STATE AND CONSUMER SERVICES AGENCY
DEPARTMENT OF GENERAL SERVICES

ELECTRONIC RECORDS MANAGEMENT HANDBOOK

State of California
Records Management Program

ELECTRONIC RECORDS MANAGEMENT HANDBOOK

State Records
Department of General Services
State of California

Published By

CalRIM

DGS CALIFORNIA
Records & Information Management

"Empowering Government with Solutions, Quality Products and Services"

California Records & Information Management
Sacramento, California
February 2002
Supersedes previous edition dated August 1995

PREFACE

The California Department of General Services (DGS), State Records, California Records and Information Management (CalRIM) is responsible for guidance of the State of California Records Management Program. The common goal is to ensure that state agencies acquire, manage, and use information resources economically and efficiently.

The Electronic Records Management Handbook is one of a series of initiatives on records and information management. This handbook is part of CalRIM's continuing effort to help state agencies improve their office systems and procedures.

The purpose of this Electronic Records Management Handbook is to provide guidance for managing electronic records and electronic recordskeeping systems for California State government to meet current and emerging record management responsibilities and the many challenges of e-government. It is not a regulation or manual, but focuses on methods and procedures, not equipment. The principles and techniques included, if followed, should increase electronic recordskeeping efficiency, effectiveness, and economy.

CalRIM revised this handbook by employing the Records Management Consulting Services provided by the DGS Procurement Division Master Services Agreement (MSA) Program, with additional information compiled by the CalRIM staff. The Secretary of State, State Archives staff and volunteer state agency members that comprised the Records Management Customer Council also contributed.

Information was also obtained from the Texas State Library, Records Management Division and the State of Oklahoma on Basic Guidelines for Disaster Planning. This handbook is based on Federal guidelines developed by the U. S. General Services Administration, Information Resources Management Service (IRMS). IRMS is responsible for developing government-wide policies and guidance for automatic data processing, records and telecommunications.

Please feel free to contact CalRIM (916) 375-4398 with any questions you may have concerning information in this handbook.

ELECTRONIC RECORDS MANAGEMENT

TABLE OF CONTENTS

INTRODUCTION

Electronic technology has greatly expanded the methods of creating, editing, maintaining, transmitting and retrieving information. Much of this electronic information is a record because it is used in state agencies to make decisions or affects citizens; therefore, it must be managed as a record. Though electronic information processing systems contain very important information, they do not perform electronic recordskeeping functions.

Electronic recordskeeping systems provide the functionality needed to enable California State government agencies and their records managers to adhere to certain standards and guidelines established by California statutes and regulations (i.e., the "State Records Management Act" under Sections 14740-14774 of the California Government Code; the State Administrative Manual, Chapter 1600, "Records Management;" and the "Specifications for Electronic Records Management Software"). That functionality, discussed in detail in the section on Electronic Recordskeeping, is based upon the need to effectively manage and control the record lifecycle and all documents constituting the record, regardless of format. Further, controlling the lifecycle of records requires knowledge of the retention assigned to the record or its components.

Records may now be found on a variety of media from creation to final disposition, making the task of properly accounting for the official record increasingly complicated. Therefore any approach to the management of records must incorporate accepted standards of functionality to adequately preserve the "official" record as certifiably authentic. The issue involving the authenticity of electronic records has, through the eighties and nineties, primarily revolved around the capability of the media to restrict changes in the original document. Now in the 21st Century, this has been greatly expanded to the more proper question concerning the document attributes and the overall system integrity to preserve and validate the record as authentic.

Electronic Information Processing System versus Electronic Recordskeeping System

It is important to distinguish the difference between an "*electronic information processing system*" and an "*electronic recordskeeping system.*" An example of an electronic information processing system would be an e-mail messaging system, whereas an electronic recordskeeping system is designed to not only manage e-mail reception, creation, identification, storage, accessibility, and integrity of the e-mail as records, but also the disposition of that e-mail through an electronically integrated records retention schedule. Many products claim to perform electronic records management or integrated document management, but they are not true electronic recordskeeping systems unless they meet the DGS "Specifications for Electronic Records Management Software."

Records management systems and methodologies must incorporate any appropriate documents into the records management plan. While some agencies may be unable to efficiently manage all aspects of the record immediately (e.g., e-mail), the records management plan should provide for a methodology and a schedule for achieving this vital goal.

Records Management Practices - General

In order to apply these practices to electronic information, you must first determine, as you would in the case of information preserved on paper, which electronic information is a "record" and which is a "non-record." As a result answering the question "what is a record?" becomes a pivotal step in determining which information should be a records management concern.

The glossary in this publication defines a record as: "all paper, maps, exhibits, magnetic or paper tapes, photographic films and prints, and other documents produced, received, owned or used by an agency, regardless of media, physical form or characteristics." Additional definitions are available in the glossary under PUBLIC RECORDS and STATE RECORDS.

You may consider the following records management guidelines:

- E-mail is a document created and transmitted as electronic information within an electronic communication medium. An e-mail message and associated information (metadata), is a document. It is also a record if it meets the recordskeeping criteria established within an organizations records management plan. That is, the fact that e-mail is the organization's property renders it subject to management under the records management plan, regardless of media.

- Voice mail is usually a non-record, unless preserved in a manner that would meet record criteria, as with other records, such as containing information necessary for that organization's business. Depending upon your requirements, you may consider managing a voice mail as a computer file, as voice communications and computer functionality continue to merge.

- Word processing files are records if they meet the criteria to be a record.

- One set of computer data containing accounting and tax information plus one copy of the visible output (e.g., printed report of computer output microfilm) are records under the Internal Revenue Service's Revenue Procedure 91-59.

- Computer back-up tapes and other duplicate computer files are non-records.

- Databases and other data compilations that are used for multiple purposes are often records. This is especially true when they are referred to by a record document that requires the information for understanding a stated policy, decision, etc.

- Electronic transactions are records.

Implementation of records management practices will depend on the needs of the organization.

When electronic information is deemed to meet the criteria of a "record," it must be managed according to sound records management practices and retained according to each organization's records retention schedule.

Electronic information that is deemed to be a "non-record" can be destroyed at the discretion of the user--generally, after a transitory period or after the official record is produced.

KEY DEFINITIONS

Electronic Record

Electronic records are informational or data files that are created and stored in digitized form through the use of computers and applications software. They are stored on various magnetic and optical storage devices and are products of computers and computer software. The format of an electronic document does not change the fact that it is a record, but its electronic form and its dependence on machines for creation and reference do change the way these records must be stored and managed.

As stated later in this handbook, the Uniform Electronic Transaction Act (UETA) defines electronic records as *"a record created, generated, sent, communicated, received, or stored by electronic means."* The UETA is an excellent reference to use as a guide when working with electronic records and covers the full spectrum of usage in electronic signatures relating to transactions. See Appendix 10 - Overview of the Uniform Electronic Transaction Act.

Usually, the definition applies to all electronic records systems, whether in microcomputers, minicomputers, or mainframe computers, regardless of storage media, in networked or stand-alone systems, including small computers, such as memory typewriters, calculators, and embedded systems. Examples include records stored on a server, or on magnetic media, such as tapes, disk packs, compact disks, or optical disks.

Electronic Records Management

Electronic records management, while involving special considerations, requires the planning, budgeting, organizing, directing, training, and controlling activities associated with managing the record in its entirety.

Electronic Recordskeeping

Electronic recordskeeping is the use of records management principles for records maintained electronically. This term is sometimes confused with "electronic recordskeeping system" which is described below.

Electronic Recordskeeping System (ERS)

An Electronic Recordskeeping System is primarily a software-based methodology used by an organization to manage all its records, regardless of format, over the entire record's lifecycle. Primary recordskeeping functions must include categorizing, locating, identifying and controlling record disposition requirements, including management of the storage, retrieval, and disposition of the records; regardless of the repository. This type of software includes the capabilities of both Integrated Document Management System (IDMS) and Records Information Management (RIM) software.

NOTE: Appendix 1 of this Handbook includes definitions of additional terms related to the management of electronic records. Throughout this Handbook the term "record" is used generally, unlike the specific computer science usage referring to a group of related data fields.

ELECTRONIC RECORDSKEEPING SYSTEMS AND PROGRAM REQUIREMENTS

All recordskeeping systems, whether paper, microform, or electronically based, should be cost effective, easy to use, provide the required information when needed, and retain the records for the required length of time.

Electronic recordskeeping systems are more vulnerable to undetected alteration, loss or unauthorized disclosure of information, than are hard copy or microform systems. This vulnerability suggests the need for comprehensive and detailed planning before electronic recordskeeping systems are implemented.

In addition, the maintenance of electronic records requires the careful management of procedures and equipment to ensure the continuing accuracy and availability of the records.

Use of electronic recordskeeping system software requires careful application of sound records management principles.

The Records Management Program Includes the Management of Electronic Records

State law requires the head of each state agency to ensure that a program for the management of electronic records is established which incorporates the necessary program elements, details are discussed below:

Program Elements

The program elements for managing electronic records are:

- Assigning the responsibility to develop and implement an agency-wide program for the management of all records, including electronic records.

- Integrating the management of electronic records with other records and information technology needs of the agency.

- Incorporating electronic records management objectives, responsibilities, and authorities in agency directives and/or guidelines and disseminating them throughout the agency as appropriate.

- Addressing records management requirements before approving new electronic records systems or enhancements to existing systems.

- Providing adequate training for users of electronic records systems in the operation, care, and handling of the equipment, software, and media used in the system and in the management of electronic records.

- Developing and maintaining up-to-date information about all electronic records systems.

- Inventorying of agency records including all electronic records, and keeping this inventory updated.

- Identifying and protecting vital records, selecting appropriate media and appraising agency records to develop the agency records retention schedule.

- Securing approval of the records retention schedule and ensuring its implementation for use in the management and disposition of records.

Management Responsibility

Although stated in other State of California Records Management Program directives, it is still important to note that each agency is required to have a Records Management Analyst and/or Manager (and an assistant or back-up). In keeping with California State law, the appointment is made by the head of the agency, in writing. Announcement of this appointment should be disseminated throughout the agency so all are aware of this individual's position, role and responsibility regarding the agency-wide records management program.

This trained and knowledgeable person acts as a liaison for the State's Records Management Program, the California State Archives, and the respective agency. Their role is to manage and/or coordinate the records activity of the agency. The main functions involved and supported by state agency's "Executive Management" in this critical responsibility are listed here and discussed in detail in this Handbook.

The agency Records Management Analyst and/or Manager:

- Administers the records management program within the agency.
- Conducts or oversees the inventory of all agency records as required.
- Conducts or oversees the preparation and maintenance of the agency records retention schedule program.
- Ensures adherence to the agency records retention schedules.
- Approves all documentation for transfer of records to the State Records Center and the California State Archives.
- Originates and/or approves all requests to dispose of state records or to transfer records to the California State Archives as designated by an approved records retention schedule.
- Attends training and information classes offered by the Records Management Program.
- Distributes the training schedule and registration information and/or conducts training for the Records Management Program classes to agency staff.

The effective discharging of the above responsibilities and functions of the agency are critical to ensure statutory compliance. It ensures that the agency establishes and maintains an active, continuing program for the economical and efficient management of all records and information collection practices, regardless of the media.

INFORMATION TECHNOLOGY AND RECORDSKEEPING PRINCIPLES

The Department of Information Technology (DOIT)

“Information technology” in California State government gained national attention and prominence when the legislature passed landmark legislation, which the Governor signed into law in October 1995, creating the Department of Information Technology (DOIT). DOIT was charged with providing leadership, guidance, and oversight to ensure successful delivery of information technology and to enhance delivery of California State government services.

The law gave DOIT the authority to provide guidance to state agencies regarding acquisition management and appropriate use of information technology. DOIT also provides guidance to all state entities to ensure that the agency’s information technology direction is consistent with the agency’s mission, business plan, and has a result-oriented management policy; that promotes reforms in information technology personnel classification. DOIT also ensures that the agency has systems and procedures that reward skill in meeting business needs and facilitation of change with effective application of information technology.

Understanding Information Technology

"Information technology" means all computerized and automated information handling, including systems design and analysis, conversion of data, computer programming, information storage and retrieval, voice, video and data communications, system controls, simulation, and all related interactions between people and machines.

Management of information technology is the proven planning, budgeting, organizing, directing, training, evaluating and other control activities associated with information technology applications. This includes procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information. This would also include associated personnel, consultants and contractors.

The Relationship of Information Technology to Records Management

Information technology must be managed as an important asset. Consistent with this principle, information technology is an indispensable tool of modern government that each state agency is expected to use and seek opportunities that will increase the quality of the services it provides and to reduce the overall costs of government.

Records management in California State government on the other hand provides the procedural infrastructure that ensures information is available, preserved, and when appropriate, destroyed. Records management evaluates information in all media based on legal, regulatory, operational and historic factors. By recognizing that all information is not equal, the records and information management program assigns cradle-to-grave handling instructions that include who keeps what, for how long, at what location (including cyberspace), in what form and format.

Records management programs demonstrate a systematic approach and provide the formality that is favored by the courts. Just as important, records management evaluates categories of information assets. Items with long-term reference value should remain accessible (and legible) for the duration.

More than media longevity, the issue is technology obsolescence: What operating system version will be used 10 years from now? Will it provide a means to glean the knowledge and insights found in reports created today? Or will today's electronic files be tomorrow's punch cards? Records management's dictum of *"the right information, at the right time, to the right people, in the right form"* attests to the long-term view.

This is the essential difference between records management and information technology. While dense storage at declining costs seem to encourage keeping everything forever, prudent records management counsels that the enterprise keep only what is required, and assure that any new system has mechanisms in place to purge the superfluous when it is time.

Finally, in California State government, the agency Records Management Manager is usually not the same person named as the agency Chief Information Officer and/or the systems technology manager. They must, however work together to coordinate and ensure that records management provides the procedural infrastructure that ensures information is available, preserved and, when appropriate, destroyed, and that electronic recordskeeping requirements are met.

AGENCY DIRECTIVES

Incorporating Electronic Records Management

Managers and staff must be aware of their recordskeeping responsibilities. Managers of state programs utilizing electronic records have the responsibility for instructing employees in the creation, use and disposition of electronic records and for ensuring that such procedures are followed and reflected in appropriate directives.

Some organizations permit each user of electronic equipment to operate independently with no established policies or standardized procedures. This tendency has fewer serious consequences in small organizations, but in larger operations this will result in chaos.

Procedures are necessary because valuable records can be lost, changed, or destroyed; and the electronic recording medium can be inadvertently erased or overwritten. Along with these hazards, there is the distinct possibility of unauthorized access to sensitive or confidential information in electronic files.

Individuals using electronic recordskeeping equipment to create, retrieve, edit, store, transmit, and dispose of electronic records are responsible for correctly using the equipment, managing the records according to prescribed procedures, and seeking assistance whenever they have questions concerning the management of electronic records.

THE RECORDS MANAGEMENT REVIEW & PLAN

Review and Evaluation of Requirements

Before approving any electronic recordskeeping system or information processing system, the Records Management Analyst and/or Manager, information systems and technology managers and other agency managers should evaluate how effectively and efficiently information is stored and retrieved using present equipment, networks, and software. They should study future requirements and recommend new systems as appropriate. Certain factors should be considered before upgrading or implementing new systems. These factors are practicality, the cost, and the effectiveness of new configurations.

The Records Management Plan

Most important, is the development of a Records Management Plan. This plan should be sufficiently detailed so as to provide a thorough file classification scheme for the entire organization. The classification scheme should anticipate supporting the possible employment of an electronic recordskeeping system that can incorporate the classification scheme as the core of its recordskeeping management functions. That is, all activities relate to the classification scheme which, in turn, ensures proper final disposition. Finally, the Records Management Plan must be incorporated into the organization's strategic and disaster recovery plans.

The Records Management Program provides general consulting in a broad range of topics involving records and workflow studies, Feasibility Study Reports (FSR), records conversion (microform and electronic), and the implementation of electronic recordskeeping and office automation.

