eligibility Verification Form	3 years after date of hire or 1 year after date of termination, whichever is later	8 U.S.C. § 1324a (Immigration and Nationality Act)
Employers having 100 or more employees, EEO-I Form	Copy of most recent report for each reporting unit must always be retained	42 U.S.C. § 2000e8c; 29 C.F.R. § 1602 (Title VII of the Civil Rights Act of 1964)
Written affirmative action program with supporting documents, including evaluations, documents regarding compliance with EEO antidiscrimination and affirmative action regulations, and test records and results (government contractors with 150 or more employees and contractors of $150,000 or more).	Retention period not specified. It is nonetheless suggested that these records be retained for at least 5 years	Executive Order No. 11246 41 C.F.R. § 60-1.4(a)

Documents Related to Employee Benefit Plans

Type of Records	Retention Period	Statute
Payroll records; collective bargaining agreements, including any changes; individual contracts; written agreements under the FLSA; sales and purchase records; and certificates and notices of the Wage and Hour Administrator	3 years	29 U.S.C. § 206(d)(1); 29 U.S.C. § 211; 29 C.F.R. § 516.5 (FLSA and National Labor Relations Act)
Supplementary basic records including basic employment and earnings records; wage and rate tables utilized to calculate straight time and overtime work schedules; worktime schedules; order, shipping, and billing records; records of additions to, or deductions from, wages paid; records used for determining costs; and records explaining basis for payment of any wage differential to employees of the opposite sex	2 years	29 U.S.C. § 206(d)(1); 29 U.S.C. § 211; 29 C.F.R. §§ 516.6 and 1620.32 (FLSA and National Labor Relations Act)
Certificates of Age	Until termination of employment	29 U.S.C. § 206(d)(1); 29 U.S.C. § 211; 29 C.F.R. § 570.6 (FLSA and National Labor Relations Act)
Payroll or other records containing name, address, birthdate, occupation, pay rate, and weekly compensation	3 years	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)
Payroll records including name, address, job category, pay rate, weekly number of hours worked, deductions made, and wages paid	3 years from completion of contract	40 U.S.C. § 276a; 29 C.F.R. § 5.5 (Davis-Bacon Act)

Documents Relating to Employee Exposure to Toxic Substances

Type of Records	Retention Period	Statute
Log and summary of occupational injuries and illnesses (OSHA form No. 200)	5 years following end of year to which records relate	29 U.S.C. § 657; 29 C.F.R. § 1904.2 (Occupational Safety and Health Act (OSHA))
Supplemental record for each occupational injury or illness (OSHA form No. 101)	5 years	29 U.S.C. § 657; 29 C.F.R. § 1904.4 (OSHA)
Annual summary of occupational injuries and illnesses	5 years	29 U.S.C. § 657; 29 C.F.R. § 1904.5 (OSHA)
Records of medical examinations required by law	Duration of employment plus 30 years, unless OSHA requirements provide otherwise	29 U.S.C. § 657; 29 C.F.R. § 1910.1020 (OSHA)
Records of monitoring exposure to hazardous materials	30 years	29 U.S.C. § 657; 29 C.F.R. § 1910.1020 (OSHA)
Manufacturers, processors, or distributors of any chemical substance must retain records of employees' "significant adverse reactions" to health or the environment	30 years from date such adverse reaction first reported to or known by person maintaining record	15 U.S.C. § 2607 (Toxic Substances Control Act)
Any other records of such adverse reactions	5 years from date first reported to or known by person maintaining the record	15 U.S.C. § 2607 (Toxic Substances Control Act)
Consumer allegations of personal injury or harm to health, reports of occupational disease or injury, and reports or complaints of injury to the environment submitted to the manufacturer, processor, or distributor from any source	30 years for employee claims of occupational disease or occupational health problems	15 U.S.C. § 2607 (Toxic Substances Control Act)

Documents Related to Drug and Alcohol Testing

Type of Records	Retention Period	Statute
Records related to positive test results and/or refusals to take a required alcohol and/or controlled substances test; driver evaluation and referrals	5 years	49 C.F.R. § 382.401 (Controlled Substances and Alcohol Use and Testing)
Records related to the collection process, including collection logbooks; documents relating to the random selection process, reasonable suspicion testing, post-accident testing; documents verifying employee's inability to provide breath for testing	2 years	49 C.F.R. § 382.401 (Controlled Substances and Alcohol Use and Testing)
Records related to negative and cancelled test results	1 year	49 C.F.R. § 382.401 (Controlled Substances and Alcohol

		Use and Testing)
Records related to breath alcohol testing–related training	2 years	49 C.F.R. § 382.401 (Controlled Substances and Alcohol Use and Testing)

Documents Related to Discrimination Charge

Type of Records	Retention Period	Statute
Personnel records concerning any discrimination charge brought by any agency or individual (e.g., records about charging party and all other employees holding similar positions, application forms, or test papers completed by all applicants for same position)	Until final disposition	42 U.S.C. § 2000(e)(8)(c); 29 C.F.R. § 1602 (Title VII of the Civil Rights Act of 1964)
In action brought against employer, any personnel records concerning employee or applicant	Until final disposition	29 U.S.C. § 626; 29 C.F.R. § 1627.3 (Age Discrimination in Employment Act)