NOTE: See Appendix 3, "Checklist of Pre-Purchase Considerations and Reviews for Electronic Records Systems" in the Appendices section of the Handbook for general questions to be examined during the review process, including the DGS "Specifications for Electronic Records Management Software."

TRAINING

Providing adequate training for users of electronic recordskeeping systems in the operation, care, and handling of the equipment, software, and media used in the system and in the management of electronic records is the responsibility of the agency records manager and the State's Records Management Program.

Training for individuals who create, edit, store, retrieve or dispose of records is an important aspect of electronic records management. Training enables agency personnel to identify records, and to understand how records are filed in an electronic recordskeeping system, how records are safeguarded, what procedures are used to edit records, and how records should be disposed of according to legal requirements. Methods of providing training for the management of electronic records include one or more of the following:

- Contact the State's Records Management Program for scheduled classes. Formal classroom training is presented several times a year on a recurring basis or as needed for special situations.

- A self-learning center within the agency, where operators can teach themselves at their own rate of learning through interactive programs. As a rule, commercial tutorial programs do not include records management information. Consequently, records management concepts should be developed and offered by the agency.

- Telephone "hotlines" or "help desk" staffed by knowledgeable computer support professionals, who can answer technical questions and provide "quick fix "solutions. This process may not be an adequate learning tool for good records management unless the computer support professionals have received specialized records management training.

- Attend specialized training offered by ARMA, AIIM and other professional organizations.

- Training offered by the manufacturer or supplier. This usually covers the operation of the equipment, but does not normally include the principles of records management.

DOCUMENTATION OF EXISTING ELECTRONIC RECORDS SYSTEMS

Developing and maintaining up-to-date documentation about all electronic records systems is the role and responsibility of the agency records management analyst and /or records manager. Documentation is a written record detailing the design, functions and operating procedures for a computer system. Adequate documentation by the records management analyst and/or records manager will:

- Specify all technical characteristics necessary to read and process the files.

- Identify all defined inputs and outputs of the system.

- Define the contents of the files and records.

- Determine restrictions on access and use.

- Provide an understanding of the purpose(s) and function(s) of the system and its records.

- Describe update cycles or conditions and rules for adding, modifying, or deleting information.

- Ensure the timely, authorized disposition of records.

- Ensure efficient and timely migration of data.

RECORDS INVENTORY

The Importance of the Inventory and Database Uses

To establish a records retention program, it is necessary to complete an inventory of all agency records, including electronic records, and keep it current. It is important to find out what records there are, where they are stored, their quantity, and how they are used. The Records Retention Handbook published by CalRIM describes in detail the process for completing an inventory.

The sample STD Form 70, Records Inventory Worksheet, included in Appendix 7 of this Handbook, can be used to gather information on records series in all formats (see the records inventory section of the Records Retention Handbook for discussion of the item numbers on the Records Inventory Worksheet).

Item 4 of the Records Inventory Worksheet is designed to list the record medium of a records series. Electronic records may be maintained on magnetic storage media (magnetic tapes, cartridges, compact disks, and diskettes), on-line, or on optical disks. The record copy of information processed on the computer may also be in the form of data processing printouts or computer output microfilm.

With a mainframe or other computers operation, there may be databases that have multiple outputs. The outputs may create several records series because they are produced for separate divisions, the data is summarized differently, and the retention periods may vary because of specialized use.

For example, an agency may have an automated database for client information. One division uses it to do research and prepare administrative reports, which are maintained for three years, then reviewed for archival value by the California State Archives. Another division uses the same database for case management computer printouts, which are maintained for five years to meet federal reporting regulations. As records are inventoried in each division, each of these records series would be documented on an inventory worksheet.

There could also be a situation in which a database is created for one function. For example, a database of fiscal information may generate several reports, but if they all have the same use and the same retention period, they can be grouped as one records series: Fiscal Internal Management Reports.

NOTE: You can develop a specialized inventory worksheet for automated information systems, which contains additional information useful for the data processing operation. For more information about this subject contact the Records Management Program for guidance.

APPRAISING RECORDS

Developing the Records Retention Schedule from the Appraisal Process

Appraisal is the process of determining the value and thus the retention or disposition of records based upon their administrative and other uses, the evidentiary and informational or research value and their arrangement and relationship to other records. Appraisal uses the information gathered during the inventory to analyze records series and develop an official records retention schedule(s).

The first step in determining recordskeeping requirements for electronic records is to identify the records creators and users. In doing so, it is important to remember individuals and offices within an organization who may use records for different purposes. Some records may exist in several formats within one office. If such records are needed for separate program purposes, the recordskeeping requirements may differ with the program. Such requirements, as determined during the records inventory, will be significant factors in deciding where; in what format, and for how long the electronic records are maintained. Records appraisal guidelines are further discussed in the Records Retention Handbook.

In addition to the information gathered during the records inventory, the following General Retention Schedules and their retention periods are listed on the DGS Procurement Website at www.dgs.ca.gov/pd. These General Retention Schedules are a primary resource for agencies to use during the records appraisal process:

- Personnel and Payroll Records
- Delegated Testing
- Fiscal Records
- Records Management Records and Related Documents
- Administrative and Common Use Records

Records series in electronic format may also be classified in other categories. For example, the records series "Support Services Records" is the appropriate classification for "mailing lists". The retention period for mailing lists is "Current Until Revised, Superseded or Rescinded." This classification and retention period are applicable to all mailing lists, whether the record copy is maintained electronically or on paper. The primary consideration in classifying a records series is its function, not its format and/or media type.

Appraising Electronic Records for Records Management Purposes Includes Identifying the Record Copy Versus Working Document or Convenience Copy

Drafts or working documents are normally kept only until the final version of a document is completed. For long or complex documents, several earlier drafts and the current draft may be retained to ensure document integrity until the final draft is approved. Previous revisions are then erased, and only the final text is kept.

However, a draft version containing information not included in the final version, but useful for preparing similar documents in the future, could be retained as a reference copy.

Often a document maintained in electronic format is a convenience copy; the record copy is in the form of paper, computer printout or computer output microfilm. For example, copies of correspondence may be kept on personal computers for the convenience of copying part of the content for the next letter, or information in an automated database may be maintained as the record copy in computer printout.

If the only copy of the information is in electronic format, then it is the record copy. If the official copy was in another format that has been destroyed and the electronic information has not been destroyed, then the electronic file becomes the record copy by default.

NOTE: Convenience copies of documents should be kept only as long as needed to meet the purpose for which they were created, and no longer than the record copy. This requires knowledge of where the record copy is being maintained in the agency and procedures to inform staff on the proper disposition of records. Unmanaged duplicates or convenience copies also pose a serious risk of litigation to an agency.

Appraisal decisions on the retention of the record copy include:

- Total retention period each records series will be maintained based on administrative, fiscal, legal, and research, historical or archival values.

- Length of time a records series will have current, active use in the agency.

- Length of time a records series should be stored if there is a period of inactive use prior to final disposition.

- Appropriate format for a records series while it has current use and during any inactive storage.

- Potential archival value of a records series.

- Identification of confidential or private information.

- Identification of vital (essential) records.

Electronic records are directly impacted by their organization and the integrity of the records. During the appraisal process, any special concerns for electronic records should be addressed. For example, plans for records in electronic format that have potential archival value should be discussed with the staff of the Chief, State Archives and Museum Division, Office of the Secretary of State.

California State Archives accepts all records, regardless of the media. When records having historical value, as noted by the archivist on the retention schedule, are no longer needed for the current business of the agency, they will be made available to the California State Archives.

APPROVAL OF THE RECORDS RETENTION SCHEDULE

All records, regardless of their format must be inventoried and scheduled per the State Records Management Act. Electronic Records are records that are machine-readable, as opposed to human readable. They must be accounted for in the same manner as their paper counterpart.

The State Administrative Manual, Chapter 1600, Records Management, the Records Retention Handbook and Records Retention Schedule Guidelines explain the statutory requirements, procedures, and process for developing, submitting, approving, and updating the records retention schedule.

Use of the STD Form 73, Records Retention Schedule (or a computer-generated facsimile of the form approved by the Forms Management Center) is required for all state agencies. When preparing the STD Form 73 for electronic records, you must enter the format and version, i.e., Word 6.0 in the "Remarks" section of the STD Form 73. STD Form 72, Records Retention Schedule Approval Request, which documents final approval, along with the STD Form 73 must also be prepared and submitted to the Records Management Program in triplicate.

The records retention schedule is reviewed and approved by the Records Management Program. Subsequently, the California State Archives reviews the schedule and "flags" archival interest. The approved retention schedule then becomes the agency's *"official basis for management and final disposition of the records series listed."*

NOTE: Convenience copies of records series do not have to be listed on the STD Form 73 since it is not necessary for them to be maintained the full length of the retention period. For example, if the record copy of "administrative correspondence" is listed on the records retention schedule as paper and there is also a convenience copy on the computer, the electronic copy does not have to be shown. However, convenience copies should be destroyed as soon as they are no longer needed.

CREATING ELECTRONIC RECORDS

When electronic records are created as documents on computers or as data files in a database management system, records management principles must be applied to provide appropriate and effective recordskeeping practices that ensure statutory compliance.

ORGANIZING COMPUTER FILES

In the absence of an electronic recordskeeping system, the usefulness of electronic records, the accessibility of electronic document files for use as needed by the agency and the efficient management of records in electronic format will be enhanced by:

- Grouping files into records series.
- Arranging files in a logical order.
- Standardizing filenames.

RECORDS SERIES GROUPS

Electronic files are created on a computer's hard drive, or on a networked hard drive, which holds large numbers of computer files just as a file cabinet holds large numbers of paper files. Paper files are organized into records series. A records series is a group of identical or related records that are normally used and filed as a unit and are evaluated as a unit for retention scheduling purposes.

This records series concept also applies to electronic records on the computer. Paper files are arranged by records series in file cabinets which have drawers and file folders. Similarly, electronic files should be arranged into records series on the computer. The organization of files is accomplished by using tree-structured directories in which major groupings of files are given a name (the directory) and sub-groupings in directories are given names (sub-directories).

The result is a hierarchical organization of information that allows files to be grouped according to function. The idea is that those files with similar uses can be organized together, while ones with entirely separate purposes can be placed in different directory structures or paths.

NOTE: The primary advantage of a system using a tree-structured directory is that searches and retrievals can be made from a specific directory or subdirectory rather than having to access all of the files for every operation.

Careful consideration is needed in the grouping of records and in the selection of a title, which appropriately describes the function of the records series. If the electronic files are convenience copies, the records series titles should be the same as those used on the retention schedule for the record copy in order to facilitate appropriate disposition.
The alternative to hierarchical organization is usage of an electronic recordskeeping system, together with a records management plan. These two items will provide the functionality necessary to manage all the records (including the computer files) placed under the system's control.

ARRANGING ELECTRONIC FILES

Evaluate the Adequacy of the Current Classification Systems

While completing the records inventory, a discussion and evaluation of the the adequacy and appropriateness of the current classification scheme (groupings of records) is necessary. In anticipation of related physical files, the classification scheme should be to incorporate information about the location and disposition of specific physical documents. For example, a physical record within the classification (i.e., personnel records) might be linked to an electronic document (i.e., e-mail) that should be accessible within that overall scheme. The main idea is to develop a system that is workable yet maintains record integrity.

As to indexing, consider developing a straight numeric system. Also consideration may be given to subject, geographic, chronological, or combination systems. Because each filing system has certain advantages and limitations, selection of the appropriate system should also be based on characteristics of the agency's records practices and software limitations.

NOTE: To make usage easier the filing of electronic records should be coordinated and compatible with the filing system for paper and/or microfilm records. In any organizational unit there must be cooperation in the use of common assets, and electronic information is a critical asset.

STANDARD TECHNOLOGY

There are many benefits to standardizing the terminology used in naming electronic files:

- Accessing files easily and rapidly.
- Training new employees in less time.
- Avoiding the loss of information.
- Naming files quickly and easily.
- Sharing files more easily.
- Identifying groups of files eligible for disposition at the same time.

ELECTRONIC RECORDS INTEGRITY

Various functions of software applications may affect the status and integrity of records created on a computer. Saving the file currently being created is one of these functions.
A new record must be saved on the proper medium, or it will be lost when you turn off your computer or quit the application.

Copying and Erasing Files Has a Direct Impact on Electronic Record Integrity

Most computer file-copying functions have a potential problem with direct impact on record integrity. It is important for computer users to keep in mind that they may be creating, manipulating, and deleting official state records. (The authorized process for final disposition of records, including recommendations for disposing of electronic records on magnetic media, is discussed in the section entitled Final Disposition of Records.)

If the user does not want to change the previous version, the file can be renamed or copied to a variety of alternative media so that multiple versions of the file are then available. Be sure to clearly identify the version so you can locate the most current version. Relying only on the internal computer generated creation date is not sufficient.

A problem in file management can arise when the copy procedure accidentally occurs in the wrong direction. If a user makes a backup copy onto a removable medium (such as a diskette) and then loads the backup copy from the diskette onto the hard disk, the preceding version of the file may replace the current file. Software functionality allows for creation of multiple versions.

Files that have been erased by individual record attribute (a specific identifiable document within the record) preserve records integrity. The user clearly intended to erase that individual file within a defined records management methodology and records retention policy. Users should be certain that the recordskeeping methodology is capable of assuring that the document has been permanently removed from the system. Otherwise, a liability may ensue if in the course of legal discovery, documents that would have otherwise been destroyed are inadvertently available because of poor records management. It is therefore important for agencies to follow appropriate procedures for disposing of electronic records as a part of their records management plan.

For these and other reasons, agencies should ensure that their electronic records are being properly managed by a fully functional electronic recordskeeping system that meets the specifications established by the DGS.

DATABASE MANAGEMENT

The records management analyst and/or records manager and the information and/or systems technology manager, have specific and important roles and responsibilities dealing with database management. The records management analyst and/or records manager is concerned with the creation, management and disposition of records generated by databases, while the systems technology manager is involved with its creation, design, and management.

Creating records on a computer is one way of electronic filing. Another type of electronic filing system is database management. A database is a collection of data that forms the basis of an activity or step within a business process. The two elements essential to a database are coherence and organization. Coherence means the data are related to a specific activity or purpose. Organization means the data are related in such a way that users can meaningfully access parts of the database.

Methods Used to Arrange Records Within a Database

- **Hierarchical databases** are tree-structured. That is, their logic goes from the broader meaning to a narrower meaning through one or several steps. Each step branches out into smaller units, and with each step, other options are eliminated. It is a process of "narrowing the field" to the desired item. Although this structure simplifies searching, it is not particularly well suited for extensive lists of information.

- **Relational databases** allow data to be accessed based on relationships among several data base files. This means that within a predetermined set of data fields and their relationships, you can retrieve specific information through one command.

- **Network databases** permit data to be arranged into groupings that can be connected through the use of pointers. These pointers give users a great deal of flexibility and speed in searching for data, although the pointer structure is relatively complex to establish.

Database Management Programs Also Access Information

To retrieve selected electronic records, software applications usually search for data in one of two basic ways:

- Key fields in a database management system.

- Hierarchies of words or phrases in a full text retrieval system.

In the key fields method, specific data fields--such as social security numbers or titles of documents--are chosen in advance. When loading data into the system, the software builds key tables/files that contain cross-references to where the corresponding data are located on the storage medium. On receiving a request for a specific set of data, the software compares the request with the data contained in the key tables to determine if there are matches.

The full text retrieval method indexes all words, with the usual exception of such common words as "and," "the," and "of" to permit flexible and detailed searching of the data. The full text method involves searching the whole contents of documents to find what the user wants.

The best form of organization for a database depends on the content and how the information is to be used. The choice of organization is made during the database design.

Database Design

Database design, much as a filing system design, entails the planning of interrelated records. It should start with an analysis of the users' needs and application requirements, and should consider the medium, unit definition, logic, indexing, and retrieval criteria. The selection, design, or adaptation of software is also part of the database design process.

Analysis and design of a database system is a complex process. A project team should be formed to work on the system. The project team should consist minimally of a project manager, technicians, a records management analyst and/or manager, and records users.