Documents Related to Employee Leaves of Absence

Type of Records	Retention Period	Statute
Basic payroll and identifying employee data, including name, address, occupation, rate of pay and terms of compensation, daily and weekly hours worked per pay period, and additions or deductions from wages	3 years	29 U.S.C. § 2616; 29 C.F.R. § 825.500 (Family and Medical Leave Act of 1993 (FMLA))
All records pertaining to compliance with FMLA's leave requirements, including dates and hours (if less than a full day) of FMLA leave; copies of employer notices; documents describing premium payments and employee benefits; and records of disputes with employees over FMLA benefits	3 years	29 U.S.C. § 2616; 29 C.F.R. § 825.500 (FMLA)
Documents describing FMLA notices and copies of employer's FMLA policy	3 years	29 U.S.C. § 2616; 29 C.F.R. § 825.500 (FMLA)

APPENDIX E: CONSTRUCTION RECORDS[166]

Type of Record	Retention Period
Administration Records—Special studies, cost analysis, bid letters and awards, contract claims review board actions, contractor records, contractor prequalifications, labor relations, ineligible contractor listings, prevailing wage rates, related correspondence, and background information	10 years
Construction Contract Project Records—Case files documenting phases of transportation construction project contracts. Contract award records, field engineers' daily and weekly reports, time records, change orders, progress estimates and costs reports, job cost summaries, subcontracts, contractor payrolls, affirmative action and equal employment documentation, utility records, project permits, legal records, photos, public relations records, work schedules, engineers' diaries, progress reports, survey records, insurance, narrative reports, correspondence, and related documentation	10 years
Material Records—Field tests, material certification, specifications for material acceptance, related correspondence, and supporting documentation	10 years

[166] *See* Michigan Department of Transportation's June 2, 2008, memo entitled, *Detention and Disposal of Construction Project Records*, found at http://www.michigan.gov/documents/mdot_construction_record_requirements_109208_7.pdf.

APPENDIX F: RIGHT-OF-WAY DOCUMENTS

Type of Record	Retention Period
Federal Aid Projects—Accounts, papers, maps, photos, documents of any sort, financial records, statistical records, acquisition, and relocation costs	3-year minimum; begins when final claims are submitted for payment to DOT; *see* 23 C.F.R. 710.201(f); *see also*, e.g., *Alabama Department of Transportation Records Disposition Authority Manual*, http://www.archives.state.al.us/officials/rdas/dot--division.pdf
Condemnation of Land Documentation—Process for planning and acquiring parcels of land. May include reports, boundary descriptions, photos, cost studies, and correspondence.	6 years after parcel acquired, then archive permanently; *see Colorado State Archive Records Management Manual*, available at http://www.colorado.gov/dpa/dort/archives/rm/rmman/sch7.htm
Land Appraisals	12 years after parcel acquired or litigation resolved; *see*, e.g., Oregon Records Retention Schedule, available at http://www2.co.multnomah.or.us/County_Management/FREDS/Records/retention/Property Valuation & Appraisal (PV3).htm
Land Sales and Conveyance Documentation	12 years after parcel acquired, then archive permanently; *see* Oregon Records Retention Policy, available at http://www2.co.multnomah.or.us/County_Management/FREDS/Records/retention/Property Valuation & Appraisal (PV3).htm
Land Title Documents	Retain permanently; *see*, e.g., *The Arkansas General Records Retention Schedule Procedural Handbook*, http://www.state.ar.us/dfa/igs/documents/records_procedures.doc
Land Inventory	Retain permanently; *see* Oregon Records Retention Policy, available at www2.co.multnomah.or.us/.../retention/Survey%20(SUR1).htm
Highway Plans	Retain permanently; *see*, e.g., *Alabama Department of Transportation Records Disposition Authority Manual*, http://www.archives.state.al.us/officials/rdas/dot--division.pdf

APPENDIX G: SUGGESTED PROTOCOL FOR DISCOVERY OF ELECTRONICALLY STORED INFORMATION

These guidelines were developed by a committee in Maryland that consisted of judges, attorneys, and technical advisors and are taken from the "Suggested Protocol for Discovery of Electronically Stored Information" as set forth by the United States District Court for the District of Maryland.[167] The guidelines are set out below.

> In light of the recent amendments to the Federal Rules of Civil Procedure regarding discovery of electronically stored information ("ESI"), a joint bar-court committee consisting of Magistrate Judge Paul W. Grimm and members of the Bar of this Court as well as technical consultants developed a proposed protocol for use in cases where ESI may be involved. This is a working model that has not been adopted by the court but may be of assistance to counsel. It is the intent of the joint committee to review the Proposed Protocol periodically to determine if revisions would be appropriate, and after a sufficient period of time to evaluate the proposed protocol has passed, to determine whether to recommend to the Court that more formal guidelines or local rules relating to ESI be considered for adoption.
>
> Given these rule changes, it is advisable to establish a suggested protocol regarding, and a basic format implementing, only those portions of the amendments that refer to ESI. The purpose of this Suggested Protocol for Discovery of Electronically Stored Information (the "Protocol") is to facilitate the just, speedy, and inexpensive conduct of discovery involving ESI in civil cases, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without Court intervention.
>
> While this Protocol is intended to provide the parties with a comprehensive framework to address and resolve a wide range of ESI issues, it is not intended to be an inflexible checklist. The Court expects that the parties will consider the nature of the claim, the amount in controversy, agreements of the parties, the relative ability of the parties to conduct discovery of ESI, and such other factors as may be relevant under the circumstances. Not all aspects of this Protocol may be applicable or practical for a particular matter, and indeed, if the parties do not intend to seek discovery of ESI it may be entirely inapplicable to a particular case. The Court encourages the parties to use this Protocol in cases in which there will be discovery of ESI, and to resolve ESI issues informally and without Court supervision whenever possible. In this regard, compliance with this Protocol may be considered by the Court in resolving discovery disputes, including whether sanctions should be awarded pursuant to Fed.R.Civ.P. 37;
>
> **SCOPE**
>
> This Protocol applies to the ESI provisions of Fed.R.Civ.P. 16, 26, 33, 34, or 37, and, insofar as it relates to ESI, this Protocol applies to Fed.R.Civ.P. 45 in all instances where the provisions of Fed.R.Civ.P. 45 are the same as, or substantially similar to, Fed.R.Civ.P. 16, 26, 33, 34, or 37. In such circumstances, if a Conference pursuant to Fed.R.Civ.P. 26(f) is held, it may include all parties, as well as the person or entity served with the subpoena, if said Conference has not yet been conducted. If the Conference has been conducted, upon written request of any party or the person or entity served with the subpoena, a similar conference may be conducted regarding production of ESI pursuant to the subpoena. As used herein, the words "party" or "parties" include any person or entity that is served with a subpoena pursuant to Fed.R.Civ.P. 45. Nothing contained herein modifies Fed.R.Civ.P. 45 and, specifically, the provision of Rule 45(c)(2)(B) regarding the effect of a written objection to inspection or copying of any or all of the designated materials or premises.

[167] The document can be found at www.mdd.uscourts.gov/news/news/ESIProtocol.pdf.

In this Protocol, the following terms have the following meanings:

A. "Meta-Data" means: (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted or otherwise manipulated by a user of such system. Meta-Data is a subset of ESI.

B. "Native File(s)" means ESI in the electronic format of the application in which such ESI is normally created, viewed and/or modified. Native Files are a subset of ESI.

C. "Static Image(s)" means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. In the absence of agreement of the parties or order of Court, a Static Image should be provided in either Tagged Image File Format (TIFF, or .TIF files) or Portable Document Format (PDF). If load files were created in the process of converting Native Files to Static Images, or if load files may be created without undue burden or cost, load files should be produced together with Static Images.

CONFERENCE OF PARTIES AND REPORT

The parties are encouraged to consider conducting a Conference of Parties to discuss discovery of ESI regardless of whether such a Conference is ordered by the Court. The Conference of Parties should be conducted in person whenever practicable. Within 10 calendar days thereafter, the parties may wish to file, or the Court may order them to file, a joint report regarding the results of the Conference. This process is also encouraged if applicable, in connection with a subpoena for ESI under Fed.R.Civ.P. 45. The report may state that the parties do not desire discovery of ESI, in which event Paragraphs 4A and B are inapplicable.

A. The report should, without limitation, state in the section captioned "Disclosure or discovery of electronically stored information should be handled as follows, the following: (1) Any areas on which the parties have reached agreement and, if any, on which the parties request Court approval of that agreement; (2) Any areas on which the parties are in disagreement and request intervention of the Court.

B. The report should, without limitation, if it proposes a "claw back" agreement, "quick peek," or testing or sampling, specify the proposed treatment of privileged information and work product, in a manner that, if applicable, complies with the standard set forth in *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. On-site inspections of ESI under Fed.R.Civ.P. 34(b) should only be permitted in circumstances where good cause and specific need have been demonstrated by the party seeking disclosure of ESI (the "Requesting Party"), or by agreement of the parties. In appropriate circumstances the Court may condition on-site inspections of ESI to be performed by independent third party experts, or set such other conditions as are agreed by the parties or deemed appropriate by the Court.

C. Unless otherwise agreed by the parties, the report described by this provision should be filed with the Court prior to the commencement of discovery of ESI.

NEED FOR PRIOR PLANNING

Insofar as it relates to ESI, prior planning and preparation is essential for a Conference of Parties pursuant to Fed.R.Civ.P. 16, 26(f), and this Protocol. Counsel for the Requesting Party and Counsel for the party producing, opposing, or seeking to limit disclosure of ESI ("Producing Party") bear the primary responsibility for taking the planning actions contained herein. Failure to reasonably com-

ply with the planning requirements in good faith may be a factor considered by the Court in imposing sanctions.

EXCHANGE OF INFORMATION BEFORE RULE 26(f) CONFERENCE

Insofar as it relates to ESI, in order to have a meaningful Conference of Parties, it may be necessary for parties to exchange information prior to the Fed.R.Civ.P. 26(f) Conference of Parties. Parties are encouraged to take the steps described in Paragraph 7 of this Protocol and agree on a date that is prior to the Fed.R.Civ.P. 26(f) Conference of Parties, on which agreed date they will discuss by telephone whether it is necessary or convenient to exchange information about ESI prior to the conference.