Although some help and advice may be available from suppliers, the ultimate responsibility for the design and implementation of the system rests with the individuals planning the records system.

Advantages and Limitations of Database Management

Information may be stored in databases that contain either elements of data or entire documents stored in digital form. Significant potential advantages of database management systems for records management include:

- Faster access to information.

- Centralization of information.

- Flexibility of information retrieval.
- Reduction in miss-filing.

Some limitations of database management systems are:

- Cost of developing the databases.

- Cost of the necessary equipment and software.

- Need for additional expertise to administer and operate the electronic system.

- Cost of maintaining duplicate systems (in many situations) when electronic files, because of legal or historical requirements, cannot replace paper or microform documents.

Legal Guidance

Crown Life Insurance Company v. Craig established that databases need to be handled as records. In a dispute between insurance companies, Crown Life was severely sanctioned by a lower court for failing to produce "raw data." One of its employees had testified as to the existence of a database containing important policy information. Craig argued that the documents furnished by the company were insufficient and that they needed access to the raw data. Crown Life argued that the data was not a document (record in this meaning) for discovery since it had never been put into hard copy and that the discovery request did not specifically ask for the data.

The Federal court held that the notes to the 1970 amendment of Federal Rule of Civil Procedure 34 made clear that computer data is included in the description of documents. The court further held that the request for documents included any "underlying data" used to support or refute the documents and that Crown Life had a duty to make that data accessible.

HARDWARE AND DATA SECURITY

Security for the electronic records created, used, and stored on computer systems is an important issue and a responsibility of the Records Management Coordinators in addition to the Information Technology Managers. The protection of records in whatever format is to be identified on the RRS. This is even more relevant if the data is personal or confidential. Mainframe computer systems have traditionally been protected, but other computers have not because they are frequently considered single-user devices.

As a result, security weaknesses may threaten the confidentiality, integrity, or availability of electronic information. There are two major means of protecting electronic records:

- Physical security of the computer hardware.

- Securing data through controlling access.

Data Concerns

A good security system for protecting electronic data will employ a number of different products, services, and resources, which are customized to an agency's particular needs. Not every system or device is appropriate for all agencies. Those responsible for implementing security systems must weigh the potential costs of suffering a loss. Then, consider the value of each method and develop a complete security system that is tailored for the situation. In order to be successful, computer security has to be an on-going management concern.

NOTE: For information on "Common Methods of Computer and Data Security That Can Be Employed to Customize a Security System" please see Appendix 3 of this Handbook.

Environmental Considerations

The effects of environmental conditions, e.g., humidity, temperature, and cleanliness--on electronic recordskeeping and information processing system components are a security concern because of the potential loss or alteration of records maintained electronically.

A large-scale recordskeeping and information processing operation maintaining great numbers of sensitive records on a large computer will require extensive environmental controls.

A smaller scale, noncritical system operating on a computer will probably involve fewer environmental considerations. However, small systems with sensitive electronic equipment require at least a minimum level of environmental control to operate reliably.

NOTE: Appendix 4 of this Handbook includes the "Environmental Checklist for Establishing an Electronic Recordskeeping System," which should be consulted for routine environmental factors to be considered.

DISASTER PREPAREDNESS AND RECOVERY

Aside from the routine management of electronic records, attention should be given to preparing for disasters. The Emergency Plan of the State of California directs all levels of government to identify, organize and protect their essential and/or vital records. As such, agencies need to develop plans for coping with emergency situations, from minor disruptions to major disasters, to ensure the continued operation of electronic recordskeeping and information processing systems. The records management plan should include disaster preparedness and recovery needs and incorporate this specific plan as a component of the overall records management plan. Contact CalRIM to obtain a copy of the Vital Records Protection and Disaster Recovery handbook for further guidelines.

Disaster recovery planning anticipates how various disasters could threaten records integrity and availability. For example:

- How likely is a disaster to happen?

- What can be done if a disaster does happen?

- What can be done to lessen the impact?

- What can be done to protect records and prepare for recovery in the event of a disaster?

- Consider using project management methodologies to assess and plan to manage risks. Additional information is available on-line from the Project Management Institute at www.pmi.org.

Assessment of Emergency Situations

Emergencies can range from a temporary disruption of power to complete destruction of an office and its occupants. No contingency plan will provide options for all types of emergencies. Planners must determine which of the types of emergencies are most likely to disrupt their operations, and gear emergency response procedures and recovery planning to expected situations.

Not every emergency can be classified as a disaster, but personnel prepared for a disaster can successfully cope with lesser emergencies.

Commonly, four levels of disruption define the severity of an emergency:

- **Limited**. A temporary interruption with no damage or loss can be classified at this level. Examples would be a power failure or fluctuation, a communications failure, evacuation of a site because of a threat, or the unavailability of key personnel.

- **Serious**. Repairable damage to equipment or the office area or replaceable loss of key people, data, records, or software could be considered a serious disruption. Examples would be an equipment breakdown, a failure of the air-conditioning system, or minor damage because of sabotage, vandalism, or human error.

- **Major**. Destruction of equipment or office area or of data can be classified as a major disruption. Examples would be a complete loss of equipment because of water damage, explosion, or structural mishap, or an accidental or deliberate loss of data.

- **Catastrophic**. This category includes the total loss of office area or equipment, data, or people. An example would be the complete destruction of the office and the loss of personnel because of fire or a natural disaster.

Disaster Recovery

Contingency plans must be broad enough in scope to cope successfully with the immediate emergency, provide interim service, and bring the electronic recordskeeping and information processing functions back to normal. Because an organization must respond quickly to a disaster, recovery procedures must be spelled out clearly.

The individuals most likely to execute an emergency plan are the ones who develop it. Developers must consider the possibility that assigned office workers may be incapacitated and unable to function following a disaster. Therefore, the plan should be written so that others less familiar with the office will have the information they need to continue operations.

Disasters resulting in severe damage to an office and its equipment may be required to assume operations at an alternate location until repairs are completed and services are restored.

Planned Backup of Electronic Records

With or without an Electronic Recordskeeping System, agencies will need to ensure that the records have been protected from disaster. Part of the disaster recovery plan will be the planned backup of agency electronic records. Several methods for providing backup are of use for different levels of data protection.

The most important factor in a backup program is to do it regularly.

"How often should I do a backup?" is a common question. The answer is a subjective one, but it can be safely said that the interval between backups is the amount of work you are willing to do over. A rule of thumb in general usage is every eight hours. Backup systems and methodologies vary, but most perform the backup programmatically (automatically) at prescribed times. So, if the computer is used all day long, then backup at least daily. If eight hours of data creation are done in a week, then back up weekly, and so on.

When users share a computer, they should be encouraged to back up their files more often, preferably after every update.

Almost as important as regular backups is labeling backup media accurately so that the following information is available for system restoration:

- Name of the organizational unit responsible for the records.

- Descriptive title of the contents.

- Dates of creation.

- Confidentiality and release information.

- Identification of the software and hardware used.

To be accessible in case of disaster, backup media must be stored in a carefully planned manner. Not only must records be backed up and stored, but agencies must also have copies of current versions of application software for essential systems and up-to-date operations manuals, system documentation, program documentation, and operating system tapes or disks.

A typical backup would consist of establishing three versions of data: the previous generation of data, the active data and a copy of the active data. Backup media should be stored off-site.

While backups provide for records protection, they do not necessarily provide for quick recovery and knowledge concerning records disposition. Electronic Recordskeeping Systems best provide for recovery and disposition.

Steps for Salvaging Damaged Records

If the circumstances require the salvaging of water-damaged electronic media, they should not be used until thoroughly cleaned and dried. This will avoid damage to equipment, especially disk drives.

Magnetic tapes, which have become wet, have a good chance for information recovery. Hand dry all external surfaces with a soft, lint-proof cloth and air-dry the tape using a tape cleaner or winder to run the tapes from reel-to-reel. A company specializing in magnetic tape restoration should be consulted.

Drain and blot floppy diskettes with soft, lint-proof cloth. Peel the jacket away from diskette and rinse the diskette with distilled water. Drain the diskette and place flat; blot and air-dry approximately eight hours. When the disk is dry, insert it into new jacket and copy the data to new diskette and/or other storage device (DVD, CD ROM, Optical disk, hard drive, etc). If the information is copied properly, discard the damaged diskette. Clean copy equipment drive heads to prevent permanent damage.

Disaster Recovery Plan

Refer to the sample format of a "Records Management Disaster Recovery Plan" in Appendix 8 of this Handbook. Please note, it is important to adapt the detailed content of each developed plan section to suit the needs of the individual agency.

State Records Center Disaster Services

The State Records Center is available for disaster recovery storage and vital records services to state agencies. Electronic backups can be delivered by an agency, as often as daily and stored at the State Records Center. Please note there is no specifically designed vault available for magnetic media. Contact the State Records Center for additional information.

CARE OF STORAGE MEDIA AND TRANSMISSION SYSTEMS

How electronic records should be stored depends on their use. The maintenance of electronic records is similar to paper records. Current records are actively used in the office for the day-to-day operations of the agency. There may also be a period of less activity when storage is needed.

There are many types of storage media for electronic records: magnetic media, optical disks, CD-ROM, and DVD. Magnetic media, commonly used for storage of state records, include hard disks, diskettes (floppy disks), and magnetic tape (cartridges). The Media Standards, Appendix 11 of this Handbook, lists recognized standards for various media.

Migration

Migration is a strategy for avoiding the obsolescence of media that is used as a repository for records and/or specific file types (i.e., MS Word "doc"). The media type can become obsolete and current software will not work with it. A migration program needs to put into practice that will insure that files are moved to a current format, preserving the content. This must be done before the media type becomes obsolete. Therefore, electronic records should be periodically migrated to stable media and stable file types within an organization's overall records management plan.

Media and file types must provide a reliable and stable repository for the authentic record to be preserved and accessible by using current equipment, methods and/or technology, consistent with the DGS "Specifications for Electronic Record Management Software."

Because media and file types vary widely, a migration strategy should establish a schedule for each media and file type individually, e.g., WordPerfect files might require review and migration to current word-processing software within four years from the date created.

Records management best practices provide that records migration is ultimately justified, even if some of the attributes of a record do not lend themselves well to the migration process, in the preservation of content and utility. The records management methodology implemented and employed in the life cycle of records ensures the security, protection, preservation, and future accessibility of information.

Migration of records is essential to guaranteeing long-term access and the preservation of valuable records. To insure that records can be migrated, records management best practices encourage the use of open systems, standard-compliant technology, and wise budgeting that accounts for training and technology upgrades, selection of dependable software, and sound management of the system.

In California State government, the Secretary of State, California State Archives must in part, rely upon the best practices of the records manager. If the records manager fails to properly maintain records, the archivist's role in the preservation of the record is compromised. If records are earmarked by the Secretary of State (via approved records retention schedules) have been migrated to a different media and/or file type, and the old media containing the records is no longer needed, the media and its contents should be made available to the California State Archives. Absolutely no such media should be destroyed without the approval of the State Archivist.

Hard Disk Maintenance

Hard disks offer on-line, immediate access to electronic records. A hard disk's advantage over a diskette is its speed and storage capacity. While similar to a floppy disk in magnetic surface, hard disks are solid. As a result, hard disks can spin much faster than diskettes. Hard disks reach speeds of 7200 revolutions per minute (rpm) and higher compared to about 300 rpm for a floppy disk.

The hard disk is more sensitive than a diskette. The smallest pieces of dust or smoke can damage the disk. Data may also be lost if a computer is subject to rough handling. This is because information is recorded to and from the hard disk by the disk drive's read/write head, which sits very close to the disk's surface but should not make contact with it. If contact between the disk and the read/write head does occur, it will probably cause severe damage by scratching the recording surface of the disk. This is one of the reasons for what is called a head crash (loss of data on the hard disk).

Always move the computer with care. Most hard disks provide a designated landing zone on which the disk head can be parked when moving the system to reduce the risk of a head crash. Some systems automatically park the head each time the system is turned off. The documentation for the computer should include specific instructions for protecting the hard disk during a move.

Another potential problem for hard disk usage is fragmentation. Through the daily creation and deletion of files, the data on hard disks becomes fragmented, which decreases disk performance (speed) and could eventually result in a head crash. Operating system instructions include procedures for reducing fragmentation. There are commercial utilities, which are simple and easy to use to "tune-up" the hard disk.

NOTE: The information recorded on a hard disk is subject to error, or even totally lost, if a device that emits a magnetic force is placed near the computer's hard disk. This also applies to electronic records stored on all types of magnetic media.

Diskettes

Diskettes are the most common storage devices for personal computers because they are inexpensive and can be reused, transported, and filed. Diskettes can have the same problem with fragmentation as was previously discussed concerning hard disks. A periodic erasure and reformatting of the diskette prior to copying files off of the hard disk can help prevent a floppy disk crash. Diskettes are delicate and require special care. For further information, refer to "Care of Diskettes" in Appendix 5 of this Handbook.

Magnetic Tape and Cartridges

Magnetic tape and tape cartridges are generally associated with large mainframe or minicomputer operations. The records residing in computers are increasingly being transferred to tape on larger computers to provide a backup copy. Computers often use cartridges, or "streaming tape," for a backup copy instead of floppy disks. Like the surface of diskettes and hard disks, magnetic tape is coated with an emulsion of magnetic oxide particles. Other chemicals are also used in the manufacturing process to give the tape good operation characteristics, such as flexibility, conductivity, and softness.

Computer magnetic tape is a fragile medium, highly susceptible to the generation of error by improper care and handling. The complete care and maintenance of magnetic tape can be a complicated and involved process. Even under ideal conditions of controlled storage, magnetic tape is not expected to retain data in a readable state any longer than 10 years. For further information, see the "Common Causes of Tape Damage and Data Loss" in Appendix 6 of this Handbook.

Optical Disks

Optical disk technology offers a stable media environment as compared to magnetic hard drives. Read/write optical disk systems provide a supplement, complement, or alternative to magnetic storage media in a broad spectrum of data and document storage applications. These systems permit the direct recording of information generated by keyboards, document scanners, and other input devices. They can also record information transferred from magnetic media and other optical media, or downloaded from a mainframe.

Read/write optical disk systems include both equipment and media. Optical disk drives are readily available for purchase as computer peripheral devices.

Considerable additional engineering and programming expertise may be required for the hardware customization and software development necessary to combine scanners, computers, optical media, video displays, printers, and other components into an effective document storage and retrieval system. Read/write optical media can be divided into write-once and erasable varieties. Write-once optical disks record irremovable information. Erasable optical disks, like their magnetic counterparts, permit reuse of previously recorded media segments.

Optical disks resemble a phonograph record/platter and are available in 12-inch, 8-inch, and 5.25-inch sizes; the sizes change depending upon the manufacturer and the technology. There has been very little standardization in the design of this media. CD- ROM and DVD are also optical disks (media) but due to their popularity in the entertainment industry this media is very standardized and can be used with a wide variety of equipment.

Optical disks differ in materials, construction, thickness, etc. Regardless of recording technology or media source, write-once optical disks are enclosed in plastic cartridges to facilitate handling and protect them from environmental contaminants. A laser beam "writes" data onto the disk. The information is represented on the disk by a change in the surface reflectivity and is read by using a low-powered laser to sense the changes. Optical disks have recording surfaces on either one side or both sides, with dual sides being the most common.

The World Wide Web & Internet

The Internet is a communications method or protocol that links servers and the individual computers attached to them. The Web page is a document residing on a server that contains text, graphics, animations and videos. All servers use hypertext markup computer language to permit them to display the Web page information on the screen of the individual user. Various pages of hypertext are linked together on a single server.

As the Web pages and the data that is captured from them become the substitute for paper transactions, retention periods and methodology will need to be applied as with other electronic records. The use of agency websites to communicate information to the public may be important records, which need to be managed and addressed in records retention schedules.

Note: For more information on the WWW, please see Appendix 12.

LEGAL ASPECTS OF ELECTRONIC RECORDS

Legal standards, for the acceptability of records other than paper records as evidence, have been slow to evolve. State and federal historical legislation, which allowed for the admissibility of microfilm as evidence, had to gradually develop. Paper copies of microfilmed records are admissible if microfilm is created with proper certification and standardized procedures.