A. A reasonable request for prior exchange of information may include information relating to network design, the types of databases, database dictionaries, the access control list and security access logs and rights of individuals to access the system and specific files and applications, the ESI document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy.

B. An unreasonable request for a prior exchange of information should not be made.

C. A reasonable request for a prior exchange of information should not be denied.

D. To the extent practicable, the parties should, prior to the Fed.R.Civ.P. 26(f) Conference of Parties, discuss the scope of discovery of ESI, including whether the time parameters of discoverable ESI, or for subsets of ESI, may be narrower than the parameters for other discovery.

E. Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel should discuss with their clients and each other who will participate in the Fed.R.Civ.P. 26(f) Conference of Parties. This discussion should specifically include whether one or more participants should have an ESI coordinator (*see* Paragraph 7.B) participate in the Conference. If one participant believes that the other should have an ESI coordinator participate, and the other disagrees, the Requesting Party should state its reasons in a writing sent to all other parties within a reasonable time before the Rule 26(f) Conference. If the Court subsequently determines that the Conference was not productive due to the absence of an ESI coordinator, it may consider the letter in conjunction with any request for sanctions under Fed.R.Civ.P. 37.

PREPARATION FOR RULE 26(f) CONFERENCE

Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel for the parties should:

A. Take such steps as are necessary to advise their respective clients, including, but not limited to, "key persons" with respect to the facts underlying the litigation, and information systems personnel, of the substantive principles governing the preservation of relevant or discoverable ESI while the lawsuit is pending. As a general principle to guide the discussion regarding litigation hold policies, Counsel should consider the following criteria:

(1) Scope of the "litigation hold," including:

(a) A determination of the categories of potentially discoverable information to be segregated and preserved;

(b) Discussion of the nature of issues in the case, as per Fed.R.Civ.P. 26(b)(1);

(i) Whether ESI is relevant to only some or all claims and defenses in the litigation;
(ii) Whether ESI is relevant to the subject matter involved in the action;

(c) Identification of "key persons," and likely witnesses and persons with knowledge regarding relevant events;

(d) The relevant time period for the litigation hold;

(2) Analysis of what needs to be preserved, including:

(a) The nature of specific types of ESI, including, email and attachments, word processing documents, spreadsheets, graphics and presentation documents, images, text files, hard drives, databases, instant messages, transaction logs, audio and video files, voicemail, Internet data, computer logs, text messages, or backup materials, and Native Files, and how it should be preserved:

(b) the extent to which Meta-Data, deleted data, or fragmented data, will be subject to litigation hold;

(c) paper documents that are exact duplicates of ESI;

(d) any preservation of ESI that has been deleted but not purged;

(3) Determination of where ESI subject to the litigation hold is maintained, including:

(a) format, location, structure, and accessibility of active storage, backup, and archives;

(i) servers;
(ii) computer systems, including legacy systems;
(iii) remote and third-party locations;
(iv) back-up media (for disasters) vs. back-up media for archival purposes/record retention laws;

(b) network, intranet, and shared areas (public folders, discussion databases, departmental drives, and shared network folders);

(c) desktop computers and workstations;

(d) portable media; laptops; personal computers; PDA's; paging devices; mobile telephones; and flash drives;

(e) tapes, discs, drives, cartridges and other storage media;

(f) home computers (to the extent, if any, they are used for business purposes);

(g) paper documents that represent ESI.

(4) Distribution of the notification of the litigation hold:

(a) to parties and potential witnesses;

(b) to persons with records that are potentially discoverable;

(c) to persons with control over discoverable information; including:

(i) IT personnel/director of network services;
(ii) custodian of records;
(iii) key administrative assistants;

(d) third parties (contractors and vendors who provide IT services).

(5) Instructions to be contained in a litigation hold notice, including that:

(a) there will be no deletion, modification, alteration of ESI subject to the litigation hold;

(b) the recipient should advise whether specific categories of ESI subject to the litigation hold require particular actions (*e.g.,* printing paper copies of email and attachments) or transfer into "read only" media;

(c) loading of new software that materially impacts ESI subject to the hold may occur only upon prior written approval from designated personnel;

(d) where Meta-Data, or data that has been deleted but not purged, is to be preserved, either a method to preserve such data before running compression, disk defragmentation or other computer optimization or automated maintenance programs or scripts of any kind ("File and System Maintenance Procedures"), or the termination of all File and System Maintenance Procedures during the pendency of the litigation hold in respect of Native Files subject to preservation;

(e) reasonably safeguarding and preserving all portable or removable electronic storage media containing potentially relevant ESI;

(f) maintaining hardware that has been removed from active production, if such hardware contains legacy systems with relevant ESI and there is no reasonably available alternative that preserves access to the Native Files on such hardware.

(6) Monitoring compliance with the notification of litigation hold, including:

(a) identifying contact person who will address questions regarding preservation duties;
(b) identifying personnel with responsibility to confirm that compliance requirements are met;
(c) determining whether data of "key persons" requires special handling (*e.g.,* imaging/cloning hard drives);
(d) periodic checks of logs or memoranda detailing compliance;
(e) issuance of periodic reminders that the litigation hold is still in effect.

B. Identify one or more information technology or information systems personnel to act as the ESI coordinator and discuss ESI with that person;

As used herein, the term "reasonably familiar" contemplates a heightened level of familiarity with any ESI that is identified by opposing counsel pursuant to Paragraph 6 of this Protocol, however, that level of familiarity is conditioned upon the nature of the pleadings, the circumstances of the case, and the factors contained in Fed.R.Civ.P. 26(b)(2)(C).

C. Identify those personnel who may be considered "key persons" by the events placed in issue by the lawsuit and determine their ESI practices, including those matters set forth in Paragraph 7.D, below. The term "key persons" is intended to refer to both the natural person or persons who is/are a "key person(s)" with regard to the facts that underlie the litigation, and any applicable clerical or support personnel who directly prepare, store, or modify ESI for that key person or persons, includ-

ing, but not limited to, the network administrator, custodian of records or records management personnel, and an administrative assistant or personal secretary;

D. Become reasonably familiar with their respective clients' current and relevant past ESI, if any, or alternatively, identify a person who can participate in the Fed.R.Civ.P. 26(f) Conference of Parties and who is familiar with at least the following:

(1) Email systems; blogs; instant messaging; Short Message Service (SMS) systems; word processing systems; spreadsheet and database systems; system history files, cache files, and cookies; graphics, animation, or document presentation systems; calendar systems; voice mail systems, including specifically, whether such systems include ESI; data files; program files; internet systems; and, intranet systems. This Protocol may include information concerning the specific version of software programs and may include information stored on electronic bulletin boards, regardless of whether they are maintained by the party, authorized by the party, or officially sponsored by the party; provided however, this Protocol extends only to the information to the extent such information is in the possession, custody, or control of such party. To the extent reasonably possible, this includes the database program used over the relevant time, its database dictionary, and the manner in which such program records transactional history in respect to deleted records.

(2) Storage systems, including whether ESI is stored on servers, individual hard drives, home computers, "laptop" or "notebook" computers, personal digital assistants, pagers, mobile telephones, or removable/portable storage devices, such as CD-Roms, DVDs, "floppy" disks, zip drives, tape drives, external hard drives, flash, thumb or "key" drives, or external service providers.

(3) Backup and archival systems, including those that are onsite, offsite, or maintained using one or more third-party vendors. This Protocol may include a reasonable inquiry into the back-up routine, application, and process and location of storage media, and requires inquiry into whether ESI is reasonably accessible without undue burden or cost, whether it is compressed, encrypted, and the type of device on which it is recorded (*e.g.,* whether it uses sequential or random access), and whether software that is capable of rendering it into usable form without undue expense is within the client's possession, custody, or control.

(4) Obsolete or "legacy" systems containing ESI and the extent, if any, to which such ESI was copied or transferred to new or replacement systems.

(5) Current and historical website information, including any potentially relevant or discoverable statements contained on that or those site(s), as well as systems to back up, archive, store, or retain superseded, deleted, or removed web pages, and policies regarding allowing third parties' sites to archive client website data.

(6) Event data records automatically created by the operation, usage, or polling of software or hardware (such as recorded by a motor vehicle's GPS or other internal computer prior to an occurrence), if any and if applicable, in automobiles, trucks, aircraft, vessels, or other vehicles or equipment.

(7) Communication systems, if any and if applicable, such as ESI records of radio transmissions, telephones, personal digital assistants, or GPS systems.

(8) ESI erasure, modification, or recovery mechanisms, such as Meta-Data scrubbers or programs that repeatedly overwrite portions of storage media in order to preclude data recovery, and policies regarding the use of such processes and software, as well as recovery programs that can defeat scrubbing, thereby recovering deleted, but inadvertently produced ESI which, in some cases, may even include privileged information.

(9) Policies regarding records management, including the retention or destruction of ESI prior to the client receiving knowledge that a claim is reasonably anticipated.

(10) "Litigation hold" policies that are instituted when a claim is reasonably anticipated, including all such policies that have been instituted, and the date on which they were instituted.

(11) The identity of custodians of key ESI, including "key persons" and related staff members, and the information technology or information systems personnel, vendors, or subcontractors who are best able to describe the client's information technology system.

(12) The identity of vendors or subcontractors who store ESI for, or provide services or applications to, the client or a key person; the nature, amount, and a description of the ESI stored by those vendors or subcontractors; contractual or other agreements that permit the client to impose a "litigation hold" on such ESI; whether or not such a "litigation hold" has been placed on such ESI; and, if not, why not.

E. Negotiation of an agreement that outlines what steps each party will take to segregate and preserve the integrity of relevant or discoverable ESI. This agreement may provide for depositions of information system personnel on issues related to preservation, steps taken to ensure that ESI is not deleted in the ordinary course of business, steps taken to avoid alteration of discoverable ESI, and criteria regarding the operation of spam or virus filters and the destruction of filtered ESI.

TOPICS TO DISCUSS AT RULE 26(f) CONFERENCE

The following topics, if applicable, should be discussed at the Fed.R.Civ.P. 26(f) Conference of Parties:

A. The anticipated scope of requests for, and objections to, production of ESI, as well as the form of production of ESI and, specifically, but without limitation, whether production will be of the Native File, Static Image, or other searchable or non-searchable formats.