Additionally, precedent has shown that if a government agency, in the regular course of business, has recorded, copied, or reproduced by any photographic or other process which accurately reproduces the original, the original may be destroyed in the regular course of business. The reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not. (See also "Legal Guidance" earlier in this Handbook.)

ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

Electronic records satisfy requirements for written materials so that the enforceability of a record or signature cannot be denied simply because it is electronic form. Electronic records must still satisfy any other formal requirements, such as notices, disclosures or completeness of terms. For example, if the parties' e-mails show agreement on the sale of widgets, these electronic records would still need a quantity term to create a valid contract. Electronic records and signatures simply satisfy requirements under existing law, such as the statute of frauds that require documents be in signed writing. An electronic signature is defined as:

"Electronic signature means 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."

One specific type of electronic signature is called a digital signature. The term "digital signature" is often used to denote the use of encryption technology to enable a computer user to transmit 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.

The Electronic Signature in Global and National Commerce Act and the Uniform Electronic Transaction Act

Electronic signatures have been incorporated as part of the Federal law as the “Electronic Signature in Global and National Commerce Act (ESGNCA);" and “The Uniform Electronic Transaction Act (UETA); the California Public Records Act, Section 6250; and Section 1633 of the California Civil Code.

The Electronic Signature in Global and National Commerce Act (ESGNCA)

On June 30, 2000, the President of the United States signed the "Electronic Signatures in Global and National Commerce Act" establishing the validity of electronic signatures for interstate and international commerce. After signing the bill with pen and ink (still required for legislation), the President also signed it electronically.

The Act is an important piece of legislation. It is cautious and conservative in that it lets the market make the important decisions about electronic signatures and about the infrastructure required to use and trust them. The focus on the market rather than legislation as the primary force to shape the use of electronic signatures has important implications for managers of businesses that might use such signatures.

Rather than simply understanding the law, business managers also need to understand the risks and benefits associated with electronic signatures. They need to be able to identify the key capabilities that they need to put in place in order to prevent fraud and to reduce the potentially significant liabilities associated with uninformed use of electronic signatures. Most important, they need to be able to make judgments about when the use of electronic signatures makes business sense.

Uniform Electronic Transaction Act (UETA)

The State of California enacted the UETA on September 16, 1999 under the 1999 California Senate Bill 820**.** California's version differs from the National Conference of Commissioners on Uniform State Law's (NCCUSL) UETA by adding provisions under the "use of electronic records and electronic signatures" section, the "notarization and acknowledgment" section, as well as the "time and place of sending and receipt" section.
Additionally, California's version of UETA eliminates sections 16-20 of the NCCUSL version that relate to transferable records and the use of electronic records by governmental agencies.

With the provisions of the UETA becoming effective January 1, 2000, the UETA is substantially the same form as the ESGNCA that became effective October 1, 2000. The UETA's limited objective 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. It is intended to eliminate any doubt about the enforceability of electronic transactions, and thereby remove barriers to their use in the business, public, and government sectors.

UETA recognizes and authorizes the conduct of business, public and governmental affairs using electronic means. The UETA applies to "electronic records and electronic signatures relating to transactions." It defines electronic record as *"a record created, generated, sent, communicated, received, or stored by electronic means."*

The UETA applies to all the electronic records and signatures related to a transaction, and would cover e-mails, reports, memoranda, accounting records, or other electronic documents prepared in connection with a transaction.

Some of the more significant provisions of the UETA are:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

- If a law requires a record to be in writing, an electronic record satisfies the law.

- If a law requires a signature, an electronic signature satisfies the law.

In summary, the UETA applies to transactions that the parties have agreed to conduct electronically. Under most circumstances, electronic records and electronic signatures may now be used in place of traditional paper-based and handwritten methods. In the area of records retention, electronic records may replace other methods so long as there is assurance the electronic records will provide the accuracy, integrity, and accessibility of traditional methods of retention. For more information on the UETA, please see Appendix 10, Overview of the Uniform Electronic Transaction Act.

Electronic Records as Evidence

Electronic records as a group involves a much newer medium than paper or microfilm. Precedent has also shown some courts, admitted records with a variety of contents and forms. Each judge is free to dismiss evidence on the basis of the court's independent evaluation of the authenticity of a given document.

The court must believe that records admitted before it, are "trustworthy" that is, they must clearly and accurately relate the facts as originally presented in summary form.

In contrast to traditional paper records, electronic records have systemic vulnerabilities and additional efforts must be taken to assure the court of their trustworthiness. Hence, an electronic recordskeeping system incorporates the functionality to assure the court of the reliability of the recordskeeping integrity. For the mini and mainframe environments, attention to the following items will enhance record trustworthiness:

- Equipment and software reliability.
- Preparing printouts in the regular course of business.
- Records retention schedule.

Equipment and Software Reliability

Since the content of a record may change if the equipment is not working properly, an organization may be required to present evidence that its equipment was operating reliably on the day the computer record was prepared.

A computer operations log indicating the absence of any malfunctions is generally adequate. Errors in computer records can also result from errors in computer programs.
An organization may be required to present evidence related to the development and testing of programs. An expert witness to determine its accuracy or reliability often examines programs. An organization may be required to present the specific version of the computer program used to process the data or manage the electronic document being entered into evidence.

A different version of the program may be considered if it is the only one available, but the absence of the exact version may raise serious questions on the trustworthiness of the computer records.

Preparing Printouts

Computer printouts prepared in the ordinary course of business activity are perceived to have higher trustworthiness than similar computer printouts prepared for trial. However, if the organization can show an adequate audit trail leading to data creation and merely a time lag before printing, the acceptability of the printouts is improved.

Records Retention Schedule

An approved records retention schedule can have a profound impact on court proceedings because the schedule establishes a retention period and specified disposition time.

Although an approved retention schedule for a record requested does not guarantee the court's acceptance of it, the fact that a record is scheduled definitely helps meet the requirement of a record being created as a "regular practice" of the agency. Courts also accept the defense that records have been disposed of under an approved records retention schedule.

Electronic recordskeeping systems incorporate the ability to associate a specific electronic document (as part of a specific record) with a specific electronic retention schedule providing further assurance of the link between the retention policy and the disposition of the specific record in question.

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 properly. Dismissal of cases, fines and sanctions has been imposed for failure to produce required records. If records are willfully withheld or the entity cannot demonstrate a good faith effort to find them, in some extreme cases criminal sanctions have been imposed.

ELECTRONIC MAIL

Electronic mail systems, commonly called e-mail, are becoming the communications method of choice for many public officials and public employees. E-mail messages are often used as communication substitutes for the telephone as well as to communicate substantive information previously committed to paper and transmitted by more traditional methods. This combination of communication and record creation/keeping has created ambiguities on the status of e-mail messages as records.

The management of e-mail systems touches nearly all functions for which a government agency is dependent on recordskeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly is the same as for other records keeping systems--to ensure compliance with California laws concerning the creation of, retention of, and access to public records.

Government agencies that use electronic mail have an obligation to make employees aware that e-mail messages must be retained and destroyed according to established records management procedures. Agencies should set up or modify e-mail systems to facilitate electronic records management. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place.

Definitions

E-mail **systems** are store-and-deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that shuffles messages to users within an agency or office; to a wide area network e-mail system that carries messages to users in various physical locations; to Internet e-mail that allows users to send and receive messages from other Internet users around the world.

E-mail **messages** are electronic documents created and sent or received by a computer system. This definition applies to the contents of the communication, the transactional information, and any attachments associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

Record Management Concerns

Government Code Section 14741 provides the following:

"Record(s)" means all paper, maps, exhibits, magnetic or paper tapes, photographic films and prints, and other documents produced, received, owned or used by an agency, regardless of media, physical form or characteristics."

An e-mail message is a document produced, received, owned or used by an agency. Whether the e-mail serves to document the organization, functions, policies, decisions, procedures, operations or other activities is the deciding factor as to its status as a record. This is true of any communication, whether electronic or paper.

E-mail messages that meet the criteria of the definition of a record must be scheduled and retained for the appropriate time period before disposition. E-mail messages that meet the criteria of the definition of a record may be considered public records and must be available to the public

As with any format, an e-mail message is considered a public record unless it falls under one or more exclusions such as individual rights to privacy. These records must be maintained and made accessible to the public upon request through the appropriate requesting process, i.e., Public Records Act.

Retention and Scheduling Requirements

E-mail itself is not considered a record series or category. It is a means of transmission of messages or information. Like paper (mail) or microfilm, e-mail is the medium by which this type of record is transmitted. Just as an agency cannot schedule all paper or microfilm records together under a single retention period, an agency cannot simply schedule e-mail as a record series.

Retention or disposition of e-mail messages must be related to the information they contain or the purpose they serve. The content, transactional information, and any attachments associated with the message are considered a record (if they meet the agency's record management plan criteria). The content of e-mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

One of the difficulties with e-mail is arbitrary size limits on e-mail user "mail boxes" which require users to purge or archive files or be restricted in their use of the system until the mail boxes are kept below the size limit. This may contribute to improper deletion of e-mails that are records. Education of Information Technology professionals on the records implications and proper training of personnel can ensure good records management procedures are followed. Use of an electronic recordskeeping system also helps to manage this increasing source of records.

NOTE: Simply backing up the e-mail system onto tapes or other media or purging all messages after a set amount of time are not appropriate strategies for managing e-mail.

For more information on records management, contact your agency's records management analyst/manager or the DGS Records Management Program.

Guidelines and Best Practices for Managing E-Mail

Record Copy E-mail

E-mail users should be aware that e-mail messages are often widely distributed to a number of various recipients. Determining which individual maintains the record copy of the message, i.e., the original message that must be retained per the retention schedule, is vital to e-mail management. If the holder of the record copy is not identified and aware of his/her responsibility, the agency may find that no one retains the message or that everyone retains the message. Neither of these scenarios is appropriate.

For example, in the absence of an electronic recordskeeping system, agency policy documents which are transmitted to multiple recipients via an e-mail system, need not be maintained by each recipient beyond his or her need for this information, if the record copy responsibility is established so that the record is maintained by some office or agent for its established retention period. In this example, a logical record copy responsibility rests with the creator of the policy document. Prompt deletion of duplicate copies of e-mail messages from an e-mail system makes the system as a whole much easier to manage and reduces disk space consumed by redundant information. Another technique to avoid proliferation of duplicate copies is to use e-mail to notify readers of a document that is then accessed by the user going to a shared drive or other source, or by providing a link to the document. The document can then can be managed in one location.

This example, however, becomes increasingly difficult to manage as the electronic records grow in volume and diversity. An electronic recordskeeping system keeps track of the originator, disposition, and relationships to other documents within the record.

NOTE: Generally speaking, the individual who sends an e-mail message should only maintain the record copy of the message under the control of the electronic recordskeeping system.

Filing

E-mail messages should be filed in a way that enhances their accessibility and that facilitates records management tasks. Agencies should set up or modify e-mail systems to facilitate records management and appropriate filing systems. Procedures and systems configurations will vary according to the agency's needs and the particular hardware and software in use, but electronic recordskeeping systems must conform to the DGS "Specifications for Electronic Record Management Software."

NOTE: Employees should be responsible for classifying messages they send or receive according to content, the agency's file classification scheme and established records series.

Distribution Lists

If you send to a "distribution list" (not a listserve, but a specified list of individuals), you must also keep a copy of the members of that list for as long as you are required to keep the message itself. It is of little value to know that the "Security Alert!" notice went to "Swat Team 7," without knowing whether Arnold S. or Judy F. received the message. Nicknames present a similar problem.

Subject Lines

Fill in the subject line on your e-mail both to help your recipient identify and file messages, and to help you file your SENT ITEMS box messages that must be retained for some period. Subject lines should be as descriptive as possible.

Following are some examples of poor and good subject lines for the same message:

Poor or confusing subject lines	**Better, descriptive subject lines**
"Helpful Info"	"Contact Info"
"Report"	"Quarterly Financial Report"
"Minutes"	"January 2001 Board Minutes"
"Important"	"Revised Admin. Procedures"
"News"	"New Agency Head Appointed"
“Contract Status”	“PO 12345 Delivery Status”

Storage of E-mail

We recommend that agencies explore retaining records from an e-mail system in a central repository managed by an electronic recordskeeping system within on-line storage.

E-mail Messages and the Rules of Evidence

Agency personnel should be familiar with both state and federal "rules of evidence" requirements. For records maintained in electronic information systems, including e-mail systems, courts concentrate on assurances that records, and the systems in which the records are created and maintained, are reliable. The reliability of the process or system used to produce records, not the type of media or technology used, determines the admissibility of records in evidence. Moreover, the federal rules of evidence place the burden for the identification of relevant records on the record creator, and within a reasonable time period.

At a minimum, agency personnel should ensure the following:

- E-mail systems used to create, receive and maintain e-mail messages have full, complete, and up-to-date systems documentation

- E-mail systems follow all recommendations for system security

- Complete systems backups are regularly and consistently performed

- E-mail system should retain all data and audit trails necessary to prove its reliability as part of the normal course of agency business

- The record copy of a message is identified and maintained appropriately

- Backup procedures should be coordinated with disposition actions (within the established methodology) so that no copies of records are maintained after the retention period for the records has expired

Again, agency records managers need to plan for records maintenance and record copy responsibilities for the records system to meet requirements for reliability and legal records disposition. Close coordination with information technology professionals is needed.

NOTE: The e-mail system should allow the server administrator to prevent destruction of records for legal and/or audit purposes.

Access

A major challenge for agency records managers is to guarantee that records maintained in electronic information systems are accessible and usable for the entire length of the retention period. Rapid changes and enhancements to both hardware and software compound this challenge. As many e-mail systems have limitations in storage space that cause operational problems when messages are stored in the system beyond a specific period (such as sixty or ninety days), procedures must be in place to transfer records from the e-mail system to another electronic recordskeeping system to meet retention requirements.

NOTE: Messages should be maintained in a format that preserves contextual information (metadata) and that facilitates retrieval and access. The system should allow deletion of messages once their retention periods expire.

Beyond this generic challenge of technology change, there are more mundane, but equally critical steps that must be in place to ensure that records created by e-mail systems can be located and retrieved when required. A central step is a system of standardized naming conventions and filing rules within the e-mail systems.

E-mail messages should be indexed in an organized and consistent pattern reflecting the ways in which records are used and referenced. Records maintained electronically, including e-mail messages, have an advantage over conventional "hard copy" document filing systems in that indexing for multiple access points is relatively simple and inexpensive, provided an effective indexing framework is in place.

Planning records indexing and retrieval points is time well spent. Unnecessary time needed to retrieve electronic records is not productive staff time, and is an annoyance to the public as well.

Messages should be stored in a logical filing system that is searchable by multiple data elements.

Responsibility

Roles and responsibilities of agency personnel should be clearly defined. Employees must understand and carry out their role in records management and agencies must ensure compliance with agency procedures and California law. Unauthorized users should not be able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology managers and server administrators have different responsibilities in managing electronic records. Agencies should clearly identify the roles of each; adopt procedures, train staff and monitor compliance on a regular basis. The creator or recipient should make decisions regarding messages. The agency should take appropriate measures to preserve data integrity, confidentiality and physical security of e-mail records.

FINAL DISPOSITION OF RECORDS

Final disposition is the last stage in the life cycle of records, when they no longer serve a useful purpose for agency business. At this point, identified records may be destroyed or transferred to the California State Archives for permanent preservation.

Records Destruction and Services

The objective of records destruction is to remove the record permanently from possible use after it has become obsolete and to ensure that sensitive or confidential information does not become public. Because destroyed records cannot be recalled, extra care should be taken before records destruction. All statutory requirements must be satisfied.

Final disposition of state records must be according to an approved STD Form 73, Records Retention Schedule, and a properly prepared STD Form 71, Records Transfer List. See the Records Retention Handbook for general procedures for the destruction of records. All destruction procedures described apply to the record (official) copy. Convenience or reference copies should be disposed of as soon as they are no longer needed. In some instances, convenience copies could be confidential and must be destroyed in accordance with the prescribing directives.