(1) If the parties are unable to reach agreement on the format for production, ESI should be produced to the Requesting Party as Static Images. When the Static Image is separate file, it should not modify the Native File in a manner that materially changes the file and the Meta-Data. After initial production in Static Images is complete, a party seeking production of Native File ESI should demonstrate particularized need for that production.

(2) The parties should discuss whether production of some or all ESI in paper format is agreeable in lieu of production in electronic format.

(3) When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to, the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data, as more fully described in Paragraph 11 of this Protocol) related to the file, and the file's creation date and time. The general process to preserve the data integrity of a file may include one or more of the following procedures:

(a) duplication of responsive files in the file system (A "dynamic system" is a system that remains in use during the pendency of the litigation and in which ESI changes on a routine and regular basis, including the automatic deletion or overwriting of such ESI, creating a forensic copy, including a bit image copy, of the file system or pertinent portion),
(b) performing a routine copy of the files while preserving Meta-Data (including, but not limited to, creation date and time), and/or

(c) using reasonable measures to prevent a file from being, or indicate that a file has been, modified, either intentionally or unintentionally, since the collection or production date of the files. If any party desires to redact contents of a Native File for privilege, trade secret, or other purposes (including, but not limited to, Meta-Data), then the Producing Party should indicate that the file has been redacted, and an original, unmodified file should be retained at least during the pendency of the case.

B. Whether Meta-Data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing said ESI.

C. Preservation of ESI during the pendency of the lawsuit, specifically, but without limitation, applicability of the "safe harbor" provision of Fed.R.Civ.P. 37, preservation of Meta-Data, preservation of deleted ESI, back up or archival ESI, ESI contained in dynamic systems, ESI destroyed or overwritten by the routine operation of systems, and, offsite and offline ESI (including ESI stored on home or personal computers). This discussion should include whether the parties can agree on methods of review of ESI by the responding party in a manner that does not unacceptably change Meta-Data.

(1) If Counsel are able to agree, the terms of an agreed-upon preservation order may be submitted to the Court;
(2) If Counsel are unable to agree, they should attempt to reach agreement on the manner in which each party should submit a narrowly tailored, proposed preservation order to the Court for its consideration.

D. Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges in light of "claw back," "quick peek," or testing or sampling procedures, and submission of a proposed order pursuant to the holding of *Hopson v. Mayor and City Council of Baltimore,* 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. If Meta-Data is to be produced, Counsel may agree, and should discuss any agreement, that Meta-Data not be reviewed by the recipient and the terms of submission of a proposed order encompassing that agreement to the Court. Counsel should also discuss procedures under which ESI that contains privileged information or attorney work product should be immediately returned to the Producing Party if the ESI appears on its face to have been inadvertently produced or if there is prompt written notice of inadvertent production by the Producing Party. The Producing Party should maintain unaltered copies of all such returned materials under the control of Counsel of record. This provision is procedural and return of materials pursuant to this Protocol is without prejudice to any substantive right to assert, or oppose, waiver of any protection against disclosure.

E. Identification of ESI that is or is not reasonably accessible without undue burden or cost, specifically, and without limitation, the identity of such sources and the reasons for a contention that the ESI is or is not reasonably accessible without undue burden or cost, the methods of storing and retrieving that ESI, and the anticipated costs and efforts involved in retrieving that ESI. The party asserting that ESI is not reasonably accessible without undue burden or cost should be prepared to discuss in reasonable detail, the information described in Paragraph 10 of this Protocol.

F. Because identifying information may not be placed on ESI as easily as bates stamping, paper documents, methods of identifying pages or segments of ESI produced in discovery should be discussed, and, specifically, and without limitation, the following alternatives may be considered by the parties: electronically paginating Native File ESI pursuant to a stipulated agreement that the alteration does not affect admissibility; renaming Native Files using bates-type numbering systems, *e.g.,* ABC0001, ABC0002, ABC0003, with some method of referring to unnumbered "pages" within each file; using software that produces "hash marks" or "hash values" for each Native File; placing pagination on Static Images; or any other practicable method. The parties are encouraged to discuss the use of a digital notary for producing Native Files.

G. The method and manner of redacting information from ESI if only part of the ESI is discoverable. As set forth in Paragraph 11.D, if Meta-Data is redacted from a file, written notice of such redaction, and the scope of that redaction, should be provided.

H. The nature of information systems used by the party or person or entity served with a subpoena requesting ESI, including those systems described in Paragraph 7.D above. This Protocol may suggest that Counsel be prepared to list the types of information systems used by the client and the varying accessibility, if any, of each system. It may suggest that Counsel be prepared to identify the ESI custodians, for example, by name, title, and job responsibility. It also may suggest that, unless impracticable, Counsel be able to identify the software (including the version) used in the ordinary course of business to access the ESI, and the file formats of such ESI.