Within the State Records Center, the Document Destruction Center operation facilitates the destruction of confidential microfilm, microfiche, computer cassettes, computer tapes as well as the traditional paper. An on-sight shredding process is provided and overseen by authorized state personnel. Appointments can be scheduled for "witness" destruction, if so required, at no extra cost.

Archival Preservation and Processing Requirements

The California State Archives “flags” developed records retention schedules as part of California's State Records Management Program approval process that their staff wishes to review. The “flag” identifies potential archival, historical, research, or uniquely significant electronic records that are important to the State of California. The final disposition of these electronic records must be coordinated with, and transferred to the California State Archives. State agencies are responsible for coordinating and ensuring the proper transfer of these electronic records.

Because of the variety of formats of electronic records, issues of proprietary software and specialized hardware, decisions must be made in consultation with California State Archives, as to whether to transfer the records or maintain them in the agency of origin. If a transfer decision is made, the method, frequency, and format of the transfer must be determined cooperatively by the agency and California State Archives.

Timing of the actual physical transfer of electronic records should be determined through the records retention schedule process. California State Archives must be involved early in the process to ensure the archival requirements are met. Special preservation measures are often required to preserve electronic records.

Electronic records may require conversion to a medium and format suitable to ensure long-term access and readability. All appropriate system documentation must accompany the transfer of electronic records. A computer database without minimum documentation is useless because the contents cannot be read or interpreted.

Electronic records containing information will, like other records containing confidential information be under the same restrictions in the State Archives as they are in the agency of origin. Transfer to California State Archives does not affect the statutory restrictions on access to confidential information.

Also, the courts have determined that e-mail in its native format may be a record and must be managed appropriately. Electronic records are stored on a variety of media, such as magnetic tapes, disks, video files and optical disks. Remember, it is not the medium that is the primary factor for determining potential archival preservation--it is the “records series” itself.

Procedures for Purging Files

Written procedures should be developed for the purging and disposition of electronic records after the retention period is complete. Depending on the volume of records and the staffing situation of the agency, purging of files can be performed on a monthly, quarterly, semi-annual, or annual basis. For electronic records, procedures for purging of records should be performed within the electronic recordskeeping system.

The Records Management Program recommends that the agency maintain a disposition log. This log reflects the records series titles, dates covered, volume, and date of final disposition. The electronic recordskeeping system software will provide an audit disposition log.

Responsibility for Approving Disposition

Written procedures or designated authorization should verify who has responsibility and authority for approving final disposition of records.

- If the agency has a current STD Forms 72, Records Retention Schedule Approval Request, which is signed by both the program manager (or person authorized to sign for the program manager) directly responsible for the records listed on the STD Form 73, Records Retention Schedule, and the Records Management Analyst and/or Manager and the Department of General Services, the disposition of all the records series as listed is authorized.

- If a records series is not listed on the approved STD Form 73, the agency must amend the STD Form 73 appropriately to dispose of that records series. A records series can also be added to the schedule for approval by amending again the STD Form 73. The details of the process to develop and update the agency records retention schedule are discussed in the Records Retention Handbook.

- If there is not an approved records retention schedule, the agency must submit both the STD Forms 72 and 73 and have them approved before final disposition is authorized. Steps for processing the STD Forms 72 and 73 are again listed in the Records Retention Handbook.

Disposition of Magnetic Media

Electronic records are usually stored on erasable, reusable, fragile and relatively inexpensive media. The data on this media are easy to revise and update. For these reasons, the disposition of electronic records should be determined as early as possible when they are no longer needed for state business.

Diskettes that contain sensitive or confidential electronic records should not be discarded in regular waste containers. They should be cleared by degaussing (a method of electromagnetic erasure) and reused, or reformatted and reused, or rendered useless by shredding. Data scrambling programs are also available as a means of making the file's data permanently unavailable. The same methods apply to hard drives except if not degaussed or reformatted, they should be rendered useless by complete destruction.

These specific precautions are required for confidential information because many computer operating systems do not actually erase the entire file when files are "deleted." They simply remove the file's name from the system directory. This allows the space occupied by the file to be declared available for a new file. The electronic records remain unchanged until that portion of the disk is reused. Consequently, "deleted" electronic records files may be recovered by using commercially available utility programs.

NOTE: For active or current records within an electronic recordskeeping system it is acceptable for authorized personnel to "delete" files, consistent with security, and then simply reuse the space on the magnetic media for new information. The recordskeeping system will preserve an audit trail regarding record disposition.

SUMMARY - WHY ELECTRONIC RECORDSKEEPING?

When properly employed, electronic recordskeeping is an efficient tool for managing the entire record, across many media, because of the unique characteristics (i.e., volatility, metadata, etc.) of electronic records and the complexity of their use. An even more thoughtful application of sound records management principles needs to be given electronic record creation, maintenance, and final disposition.

To have an effective electronic records management program, the agency Records Management Analyst and/or Manager--in cooperation with administrative, professional, technical, and administrative support staff must:

- Establish the necessary program elements to manage all records using electronic recordskeeping.

- Use the electronic recordskeeping systems to provide an up-to-date records inventory.

- Make the decisions necessary for developing the agency records retention schedule.

- Organize electronic files to maximize their usefulness.

- Implement security measures to protect electronic information.

- Cooperate with the California State Archives to preserve the State's historical heritage.

- Apply the approved retention schedule and agency procedures to dispose of obsolete electronic records.

A FINAL COMMENT

Agencies are encouraged to contact staff at CalRIM, State Records Program, Department of General Services with any concerns regarding the management of electronic records. We trust that this Handbook will prove helpful in developing and improving effective electronic records management in all state agencies. As standards for electronic recordskeeping systems and procedures for their management continue to develop, the State of California Records Management Program will provide further information and guidelines to state agencies.

APPENDICES

APPENDIX 1 - GLOSSARY OF RECORDS MANAGEMENT TERMS

ACCESS: Permission to use and reproduce records. May be limited or qualified (restricted by the agency having legal custody).

ACTIVE FILE: Materials, which are maintained in the office of an agency for current daily operations and are referred to frequently.

ACTIVE RECORD: A record, which is regularly referred to and required for current use. Usually considered those records that are referred to more than once per file drawer per month.

ADMINISTRATIVE RECORDS: Records that are created to help an agency accomplish its current administrative functions.

ADMINISTRATIVE VALUE: The usefulness of records to the agency in making administrative decisions and determining policy or in explaining organizational structure or procedures.

ALPHABETIC FILING: A filing arrangement of names, subjects, or geographic locations.

ALPHANUMERIC FILING: Arrangement of files using a combination of alphabetic and numeric characters.

APPRAISAL: See RECORDS APPRAISAL.

ARCHIVAL RECORDS: Records identified as having archival value or potential archival value on the agency records retention schedule.

ARCHIVAL VALUE: The determination in appraisal that records are worthy of permanent preservation by an archival institution. See also HISTORICAL VALUE (the values that justify the indefinite or permanent retention of records as archives).

ARCHIVES: (1) The agency responsible for selecting, preserving, and making available archival materials. (2) The building in which an archival institution is located. (3) Those records that are no longer required for current use but have been selected for permanent preservation because of their evidential, informational, or historical value.

ARCHIVING: For data processing usage, generally means creating a backup copy of computer files--especially for long-term storage. Can also mean transfer of records to archives for permanent preservation.

ARCHIVIST: (1) A person professionally responsible for the administration, management, and identification of historical records. (2) A person responsible for or engaged in one or more of the following activities in an archives: appraisal and disposition; accessioning; preservation; arrangement; description; reference service; exhibition or publication.

ASP: An Application Service Provider often providing one or more products and/or services. The advantage of the ASP is the opportunity for organizations to, in effect, lease software applications and storage space and to perform transactions without having to maintain software and various electronic repositories. This is a variation on the Internet Service Provider (ISP) concept, extended into a more specialized domain (i.e., recordskeeping software & repositories).

BACKING UP: Making a copy of a computer file for use if the original is lost, damaged, or destroyed. See also ARCHIVING and DUMPING.

CENTRAL PROCESSING UNIT (CPU): the component of a computer system that interprets and carries out program instructions, and controls the overall activity of the computer.

CERTIFICATION: (1) Attestation of the authenticity or official character of a document or reproduction of the document. (2) The document embodying the attestation.

CHARACTER: Any symbol, such as a number, letter, or punctuation mark, that represents data and that, when encoded, can be processed or stored by a computer.

CHRONOLOGICAL FILING: Arrangement of files by date.

CODING: The act of applying file designations on records for the purpose of classification or condensation.

COMPUTER: An electronic device designed to accept data (input), perform prescribed mathematical and logical operations at high speed (processing), and supply the results of these operations (output). A digital computer processes data as numbers and includes mainframe computers, minicomputers, and microcomputers.

COMPUTER-ASSISTED RETRIEVAL (CAR): A records storage and retrieval system, normally microfilm-based, that uses a computer for indexing, automatic markings such as blips or bar codes for identification, and automatic devices for reading those markings and for transporting the film for viewing.

COMPUTER CODE: A set of rules to convert data to a form that computers can process. Examples include ASCII (American Standard Code for Information Interchange) and EBCDIC (Extended Binary Coded Decimal Interchange Code).

CONVENIENCE COPY: A copy created for administrative ease of use, also called a working or reference copy; not the official record copy.

COPY: The reproduction, by any method, of the complete substance of a record; a reproduction of an original.

CROSS-REFERENCE: A notation in a file or on a list showing that a record has been stored elsewhere.

CUSTODY: The guardianship of records. Features of custody differ between (a) physical custody and (b) legal custody. See also LEGAL CUSTODY and PHYSICAL CUSTODY

DATA: Symbols, or representations, of facts or ideas that can be communicated, interpreted, or processed by manual or automated means. Often associated with electronic data or with statistics or measurements.

DATABASE: A set of data, consisting of at least one data file or a group of integrated data files, usually stored in one location and made available to several users at the same time for various applications.

DATABASE MANAGEMENT SYSTEM (DBMS): A software system used to access and retrieve data stored in a database.

DATA ELEMENT: A combination of characters or bytes referring to one separate item of information, such as a name, address, or age. See also LOGICAL RECORD.

DATA FILE: (1) An organized collection of related data, usually arranged into logical records that are stored together and treated as a unit by a computer. (2) Related numeric, textual, or graphic information that is organized in a strictly prescribed form and format. Used in contrast to text documents that may be recorded on electronic media.

DATA PROCESSING: Handling and processing of information necessary to record the transactions of an organization. Usually used in conjunction with mechanical and electronic data-handling equipment.

DATA RANGE: The period of time covered by records in a file.

DBMS: See DATABASE MANAGEMENT SYSTEM.

DECENTRALIZED FILES: Files scattered throughout an organization; not centralized. Usually contain records that are generated and used by a single organizational unit and maintained and controlled at the point of origin.

DELETING: The process of removing, erasing, or obliterating recorded information from a medium, especially a magnetic tape or disk, which then may be reused.

DICTIONARY ARRANGEMENT: A system of filing records in alphabetic order by subject. Also referred to as topical arrangements.

DIRECT ACCESS FILING: A method in which no code is needed to reference a file.

DISK DRIVE: A device that spins the disk and writes/reads information on/off disks.

DISKETTE: In word processing and computer systems, a recording/storage medium consisting of a flexible disk of Mylar, which is coated with a material that can be magnetized to store data and enclosed in a protective envelope.

DOCUMENT: An instrument containing recorded information.

DOCUMENTATION: A collection of written descriptions and procedures that provide information and guidance about a program or about all or part of a computer system so that it can be properly used and maintained.

DOCUMENT REQUEST: An inquiry for a document or documents, including copies or reproduction thereof. See also ACCESS.

DUMPING: (1) The process of copying recorded information from internal memory to an external storage medium, such as a magnetic tape or a printout, for backup, analysis, or some other purpose. (2) The process of transferring recorded information from one storage device to another, such as from a disk to a tape.

DUPLEX-NUMERIC FILING: Arrangement of files using two or more sets of code numbers, with the sets separated by dashes, commas, periods, or spaces.

DVD: See OPTICAL DISKS.

ELECTRONIC DATA PROCESSING (EDP): The use of a computer to process data. Often used as a synonym for automated data processing (ADP) or data processing (DP).

ELECTRONIC DOCUMENT IMAGING (EDI): A technology designed to provide for the storage and retrieval of all bitmapped documents, regardless of format, though most often a group four (compression) tiff (tagged information file format).

ELECTRONIC INFORMATION PROCESSING SYSTEM: All computerized and automated information handling, including systems design and analysis, conversion of data, computer programming, information storage and retrieval, voice, video, and data communications, system controls, simulation, and all related interactions between people and machines.

ELECTRONIC RECORDSKEEPING: The use of records management principles for records maintained electronically as opposed to electronic recordskeeping system which is designed specially to merge electronic and paper records primarily in an automated manner.

ELECTRONIC RECORDSKEEPING SYSTEM (ERS): Software used by an organization to manage all its records, regardless of format, over the entire record's lifecycle. Primary recordskeeping functions must include categorizing, locating, identifying and controlling record disposition requirements, including management of the storage, retrieval, and disposition of the records, regardless of the repository. This type of software includes the capabilities of both Integrated Document Management System (IDMS) and Records Information Management (RIM) software.

ELECTRONIC RECORDS: Records stored in a form that only a computer can process. Also called machine-readable records. See UETA definition that meets the State's requirements.

ELECTRONIC SIGNATURE: An electronic 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.

ENCYCLOPEDIA ARRANGEMENT: A system of filing records in alphabetical order by major topic names, then according to related subheadings.

ESSENTIAL RECORDS: See VITAL RECORDS.

EVIDENTIARY VALUE: The value of providing evidence of the origins, structure, functions, policies, and operations of an agency.

FIELD: An assigned area in a record to be marked with information.

FILE INTEGRITY: Accuracy and completeness of the records.

FILE PLAN: The planned methodology of classification and indexing records for storage and retrieval consistent with the records management plan.

FILES MANAGEMENT: The management function which provides for the analysis of filing equipment and the procedures to determine the most efficient type of equipment and system for a given operation at the most economical price.

FILING: The process of arranging and sorting records so that they may be retrieved rapidly when needed.

FILING SYSTEM: A system, often involving equipment and/or software, for arranging records for efficient storage and retrieval (See file plan and files management).

FINAL DISPOSITION: See RECORDS DISPOSITION.

FINDING AID: Any written guide such as an index, list, inventory, or catalog that is descriptive or analytical with respect to a body of records, and having the purpose of clarifying the subject content and organization of the records in order to facilitate their use.

FISCAL RECORDS: Financial records of an organization that have a fiscal value.

FISCAL VALUE: The usefulness of records to the organization as relating to financial transactions and the movement and expenditure of state, federal, or other funds.

GEOGRAPHIC FILING: Arranging records alphabetically according to the names of geographic locations.

HARD COPY: (1) The original document, the reproduced paper copy made from microfilm, or the printout made from data processing media. (2) A record that can be read without the use of a viewer or magnifying device.

HARD DISK: A disk made of a rigid base, such as ceramic or aluminum, coated with a magnetic material. See also DISKETTE.

HARDWARE: In a data processing system, the mechanical components such as computers, monitors, and tape drives. See also SOFTWARE.

HEAD: An electromagnetic device that transfers data to and from the surface of a magnetic storage device, such as disk or tape. Also called read/write head.

HEAD CRASH: The destruction of data on a magnetic disk caused when the read/write head unintentionally comes in contact with the disk.

HISTORICAL VALUE: (1) The usefulness of records for historical research concerning the agency of origin or for information about persons, places, events, or things. (2) The value arising from exceptional age, and/or connection with some historical event or person.

HOLDINGS: All of the records in the custody of a given agency, organizational element, archival establishment, or records center.

INACTIVE RECORDS: Records that have a reference rate of less than one search per file drawer per month. Records that are not needed immediately, but which must be kept for administrative, fiscal, legal, historical, or governmental purposes, prior to disposition.