I. Specific facts related to the costs and burdens of preservation, retrieval, and use of ESI.

J. Cost sharing for the preservation, retrieval and/or production of ESI, including any discovery database, differentiating between ESI that is reasonably accessible and ESI that is not reasonably accessible; provided however that absent a contrary showing of good cause, *e.g.,* Fed.R.Civ.P. 26(b)(2)(C), the parties should generally presume that the Producing Party bears all costs as to reasonably accessible ESI and, provided further, the parties should generally presume that there will be cost sharing or cost shifting as to ESI that is not reasonably accessible. The parties may choose to discuss the use of an Application Service Provider that is capable of establishing a central repository of ESI for all parties.

K. Search methodologies for retrieving or reviewing ESI such as identification of the systems to be searched; identification of systems that will not be searched; restrictions or limitations on the search; factors that limit the ability to search; the use of key word searches, with an agreement on the words or terms to be searched; using sampling to search rather than searching all of the records; limitations on the time frame of ESI to be searched; limitations on the fields or document types to be searched; limitations regarding whether back up, archival, legacy or deleted ESI is to be searched; the number of hours that must be expended by the searching party or person in conducting the search and compiling and reviewing ESI; and the amount of preproduction review that is reasonable for the Producing Party to undertake in light of the considerations set forth in Fed.R.Civ.P. 26(b)(2)(C).

L. Preliminary depositions of information systems personnel, and limits on the scope of such depositions. Counsel should specifically consider whether limitations on the scope of such depositions should be submitted to the Court with a proposed order that, if entered, would permit Counsel to instruct a witness not to answer questions beyond the scope of the limitation, pursuant to Fed.R.Civ.P. 30(d)(1).

M. The need for two-tier or staged discovery of ESI, considering whether ESI initially can be produced in a manner that is more cost-effective, while reserving the right to request or to oppose additional more comprehensive production in a latter stage or stages. Absent agreement or good cause shown, discovery of ESI should proceed in the following sequence: 1) after receiving requests for production of ESI, the parties should search their ESI, other than that identified as not reasonably accessible without undue burden or cost, and produce responsive ESI within the parameters of Fed.R.Civ.P. 26(b)(2)(C); 2) searches of or for ESI identified as not reasonably accessible should not be conducted until the prior step has been completed; and, 3) requests for information expected to be found in or among ESI that was identified as not reasonably accessible should be narrowly focused, with a factual basis supporting each request.

N. The need for any protective orders or confidentiality orders, in conformance with the Local Rules and substantive principles governing such orders.

O. Any request for sampling or testing of ESI; the parameters of such requests; the time, manner, scope, and place limitations that will voluntarily or by Court order be placed on such processes; the persons to be involved; and the dispute resolution mechanism, if any, agreed-upon by the parties.

P. Any agreement concerning retention of an agreed-upon Court expert, retained at the cost of the parties, to assist in the resolution of technical issues presented by ESI.

PARTICIPANTS

The following people:

A. Should, absent good cause, participate in the Fed.R.Civ.P. 26(f) Conference of Parties: lead counsel and at least one representative of each party.

B. May participate in the Fed.R.Civ.P. 26(f) Conference of Parties: clients or representatives of clients or the entity served with a subpoena; the designated ESI coordinator for the party; forensic experts; and in-house information system personnel. Identification of an expert for use in a Fed.R.Civ.P. 26(f) Conference of Parties does not, in and of itself, identify that person as an expert whose opinions may be presented at trial within the meaning of Fed.R.Civ.P. 26(b)(4)(A, B).

C. If a party is not reasonably prepared for the Fed.R.Civ.P. 26(f) Conference of Parties in accordance with the terms of this Protocol, that factor may be used to support a motion for sanctions by the opposing party for the costs incurred in connection with that Conference.

REASONABLY ACCESSIBLE

No party should object to the discovery of ESI pursuant to Fed.R.Civ.P. 26(b)(2)(B) on the basis that it is not reasonably accessible because of undue burden or cost unless the objection has been stated with particularity, and not in conclusory or boilerplate language. Wherever the term "reasonably accessible" is used in this Protocol, the party asserting that ESI is not reasonably accessible should be prepared to specify facts that support its contention.

PRINCIPLES RE: META-DATA

The production of Meta-Data apart from its Native File may impose substantial costs, either in the extraction of such Meta-Data from the Native Files, or in its review for purposes of redacting non-discoverable information contained in such Meta-Data. The persons involved in the discovery process are expected to be cognizant of those costs in light of the various factors established in Fed.R.Civ.P. 26(b)(2)(C). The following principles should be utilized in determining whether Meta-Data may be discovered:

A. Meta-Data is part of ESI. Such Meta-Data, however, may not be relevant to the issues presented or, if relevant, not be reasonably subject to discovery given the Rule 26(b)(2)(C) cost-benefit factors. Therefore, it may be subject to cost-shifting under Fed.R.Civ.P. 26(b)(2)(C).

B. Meta-Data may generally be viewed as either System Meta-Data, Substantive Meta-Data, or Embedded Meta-Data. System Meta-Data is data that is automatically generated by a computer system. For example, System Meta-Data often includes information such as the author, date and time of creation, and the date a document was modified. Substantive Meta-Data is data that reflects the substantive changes made to the document by the user. For example, it may include the text of actual changes to a document. While no generalization is universally applicable, System Meta-Data is less likely to involve issues of work product and/or privilege.