INDEX: An organized finding aid to the contents of a document, data base, or filing system, arranged in a logical array, giving document or data location in storage. Usually a list or file that is arranged alphabetically or numerically for the purpose of facilitating references to topics, names, numbers, or captions within a body of information.

INDEXING: The action of specifying or determining the predestined topic, name, number, or caption under which a document is to be filed.

INDIRECT ACCESS FILING: A system in which reference to the code under which material is filed must be made before the file can be located.

INFORMATION: Knowledge communicated by others or obtained by study and investigation. In records management this is information that has been communicated in some format.

INFORMATION PROCESSING: The manipulation of data through a series of changes in order to put it into a new form for use.

INFORMATION REQUEST: A form of reference service request, asking for information to be retrieved from records in custody. Also referred to within the Records Management activity as a document request or access. See also, PUBLIC RECORDS.

INFORMATION RESOURCES: The procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

INFORMATION RESOURCES MANAGEMENT (IRM): The planning, budgeting, organizing, directing, training, and controlling activities associated with managing information resources.

INFORMATION RESOURCES TECHNOLOGIES: Data processing and telecommunications hardware, software, services, supplies, personnel, facility, resources, maintenance, and training.

INFORMATION RETRIEVAL: Recalling and repossessing data at any time needed. The manual or machine searching of a database to retrieve specific data or documents to satisfy requests for information from the database.

INFORMATION SYSTEM: The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Sometimes called a record system.

INFORMATIONAL VALUE: The value for reference or research deriving from the information the records contain, as distinct from evidential value; often records have informational value that the creators did not envision.

INTERFILE: The process of putting documents in their proper sequence in a file of which they have not previously been a part.

INVENTORY: See RECORDS INVENTORY.

IRM: See INFORMATION RESOURCES MANAGEMENT.

JUKEBOX: An automated optical disk library. This device stores disks, uses robotic technology to retrieve a disk and has one or more read/write drives.

LAN: See LOCAL AREA NETWORK.

LEGAL CUSTODY: Control of, access to, possession of, or responsibility for records based on specific statutory authority. Ownership or title to documentary materials.

LEGAL VALUE: The usefulness to an agency of records that provide legal proof of agency authority and agency business transactions; also refers to the usefulness of records that form the basis of legal actions, or that contain evidence of legally enforceable rights or obligations of government or private persons.

LIFE CYCLE OF RECORDS: The management concept that records pass through the stages of creation, maintenance, use, and disposition.

LOCAL AREA NETWORK (LAN): A system for linking together computers, terminals, printers, and other equipment, usually within the same office or building.

LOGICAL RECORD: A collection of related data elements, referring to one person, place, thing, or event that are treated as a unit by a computer.

MACHINE-READABLE RECORDS: See ELECTRONIC RECORDS.

MAGNETIC TAPE: A tape or ribbon of any material impregnated or coated with magnetic material (iron oxide) on which information may be placed in the form of magnetically polarized spots. Commonly used as a medium for carrying computer programmed information.

MAINFRAME COMPUTER: A large digital computer, normally able to process and store more data than a minicomputer and far more than a microcomputer, designed to do so faster than a minicomputer or a microcomputer, and often serving as the center of a system with many users.

MASTER RECORD: The original record from which copies may subsequently be made.

MIDDLE-DIGIT FILING: File arrangement using the middle digit or set of digits as the primary filing unit.

MINICOMPUTER: A small digital computer, normally able to process and store less data than a mainframe but more than a microcomputer while doing so less rapidly than a mainframe but more rapidly than a microcomputer.

MIGRATION: A strategy for avoiding obsolescence in media or file type that involves the periodic duplication of files and/or content into new media and/or file type, respectively.

NONESSENTIAL RECORD: Record that is not vital to the continued operation of an agency.

NUMERIC FILING: Arrangement of numeric characters in various combinations.

NUMERIC HISTORY FILE: A forms control file consisting of copies of each form used by the agency, placed in numerical order.

OCR: See OPTICAL CHARACTER RECOGNITION.

ODSS: See OPTICAL DATA STORAGE SYSTEM.

OFFICIAL RECORD: See RECORD COPY.

OFF-LINE: Not under the direct control of a computer. Refers to data on a medium, such as a magnetic tape, not directly accessible for immediate processing by a computer.

ON-LINE: Under the direct control of a computer. Refers to data on a medium, often a hard drive, directly accessible for immediate processing by a computer.

OPTICAL CHARACTER RECOGNITION (OCR): A process that scans text images and stores the scanned characters in digital form.

OPTICAL DATA STORAGE SYSTEMS (ODSS): An electronic imaging system which stores digitized document images on optical disks and has a supporting database of index information for on-line retrieval.

OPTICAL DISKS: Platter-shaped, computer-oriented storage media, which permit the recording and/or retrieval of information by optical processes, typically through the use of lasers. Optical disks are recorded and/or read by specially designed drives, which function as computer peripheral devices. Optical disks and their associated drives are available in both read/write and read-only configurations, and include various proprietary optical platters, CD-ROM and DVD.

OPTICAL MEDIA: Storage media which permit the recording and/or retrieval of information by optical processes, typically through the use of lasers, includes optical disks, tapes, cards, and other similar media.

ORDER OF ENTRY: First unit to be considered in filing.

ORIGINATING AGENCY: The agency, which generates and has legal custody of a record.

PERIPHERAL DEVICE: Any device used for input/output operations with the central processing unit (CPU). Peripheral devices include the tape drives, disks, terminals, printer, etc., that are a part of a computer system and operate under the control of the CPU.

PERMANENT RECORD: A record considered being so valuable or unique that it is to be permanently preserved.

PERMANENT TRANSFER: Permanent recall of records from records center custody back to agency custody; considered to be disposition and not a reference service loan.

PERPETUAL AUTHORIZATION: Authority to dispose of records based on an approved records retention schedule.

PERSONAL COMPUTER: See MICROCOMPUTER.

PHYSICAL CUSTODY: The actual housing and maintenance of records without legal ownership, as authorized by the legal custodian.

PLAYBACK STABILITY: The period of time during which previously recorded information can be retrieved from magnetic or optical media.

POLICY: A basic guide to action that prescribes the boundaries within which activities are to take place.
PRESERVATION DUPLICATE: A copy of a vital (essential) record used to preserve the record in the event of a disaster.

PROCEDURE: A group of methods, consisting of all the steps that are taken to record, analyze, transmit, and store information needed to serve a single, specific purpose.

PUBLIC RECORDS: (1) The portion of all documents, writings, letters, memoranda, or other written, printed, typed, copied, or developed materials which contains public information. (2) In California Government Code Section 6252(e): includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. Government Code Section 6252(f): "Writing" means handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums, and other documents.

PURGING FILES: The process of clearing out inactive or obsolete records from active file storage areas for retention elsewhere or for destruction.

RAM: See RANDOM ACCESS MEMORY.

RANDOM ACCESS MEMORY (RAM): One of two main types of internal memory in the computer which holds programs and data that the user enters into the computer as well as the results of the data's manipulation. RAM is volatile in that the information is eliminated when the power of the computer is turned off. See also READ ONLY MEMORY.

READ ONLY MEMORY (ROM): One of two main types of internal memory in the computer, which holds system programs and the data that is used frequently in user programs. It retains the information even after the computer is turned off. See also RANDOM ACCESS MEMORY.

READ/WRITE HEAD: See HEAD.

RECORD (S): All paper, maps, exhibits, magnetic or paper tapes, photographic films and prints, and other documents produced, received, owned or used by an agency, regardless of media, physical form or characteristics. See also PUBLIC RECORDS and STATE RECORDS.

RECORD COPY: A record that is designated to be kept for the full retention period; not a reference, working, or convenience copy. Also known as OFFICIAL RECORD.

RECORDS ADMINISTRATOR: The person appointed by each state agency to act as the agency's representative in all issues of records management policy, responsibility, and statutory compliance.

RECORDS APPRAISAL: The analysis of records with the objective of establishing retention policy.

RECORDS CENTER: A low cost, high density centralized area for housing and servicing inactive or non-current records with reference rates which do not warrant their retention in office space and equipment.

RECORDS CONTROL: The management of documents generated or received by an organization.
RECORDS CREATION: The process of production or reproduction of records.

RECORDS DISPOSAL AUTHORIZATION: Preparing a written description of records in existence and showing the disposition actions to be taken.

RECORDS DISPOSITION: Final processing of records; either destruction, permanent retention, or archival preservation.

RECORDS INVENTORY: The physical listing of all records series created and maintained by an agency, conducted prior to the development of retention schedules. Includes data such as records series titles, media, inclusive dates, use, location, quantity, arrangement, duplication, and other pertinent information.

RECORDS MANAGEMENT: The systematic control of recorded information required in the operation of an organization's business, from creation and active maintenance and use, through inactive storage, to final disposition.

RECORDS MANAGER: The individual within an organization who has the responsibility of systematically controlling the recorded information generated and received by the organization.

RECORDS MANAGEMENT PLAN: A plan for an integrated classification and indexing scheme for the entire agency and an integral component of the agency strategic plan.

RECORDS PREPARATION: a series of steps that could include sorting, flattening, removing fasteners such as staples and paper clips, and index planning preliminary to microfilming or electronic imaging/scanning. Also called document preparation.

RECORDS PRESERVATION: The maintenance of documents in usable form.

RECORDS PRESERVATION OFFICER: A position whose duties include adopting rules concerning the selection and preservation of essential or vital records.

RECORDS PROTECTION: Safeguarding documents against unintentional destruction.

RECORDS RETENTION: Holding documents for further use.

RECORDS RETENTION SCHEDULE: A document that identifies the length of time a records series must be retained in active/current and inactive/non-current storage before its final disposition to permanent storage, archival preservation, or destruction. The schedule also indicates confidentiality, privacy, and vital records of each record series.

RECORDS RETRIEVAL: Locating documents and delivering them for use.

RECORDS SERIES: A group of identical or related records that are normally used and filed as a unit, and that permit evaluation as a unit for retention scheduling purposes.

RECORDS STORAGE: The systematic assembling of documents in containers or depositories for possible future use.

REDUCTION RATIO: The relationship (ratio) between the dimensions of the original or master and the corresponding dimensions of the micro image; e.g., a 24:1 reduction ratio would indicate that the original has been reduced to 1/24 of its original size.

REFERENCE ANALYSIS: A study or review of all requests for records during a specific time. Also referred to as reference rate.

REFERENCE COPY: A copy of an official record, which serves as a substitute for reference purposes. Also called convenience or working copy.

REFILE: The process of returning a record to its original place in a file after it has been withdrawn.

RELATIVE INDEX: An alphabetic listing of all words and combinations of words by which records may be requested. Also called a listing index.

RESOLUTION: The ability of a photographic system to record fine detail. Resolution is expressed in lines per millimeter.

RETENTION PERIOD: The period of time during which records must be kept before final disposition.

RETENTION SCHEDULE: See RECORDS RETENTION SCHEDULE.

ROM: See READ ONLY MEMORY.

SERIES: See RECORDS SERIES.

SHARPNESS: The degree of line/edge clarity in a micrographic or electronic image.

SOFTWARE: Non-hardware elements of a computer system. A set of programs, procedures, and documents concerned with the operation of a data processing system. Includes programs that enable a computer to function and control its own operation (system software) and application programs, which accomplish some user-specified task. See also HARDWARE.

STATE RECORD(S): Document, book, paper, photograph, sound recording or other material, regardless of physical form or characteristic, made or received by a state agency, department, board, commission or institution according to law or in connection with the transaction of official state business. The term does not include library or museum material made or acquired and preserved solely for reference or exhibition purposes, an extra copy of a document preserved only for convenience or reference, or a stock of publications or of processed documents.

STRAIGHT-NUMERIC FILING: Arrangement of files in consecutive order, from the lowest number to the highest.

STRATEGIC PLAN: An agency's strategic plan for achieving its vision, mission, and the means to ensure their success.

SUBJECT FILING: Classification and coding of records by subject.

SUSPENSE FILE: A file usually organized chronologically, in which documents or data are entered or filed temporarily, awaiting action.

TEMPORARY RECORDS: Records that are disposable as valueless after a stated period of time.

TERMINAL-DIGIT FILING: Files arrangement using the last digit or set of digits as the primary filing unit.

TEXT DOCUMENTS: Narrative or tabular documents, such as letters, memoranda, and reports, organized in a loosely prescribed form and format.

TRANSFERRING: moving inactive/noncurrent records to a records center pursuant to an approved records retention schedule.

UTILITY PROGRAM: A program provided by a computer center or supplier to perform a task that is required by many of the programs using the system. Common utility programs are those that copy data from one storage medium to another and sort/merge programs. Others may provide text editing, initiate the execution of programs, and perform other functions not directly related to the processing of data in a program.

VAULT STORAGE: Storing records in a completely fire-resistive enclosure designed exclusively for such storage.

VIEWER: A device having a viewing screen for displaying micro images that are on either roll film or fiche. See also READER.

VITAL RECORDS: Records containing information necessary to the operation of government in an emergency created by disaster; and records to protect the rights and interests of individuals or to establish and affirm the powers of government in the resumption of operation after a disaster.

VITAL RECORDS RETENTION SCHEDULE: The document which identifies those records and records series that are classified as vital and specifies the means for the protection of those records. The document that provides each department with a complete listing of all vital records for which the department is responsible. NOTE: This information is normally listed within a regular records retention schedule in California State government.

WAN: See WIDE AREA NETWORK.

WIDE AREA NETWORK (WAN): A system for linking together computers, terminals, printers, and other equipment that are located in extensively separated offices and buildings.

WORD PROCESSING: Creating and modifying text documents by using a computer.

WORM: Write once, read many times.

APPENDIX 2 - STATUTORY AND OTHER REGULATORY REQUIREMENTS AND INFORMATON RELATED TO ELECTRONIC RECORDS

The State Records Management Act

The concern and management for records in California State government began with the establishment of the State Archives in 1850 under the Secretary of State. Until 1963, with the passing of the State Records Management Act, bits and pieces of the function had, until then, been in various agencies, i.e., Records Centers were under the Secretary of State; approval of records destruction under the Audits Division, Department of Finance; and general records management studies and the Standards Forms Program, under Management Analysis, Department of General Services.

The State Records Management Act containing Government Codes 14740-14774, required the Director of the Department of General Services to*:* *"Establish and administer, in the executive branch of government, a records management program which will apply efficient and economical management methods to the creation, maintenance, retention, preservation, and disposal of state records."*

In passing the State Records Management Act in 1963, the Legislature was convinced of the urgent need to apply controls to the ever-increasing proliferation of the State's records collection. It was also apparent that if such a program were to be successful it must address itself to the entire spectrum of the records problem and be a comprehensive and coordinated statewide effort. Accordingly, the State Records Management Act consolidated responsibility for administration of the program within one department, the Department of General Services.

The statutory responsibilities of the Department of General Services (and of state agencies to establish efficient, economical management of California State government records are specifically mandated in the California Government Code, Chapter 5, Sections 14745, 14746 and 14750 of the State Records Management Act. Also, the Director of the Department of General Services has assigned the development, coordination, and administration of state records to the Procurement Division's, State Records Program, California Records and Information Management (CalRIM).

Section 14741. As used in this chapter "record(s)" means all paper, maps, exhibits, magnetic or paper tapes, photographic films and prints, and other documents produced, received, owned or used by an agency, regardless of media, physical form or characteristics…."

Based on this definition, electronic records used for official state business are state records and must comply with the State's Records Management Program requirements.

The state agency records management responsibilities are outlined in the California Government Code, Chapter 5, State Records, inclusive; the California State Administrative Manual (SAM), Chapter 1600, Records Management; the California Acquisition Manual (CAM), Section 4.9 (CAM), and the Specifications for Electronic Records Management Software published by CalRIM. Responsibilities include but are not limited to:

- Establish and maintain an active, continuing program for the economical and efficient management of **all** agency records.

- Conduct an inventory of **all** records holdings.

- Create a retention schedule for **all** records and submit the schedule to the CalRIM for approval.

- Identify and protect **all** vital/essential records.

- Provide legal authority for disposal of **all** records.

- Implementation of a forms management simplification and paper reduction program.

- Compliance with standards and specifications set forth as mandatory baseline functional requirements for electronic recordskeeping system application software and consider those that are optional.

NOTE: You may refer to your legislative analyst for more information on current legislation that may affect your program and your records management program. Records management requirements cover records in all formats, including electronic records.

The California Public Records Act (PRA)

The free flow of public information is fundamental to preserving individual liberties. When information is restricted, the ability to think and act independently is diminished. With this in mind, the Legislature passed the California Public Records Act in 1968. The Act details what information is available to the public and what is not.

Section 6253(a) states that public records are open to inspection at all times during the office hours of the state or local agency and every person has a right to inspect any public record, except as provided. Every agency may adopt regulations stating the procedures to be followed when making its records available in accordance with this section.

Records Subject to the Act:

- All records of public agencies are open for inspection and copying during office hours of the agency.

- "**Public Records**" includes every means of recording or communication or representation: any writing, photograph, drawing, sound or symbol, whether paper, film, magnetic media **"computer"** data or other document -- which relates to the public business, and which is prepared, owned, used, or retained by the agency.

- **Files** and any other "identifiable records" are subject to the PRA. The PRA does not require that the requestor know the precise name of the record being sought.

- **Draft Documents** are "public records" under the PRA, and must be disclosed if: (1) They are retained by the agency in the ordinary course of business and (2) the public interest in disclosure is not clearly outweighed by the public interest and withholding the draft documents

- **Private papers** belonging to an agency employee that are incidentally at the office are not "public records" unless the papers "relate to the conduct of the people's business [and are] prepared, owned, used or retained by the agency." **Computer records** and computer data are included in the definition of public records under the PRA: data are included in the definition of "records" (§6252(e)). "Nothing in this section is intended to affect the public record status of information merely because it is stored in a computer. Public records stored in a computer shall be disclosed..." Section 6254.9 BUT: Computer software developed by an agency is not a public record (§6254.9(a)).

  This means that an agency is not required to release software developed in house. If it does, the agency may "sell, lease, or license the software [at any cost] for commercial or noncommercial use."

- **Only records that already exist are covered.** The PRA does not require agencies to create a records, compilation or list for the convenience of the requester.

The aforementioned is a summary of the basic elements of the Act. To assist you with questions you may have regarding the Act, the California State Legislature has published “Your Guide to Public Information, The California Public Records Act.” You may obtain copies of the Guide by contacting the Senate Rules Committee.

The Information Practices Act (IPA) of 1977

The Legislature passed the IPA in order to insure individuals in California their right to privacy. The California Publics Records Act was modeled after the Federal Freedom of Information (FOIA) and the IPA follows the Federal Privacy Act of 1974.

The IPA took effect in 1978 and can be found in the California Civil Code beginning at Section 1798. The premise behind the Act is that personal privacy must be protected by placing constraints on state agencies which collect, maintain and disseminate information about individuals.

Unlike the California Public Records Act, the IPA only applies to information about individuals maintained by California State agencies, like the Department of Education. The law does not cover the State Legislature, the Courts, the State Compensation Insurance Fund, or local government agencies.

Other Public Access Laws That Could Affect the Proper Management of Electronic Records

The California Public Records Act and the Information Practices Act are not the only laws that control access to information. Two very important acts to be familiar with at the federal level are:

- The Freedom of Information Act (FOIA)
- The Privacy Act of 1974

Two important other state laws to be familiar with are:

- The Ralph M. Brown Act (Open Meetings Act)
- The Legislative Open Records Act

The Brown Act – The Brown Act is contained in section 54950 et seq. of the Government Code. The Brown Act is California's law guiding local public meetings. Multi-member legislative bodies of cities, counties, and special district must open their meetings to the public. This allows the citizen to know about the actions taken by local public officials. The Brown Act ensures the public's right to observe and comment upon decisions, which affect home, business, organization, and community. You may contact the Attorney General's office for any specific questions regarding open meetings.

The Legislative Open Records Act – Because records of the Legislature (i.e., the Senate, the Assembly, and their committees) are not covered by the Public Records Act and the

Information Practices Act, the Legislative Open Records Act insures that records which contain information relating to the conduct of the public's business is available to the public.

APPENDIX 3 - COMMON METHODS OF COMPUTER AND DATA SECURITY THAT CAN BE EMPLOYED TO CUSTOMIZE A SECURITY SYSTEM:

- **Risk Analysis.** Software packages are available to help quantify potential exposure to security breaches. This is a good starting point in determining your need for and development of a plan of action.

- **Access Levels.** Users can be assigned a variety of access privileges, such as read only, remote access, specific file or directory access, and ability to upload or download data from a mainframe or network database.

- **Passwords.** Passwords can be used to control access to terminals, files, records, or even fields within a record. In a password system, users must enter the appropriate password to gain access to the data for which they have been cleared. Multiple levels of passwords can provide entry to different layers of information in an agency database. The best approach is to use passwords to create a hierarchy of entry and progressively more complex entry codes, as the information becomes more sensitive.

- **Callbacks.** Callback devices prevent unauthorized access to the communications channels of a computer. Some devices require a caller to provide an identification number and hang up. After verifying the user's access rights, the device calls the user back. When combined with a password, the system requires that the correct user identification also be provided from a specific location (modem number).

- **Audit Trails.** Security software programs can audit computer use by providing a comprehensive record of all network or system activity, including who is accessing what data, when, and how often.

- **Encryption.** Data encryption is a process that "scrambles" data when it is stored or transmitted. Data so treated become unintelligible without a data "key." When the encrypted data are sent to another terminal, the required software key on the receiving end decodes the information. The use of encryption can be a complex process and should be used only for data that is highly confidential and require utmost security.

- **Data Backups**. Backing up disks will be discussed later in the Disaster Preparedness and Recovery section of this handbook as a common-sense measure to safeguard data in the event of loss through disaster. It is also important for basic computer security. Data backup is an important safeguard should an unauthorized user access and change an electronic file or document.

- **Security Levels.** Distinguishing the levels of security for records (confidential, personal, or open) is useful for determining each records series' appropriate level of protection. Access by the public to records in the custody of state agencies is covered by the Public Records Act (Government Code Section 6250 et seq.). The Public Records Act basically states that all Public Records are open to inspection at all times during the office hours of the state or local agency and every citizen has a right to inspect any public record, except as noted. It further states that every agency may adopt regulations stating the procedures to be followed when making its records available in accordance with the Act.

NOTE: Electronic records that are confidential according to the Information Practices Act (Civil Code Section 1798, et seq.) or because of federal regulations or law, such as the Privacy Act of 1974, should not be maintained on computers that can be accessed by anyone in the office.

APPENDIX 4 - CHECKLIST FOR PRE-PURCHASE CONSIDERATIONS AND REVIEWS FOR ELECTRONIC RECORSDKEEPING SYSTEMS

Requirements Analysis:

- What is it exactly that we want the new or modified system to do?
- Do we really need it?
- Will the proposal further accomplish the agency's mission?
- What advantages will it provide?
- What problems will be solved?
- Is there money budgeted for it?

Feasibility Considerations:

- Is the system we are planning or proposing within the realm of possibility?
- Have such things as space, electrical requirements, and other environmental factors been taken into consideration?
- Are the personnel available?
- What additional training will be necessary?

Cost Benefit Analysis:

- Will the cost of what we are proposing be more or less than the benefits derived?

Consideration of Equipment Alternatives:

- Does other equipment exist that could do the same or a better job at a similar or reduced cost?

Compatibility Considerations:

- Are the computers used for electronic recordskeeping able to communicate among themselves?
- Are they able to exchange and manipulate information by using the same operating system?
- Are there plans for networking some or all of the equipment?
- Is there a need to communicate between or among other pieces of similar equipment?

Disposition:

- Have provisions been made for the authorized disposition of records determined by an approved records retention schedule?

Security:

- Has adequate security been provided for the electronic records and equipment?
- Does the potential for misuse or unauthorized disclosure, modification, or destruction require this material to be afforded greater protection than other office equipment and records?

Standards:

- Does the electronic recordskeeping system being considered meet or exceed the DGS "Specifications for Electronic Records Management?"

(Source: *Electronic Recordskeeping,* U.S. General Services Administration**)**

APPENDIX 5 - ENVIRONMENTAL CHECKLIST FOR ESTABLISHING AN ELECTRONIC RECORDSKEEPING SYSTEM

- Provide reliable electrical power for the equipment processing electronic records. A dedicated power circuit may be needed for the dependable operation of the equipment. Install electrical surge protectors to counter or cope with utility power fluctuations. Establish backup power sources such as auxiliary electrical generators or battery systems, if power outages are a problem.

- Install/Decide if cooling, heating, dust, or humidity control equipment is needed at the record processing or storage sites.

- Determine if static electricity discharges are likely to cause data losses at electronic record processing or storage sites. The danger of static electricity can be minimized with antistatic sprays, carpets, or pads.

- Prohibit eating or drinking in the immediate vicinity of the records media and the processing equipment. These restrictions prevent contaminants from harming the records or equipment.

- Install fire protection systems, as needed, in electronic records processing and storage facilities.

- Determine if physical security measures, such as door locks or intrusion alarms, are needed at electronic recordskeeping sites.

- Plan for the secure offsite storage of backup copies of valuable electronic records.

- Obtain special furniture, such as printer stands or magnetic tape rack, to help provide for the effective operation of the recordskeeping system.

(Source*:* *Electronic Recordskeeping,* U.S. General Services Administration**)**

APPENDIX 6 - CARE OF DISKETTES

- Maintain storage temperatures between 50 and 120 Fahrenheit.
- Avoid disk contact with equipment generating magnetic fields, such as telephones.
- Protect disks from direct sunlight.
- Avoid using clips of any kind to attach things to floppy disk.
- Protect disks from liquids or dampness.
- Do not bend or handle roughly.
- Do not touch exposed portions of a disk.
- Do not lay metal objects on a disk.
- Use care when inserting a disk into or removing a disk from a computer's disk drive.
- Store disks vertically in a rigid container that is not vulnerable to light and dust.

(Source: *Electronic Recordskeeping,* U.S. General Services Administration**)**

APPENDIX 7 - COMMON CAUSES OF TAPE DAMAGE AND DATA LOSS

- Physical mishandling by operational personnel.

- Failure to properly label recorded tapes.

- Poor on-site maintenance.

- Failure to control the temperature and the humidity in the storage area or during use.

- Contamination, debris, and cumulative wear products in the tape pack caused by poor tape manufacturing control, operator mishandling, and defective tape transport components.

- Maladjusted or misaligned transports or other tape winding equipment that caused improper tape tensioning and winding.

- Lack of environmental cleanliness and failure to adhere to proper clean operating practices.

- Subjecting recorded tape to close-in, high-intensity magnetic fields.

- Failure to properly select and pretest tape for use in long-term storage.

- Improper preparation of tape for shipment.

- Lack of protective measures against catastrophic events, such as fire and floods.

- Failure to provide a proper tape and system maintenance schedule.

- Failure to perform visual inspection of the tape, tape reel flanges, and hubs before operation and storage.

- Failure to properly clean and evaluate tapes before using.

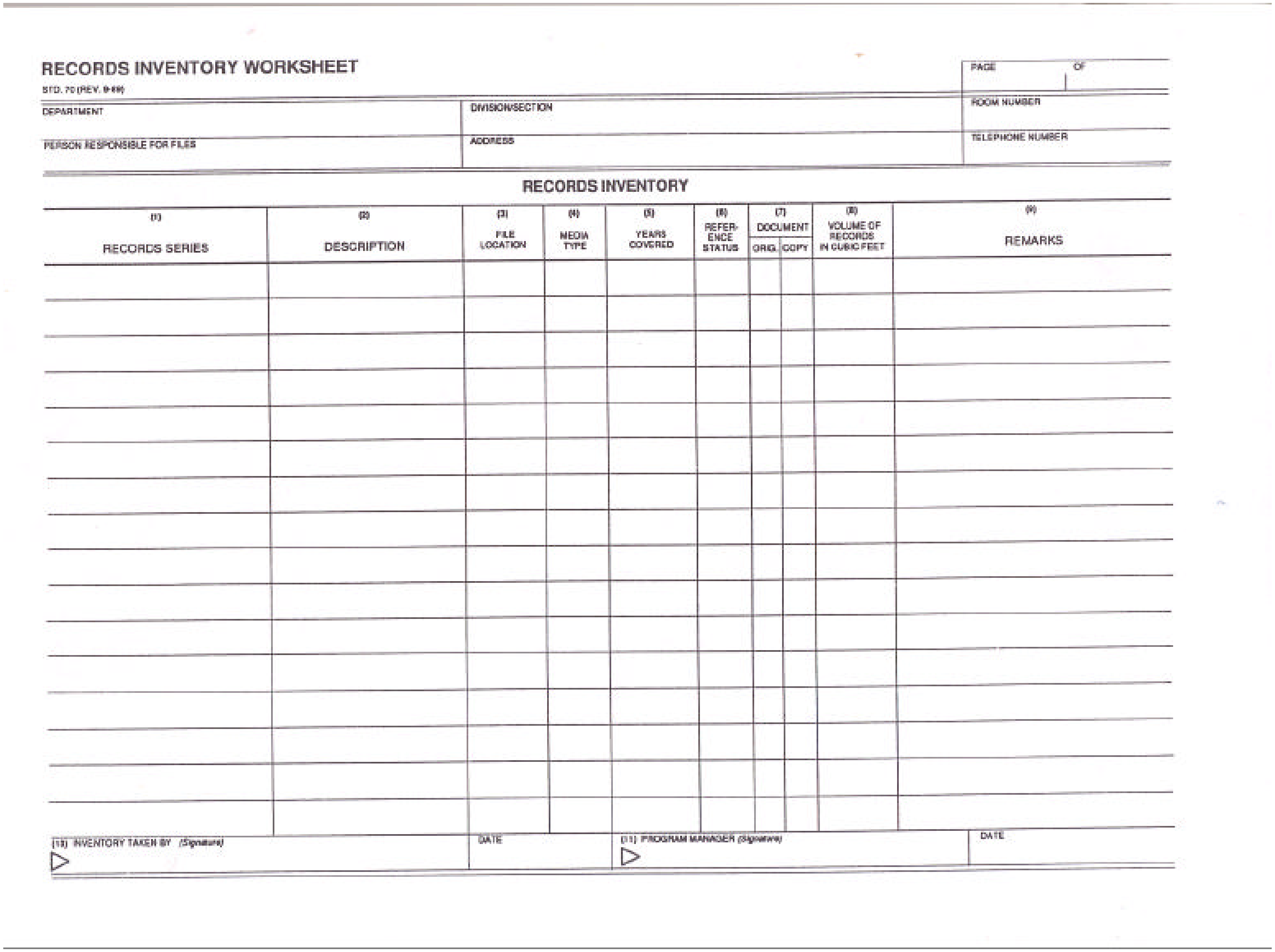
- Failure to sample three percent of holdings annually to determine condition of data and to periodically recopy older tapes.

- Failure to periodically rewind tapes at constant tension, at normal tape speed.

- Failure to copy data on the tapes to new or re-certified tapes at least once every two years or more frequently when necessary to prevent the physical loss of data or technological obsolescence of the medium.