C. Except as otherwise provided in sub-paragraph E, below, Meta-Data, especially substantive Meta-Data, need not be routinely produced, except upon agreement of the requesting and producing litigants, or upon a showing of good cause in a motion filed by the Requesting Party in accordance with the procedures set forth in the Local Rules of this Court. Consideration should be given to the production of System Meta-Data and its production is encouraged in instances where it will not unnecessarily or unreasonably increase costs or burdens. As set forth above, upon agreement of the parties, the Court will consider entry of an order approving an agreement that a party may produce Meta-Data in Native Files upon the representation of the recipient that the recipient will neither access nor review such data. This Protocol does not address the substantive issue of the duty to preserve such Meta-Data, the authenticity of such Meta-Data, or its admissibility into evidence or use in the course of depositions or other discovery.

D. If a Producing Party produces ESI without some or all of the Meta-Data that was contained in the ESI, the Producing Party should inform all other parties of this fact, in writing, at or before the time of production.

E. Some Native Files contain, in addition to Substantive Meta-Data and/or System Meta-Data, Embedded Meta-Data, which for purposes of this Protocol, means the text, numbers, content, data, or other information that is directly or indirectly inputted into a Native File by a user and which is not typically visible to the user viewing the output display of the Native File on screen or as a print out. Examples of Embedded Meta-Data include, but are not limited to, spreadsheet formulas (which display as the result of the formula operation), hidden columns, externally or internally linked files (*e.g.,* sound files in Powerpoint presentations), references to external files and content (*e.g.,* hyperlinks to HTML files or URLs), references and fields (*e.g.,* the field codes for an auto-numbered document), and certain database information if the data is part of a database (*e.g.,* a date field in a database will display as a formatted date, but its actual value is typically a long integer). Subject to the other provisions of this Protocol related to the costs and benefits of preserving and producing Meta-Data (see generally Paragraph 8), subject to potential redaction of Substantive Meta-Data, and subject to reducing the scope of production of Embedded Meta-Data, Embedded Meta-Data is generally discoverable and in appropriate cases, *see* Fed.R.Civ.P. 26(b)(2)(C), should be produced as a matter of course. If the parties determine to produce Embedded Meta-Data, either in connection with a Native File production or in connection with Static Image production in lieu of Native File production, the parties should normally discuss and agree on use of appropriate tools and methods to remove other Meta-Data, but preserve the Embedded Meta-Data, prior to such production.

APPENDIX H: AFFIDAVIT OF ENGINEER

JONES)
v.)
MHTC)

My name is Mike Engineer. I am the Maintenance Operations Engineer for the southern district of the Missouri Department of Transportation. The southern district includes highway T, in Newton County. I am of sound mind and capable of making this affidavit.

1. The activities of the Missouri Department of Transportation (MoDOT) involve the compilation and analysis of accident data with the goal of identifying and addressing problem locations, i.e. those locations with higher than typical accident rates, in order to evaluate the possible use of federal highway safety funding.

2. MoDoT collects and compiles accident and road condition information and reports, including but not limited to traffic accident detail reports, summaries and studies. Collection of raw data and analysis of this data constitute part of Missouri's response to the requirements of 23 U.S.C. Section 152 (a) (1) to "identify" hazardous locations and "assign priorities" for remediation. The data is used to identify and evaluate locations as well as to plan for safety enhancement of potential accident sites and hazardous roadway conditions. The data is also used to develop highway safety construction improvement projects which may be implemented by securing federal road safety funds to eliminate road hazards.

3. These activities are supported by federal funds.

4. I have reviewed the requests for production related to the case of Jones v. MHTC and others. Materials requested include those that are specifically gathered pursuant to the provisions of 23 U.S.C. Section 152 and 23 U.S.C. Section 409.

5. This data is used to evaluate Missouri's highways in order to determine how best to use the limited federal highway safety funds made available by Congress through the federal highway administration.

6. Federal funding is potentially available to the district for improvements to highway T in Newton County.

Further, affiant sayeth not.

Mike Engineer
Maintenance Operations Engineer

ACKNOWLEDGMENTS

This study was performed under the overall guidance of the NCHRP Project Committee SP 20-6. The Committee is chaired by MICHAEL E. TARDIF, Friemund, Jackson and Tardif, LLC. Members are RICHARD A. CHRISTOPHER, HDR Engineering; JOANN GEORGALLIS, California Department of Transportation; WILLIAM E. JAMES, Tennessee Attorney General's Office; PAMELA S. LESLIE, Miami-Dade Expressway Authority; THOMAS G. REEVES, Consultant; MARCELLE SATTIEWHITE JONES, Jacob, Carter and Burgess, Inc.; ROBERT J. SHEA, Pennsylvania Department of Transportation; JAY L. SMITH, Missouri Highway and Transportation Commission; JOHN W. STRAHAN; ROY M. TIPTON, Mississippi Department of Transportation; and THOMAS VIALL, Attorney, Vermont.

JO ANNE ROBINSON provided liaison with the Federal Highway Administration, and CRAWFORD F. JENCKS represents the NCHRP staff.

Transportation Research Board
500 Fifth Street, NW
Washington, DC 20001