(**Source:** Electronic Recordskeeping, U.S. General Services Administration)

APPENDIX 8 - RECORDS INVENTORY WORKSHEET, STD. FORM 70



RECORDS INVENTORY WORKSHEET

STD. 70 (REV. 9-88)

PAGE OF

DEPARTMENT

DIVISION/SECTION

ROOM NUMBER

PERSON RESPONSIBLE FOR FILES

ADDRESS

TELEPHONE NUMBER

RECORDS INVENTORY

(1) RECORDS SERIES	(2) DESCRIPTION	(3) FILE LOCATION	(4) MEDIA TYPE	(5) YEARS COVERED	(6) REFERENCE STATUS	(7) DOCUMENT		(8) VOLUME OF RECORDS IN CUBIC FEET	(9) REMARKS
						ORIG.	COPY		

(10) INVENTORY TAKEN BY *(Signature)* ▷

DATE

(11) PROGRAM MANAGER *(Signature)* ▷

DATE

APPENDIX 9 – SAMPLE RECORDS MANAGEMENT DISASTER RECOVERY PLAN

I. Name of agency:____

II. Date of completion or update of this plan:__________________________

III. Agency staff to be called in the event of a disaster:

Position	**Name**	**Telephone**
Numbers		
		(Home and Office)

Disaster recovery team:

Leader____

Members/alternates____

____

____

____

____

____

____

____

Building maintenance____

Building security____

Legal advisor____

Note below who is to call whom upon the discovery of a disaster ("telephone tree"):

____

____

IV. Emergency services to be called (if needed) in the event of a disaster:

Service **Name of Contact** **Telephone Number**

Ambulance____

Carpenters____

Chemist____

Data processing backup_______________________________

Electrician____

Emergency management coordinator_____________________

Exterminator____

Fire department____

Food services____

Locksmith____

Micrographics Contractor______________________________
____

Plumber____

Police department______________________________________

Security personnel (extra)______________________________

Software Contractor____________________________________

Temporary personnel___________________________________

Utility companies: Electric________________________________

Gas_____________________________________

Water___________________________________

Other individuals and/or organizations to assist in cleanup_______________
____

RECORDS MANAGEMENT DISASTER RECOVERY PLAN

V. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):

Batteries____

Badges (employee identification)_______________________________________

Camera and film____

Cut-off switches and valves____

Electric____

Gas____

Water____

Sprinkler system (if separate)____

Extension cords (heavy-duty)____

Fire extinguishers____

First aid kits____

Flashlights____

Ladders____

Mops, sponges, buckets, and brooms_____________________________________

Nylon monofilament____

Packaging tape and string____

Paper clips (non-rust)____

Paper towels (not colored)____

Pencils/waterproof ballpoint pens______________________________________

Plastic trash bags____

Rubber gloves____

Scissors____

V. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):

Transistor radio (battery powered)______________________________________

Wiping cloths____

Writing tablets____

VI. Sources of off-site equipment and supplies (if maintained on-site, note location):

Item Number **Contact/Company** **Telephone**

CB radio____

Dehumidifiers____

Drying space____

Dust masks____

Fans____

Forklift____

Freezer or wax paper____

Freezer space____

Fungicides____

Generator (portable)____

Hard hats____

Pallets____

Plastic milk crates____

Plastic sheeting (heavy)____

Pumps (submersion)____

Rubber boots or overshoes____

Refrigeration truck____

VI. Sources of off-site equipment and supplies (if maintained on-site, note location):

Item Number	**Contact/Company**	**Telephone**

Safety glasses____

Spot lights____

Trash cans (plastic, small and large)_____________________________________

Plastic trash bags____

Unprinted newsprint____

Vacuum/freeze drying facilities_______________________________________

Waterproof clothing____

Wet-dry vacuum____

Worktables and chairs____ ______

Computer equipment____

VII. Salvage priority list:

Attach a copy of the records retention schedule identifying all vital (essential) records series. The location and record medium of the preservation duplicate for each vital records series should be noted.

It is also very helpful if other records series are reviewed to determine their priority for salvage should a disaster occur. The following questions can be helpful in determining priorities:

- Can the records be replaced? At what cost?
- Would the cost of replacement be less or more than restoration of the records?
- How important are the records to the agency?
- Are the records duplicated elsewhere?

To simplify this process, priorities may be assigned as follows:

- Salvage at all costs, for example, records that are historically valuable or non-vital records that are important to agency operations and very difficult to recreate.

- Salvage if time and resources permit, for example, records that are less important to the agency or somewhat easier to recreate.

- Dispose of as part of general cleanup, for example, records that do not need to be salvaged because they are convenience copies and the record copy is at another location.

VIII. Agency disaster recovery procedures:

Attach a list of specific procedures to be followed in the event of a disaster in your agency, including responsibilities of in-house recovery team members.

IX. Follow-up assessment:

A written report, including photographs, should be prepared after recovery and attached to a copy of the disaster plan. The report should note the effectiveness of the plan, and should include an evaluation of the sources of supplies and equipment, and of any off-site facilities used.

(Adapted from: Basic Guidelines for Disaster Planning in the State of Oklahoma**)**

APPENDIX 10 - INFORMATION ON OTHER RECORDS MANAGEMENT APPLICATONS AND THEIR APPROPRIATE USE

Automated recordskeeping systems have been developed which use databases for specialized records management functions. These include but are not limited to:

- Electronic Document Imaging (EDI)
- Enterprise Report Management (ERM)
- Computer-Assisted Retrieval (CAR)
- Scan On Demand Document Conversion Systems
- Records Center Management Systems

Electronic Document Imaging (EDI)

Electronic Document Imaging (EDI) is a technology designed to provide for the storage and retrieval of all bitmapped documents, regardless of format, though most often a group four (compression) tiff (tagged information file format). Tiff files have become a standard primarily due to their loss-less attributes. That is, the bitmap is an accurate map of the pixels as compared to jpeg, etc. Storage and retrieval approaches have often included various aspects of "hierarchical storage management" (HSM) and database strategies for scaleable (expandable from a few users to the entire organization) document imaging solutions.

HSM software works with document imaging to manage equipment-storing images on multiple optical disks (in a "jukebox" like device). As hard drive costs have plummeted jukeboxes are less in demand and HSM software is also in less demand.

Image backups are made on various media, however, CD ROMs and other optical media are currently **favored for their stability**. Estimates of their storage reliability range from fifteen to one hundred years, though thirty to fifty years is considered by most to be reliable and is discussed in further detail in the Care of Storage Media section of this publication. Electronic Recordskeeping Systems (ERS) utilize EDI as a records repository resource.

Computer-Assisted Retrieval (CAR)

Broadly defined, the phrase computer-assisted retrieval (CAR) denotes an automated document storage and retrieval technology that uses computer hardware and software to index and locate documents or document images recorded on any media. CAR systems use database management software to create, maintain, retrieve and manipulate machine-readable records that contain index information accompanied by pointers to document locations. At retrieval time, the index is searched to determine the existence and storage locations of documents related to specific information needs.

While computer-assisted retrieval concepts can be applied to paper documents and to document images recorded on magnetic or optical media, the most common use of CAR in State government is with systems that utilize microforms for document storage. This use of computer-assisted retrieval combines the space savings and other advantages of microform storage with the ability of computers to rapidly manipulate index information. From the computer standpoint, the CAR approach simplifies data entry and on-line storage by limiting those activities to index data rather than entire documents.

A microform-based computer-assisted retrieval system includes computer and micrographic subsystems. A CAR system's computer components support the entry, maintenance, and processing of index records that are linked to document images stored by the micrographic subsystem.

The computer system includes a central processor, a display unit with keyboard, and sufficient magnetic disk capacity for on-line storage of data base records, supporting files, and CAR software.

Optional hardware components include a printer and telecommunication links to other computer systems. Computer configurations will vary with application characteristics.

Scan on Demand Document Conversion Systems

Electronic recordskeeping systems manage all types of documents that constitute a specific record. This may include paper or microfilm left in their original form. Depending upon an organization’s business requirements, it may not be necessary to have all documents available to the system in electronic format. Time or other constraints may prohibit the immediate conversion to electronic format. Scan on demand allows conversion at or near the time the system becomes operational.

When the need for an electronic copy arises, the electronic recordskeeping system can incorporate a “scan on demand” methodology that can provide a document upon request. This can be initiated by a simple e-mail message or be part of a more complex rule based electronic workflow. The key to utilizing this approach is a thorough understanding of the underlying business need, which can result in a dramatic cost reduction associated with document conversion.

Enterprise Report Management (ERM)

Enterprise Report Management (ERM), previously known as Computer Output to Laser Disk or COLD, is an integrated software and hardware solution that captures, stores and indexes formatted computer output (pages) on optical disks, magnetic disk, or magnetic tape as an alternative to paper printouts or computer-output-to-microfilm (COM).

Fields on any ERM report can be used to create indexes for quick retrieval. Print output files are stored in their native “raw” format--not converted into a raster file--and compressed to reduce storage space requirements. Any individual with proper security privileges can access the data.

The type of data that ERM technology is typically concerned with is the result of transactions (data files and database records) being formatted by the application into page-oriented form for printing on paper or computer output to microfiche (COM). The data focuses on a particular time period and the output has a specific, known structure and format.

The ERM process mainly involves two procedures: recording (indexing and storing the data) and retrieving (making the data available to users). However, there are other complex tasks that need to be addressed. Data must be downloaded or transferred to the ERM server before it can be processed; and the method of transfer from the mainframe/host system to the ERM subsystem depends on the communications capability in place.

The ERM systems have the capability to deliver productivity and customer service benefits with a minimum level of disruption to existing operations.

- New reports can be created from existing (standard) legacy reports without programming. **Benefit:** significant time and cost savings in responding to user needs.

- A common application server is created which stores document output from heterogeneous computer systems in a standard format. **Benefit:** a “middleware” server providing both internal client and web to legacy data access from many different computer systems.

- Outbound documents such as statements and invoices can be stored for access by customers on a self-service basis. **Benefit:** reduction of call center staffing requirements and improved service levels.

Records Center Management Systems

In a computer-based records center management system, the computer is used to manage data concerning existing records location and retention; without altering the format or storage of the records. Records center management system software tracks records throughout the life cycle, provides appropriate reports, and allows queries of records. However, this type of software has not been designed to be a fully functional electronic recordskeeping system as defined by the DGS "Specifications for Electronic Records Management Software."

An efficient records center management system should be able to accurately describe the status of records in the record center in terms of their location and characteristics. The system also contains action prompts that tell when to purge, transfer, and alter the status of records. To fulfill these requirements, the system should be capable of producing routine system reports, such as:

- Records by retention status.
- Records by type (vital, active, inactive, and archival).
- Records by location.
- Records by confidentiality designation.
- Records to be moved.
- Records update.
- Equipment location.

This type of software can help an agency to locate, retrieve, and share files in central and decentralized locations. The computerized master index for records brings together information on each file as well as on files in every location, provides faster retrieval time, facilitates accurate maintenance of statistics on activity rates, and enables better records management planning.

Some of the functions that records center management systems perform are keyword indexing/searches, records location management, records retrieval assistance, automated file label creation (with bar codes), retention schedule maintenance, records inventory, box/file/record tracking, and destruction notifications. This software typically utilizes bar codes (label printing and bar code reader support) for tracking the locations and actions related to a specific file.

APPENDIX 11 - OVERVIEW OF THE UNIFORM ELECTRONIC TRANSACTIONS (UETA) ACT

As of the date of this Handbook, five states (California, Pennsylvania, Indiana, South Dakota, Utah) have adopted a uniform electronic commerce law: the Uniform Electronic Transactions Act (UETA). Governor Ridge of Pennsylvania signed UETA into law December 16, 1999, and it became effective January 15, 2000. Although California had previously adopted UETA, its version has 76 amendments that may result in substantial non-uniformity. States are adopting UETA at a fast pace, UETA awaits the governors signature in Kentucky and will likely pass soon in Virginia. UETA promises to simplify divergent forms of e-Commerce laws that nearly 40 states had previously adopted. States slow to act may see federal law imposed on them until UETA is adopted, S.761 and/or HR.1714 may emerge from the 106th Congress to preempt other state e-Commerce laws.

Uniform laws like UETA are developed by the American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Laws (NCCUSL). Uniformity is widely considered to be a significant factor that promotes commerce through national certainty. For example, the Uniform Commercial Code (UCC) governs commercial law in all 50 states. This cooperative uniformity has permitted the states to retain considerable self-governance and preserve many benefits of federalism.

UETA enables business and government to agree to use electronic forms of records, signatures, acknowledgments and notarization. It is more procedural than substantive, a perspective dramatized by this caricature: “the medium shall not be the message.” UETA requires no standard or particular form of electronic transaction. Instead, UETA validates the use of electronic means where traditional paper documents and signatures were previously required.

UETA also authorizes the use of electronic agents. Electronic forms of various traditionally paper-based negotiable instruments are also enabled, including notes, bills of lading, warehouse receipts and documents of title. UETA does not apply to some classes of documents, such as wills, codicils and testamentary trusts, nor to the most common negotiable documents such as checks, drafts, letters of credit and investment securities. Nevertheless, the experience of UETA should influence how negotiable instruments eventually migrate to electronic form. UETA does not alter many states’ consumer protections, such as requirements for written or mailed notices. At this time, it appears that UETA and its companion proposal, the Uniform Computer Information Transactions Act (UCITA, enacted by Virginia in March 2000), will be the most important Cyberlaws for many business persons. For a section by section analysis of UETA Provisions, you may refer to the UETA web site and click to see the UETA chart.

Impact of UETA

UETA's impact will be felt most immediately on attorneys practicing in states having enacted or soon to enact UETA. Knowledge of UETA will directly impact attorneys in transactional practices and in representing business clients located in UETA states. Clients in other states may also be impacted if they do business with counter-parties in UETA states. Knowledge of UETA is important to businesses, which create, process and accept paper-based contracts but seek to convert to electronic forms of these documents. Understanding of UETA is needed for persons proposing to use electronic records and who are doing business or government activities in states where UETA applies. Knowledge of UETA may also be important to counsel and clients evaluating transactions that include choice of law or choice of forum provisions that either directly elect UETA or choose the law of a particular state that has enacted UETA. State regulatory agencies must determine how and to what extent UETA will be implemented. For example, the PA Office of Administration is charged to promote consistency and interoperability among PA agencies and with other states and the federal government.

Overview of UETA's Provisions

UETA establishes several new terms of commercial practice and thereby expands traditional contracting concepts to work in the digital age. A record is information inscribed in a tangible medium or stored and retrievable in perceivable form; an electronic record is a record that is created, generated, sent, communicated, or received by electronic means. Information means data, text, images, sounds, codes, computer programs, software, databases, etc. An electronic signature is an electronic sound, symbol, or process attached to or logically associated with a record with the intent to sign the record. An electronic agent is an automated means (machine, computer program), essentially a tool that independently initiates action or response to electronic records or performances, without human intervention. Eventually, electronic agents may develop artificial intelligence enabling autonomous action. Electronic agents may form automated transactions, these are contracts formed without human intervention. Automated transactions may also be formed with interaction between a human and an electronic agent.

UETA permits but does not require electronic contracting, that is, parties must agree to use electronic records and electronic signatures rather than their written counterparts. When parties agree to transact electronically, their records, signatures and contracts must be enforced if made in electronic form. this means that electronic records and electronic signatures will satisfy requirements under other laws that require signatures and writings. UETA must be applied to facilitate electronic transactions and it must be construed consistent with reasonable commercial practice and promote uniformity among the states. UETA applies only prospectively, that is to transactions using electronic records or electronic signatures that are created, generated, sent, communicated, received, or stored after the adopting legislation becomes effective.

Electronic Records and Electronic Signatures

The centerpiece of UETA is §7, which validates the use of electronic records and signatures. Electronic records satisfy requirements for writings so that the enforceability of a record or signature cannot be denied simply because it is electronic form. Electronic records must still satisfy any other formal requirements, such as notices, disclosures or completeness of terms. For example, if the parties' e-mails show agreement on the sale of widgets, these electronic records would still need a quantity term to create a valid contract. Electronic records and signatures simply satisfy requirements under existing law, such as the statute of frauds that require documents be in signed writings.

Legal requirements to provide information in writing are satisfied with an electronic record if it is capable of retention (printing & storing) by recipient when received. UETA makes electronic records the equivalent of writings but does not alter other substantive requirements of contract law. Many other laws have specific requirements for the posting, display, communication or transmittal of records, usually a physical, printed form is required. While UETA validates electronic records, it does not override these existing legal requirements under other laws mandating particular methods of posting, sending or formatting records. For example, eviction notices generally must be posted where the tenant is most likely to see it, right on the front door of the dwelling. Even if the landlord and tenant agree to electronic transactions, UETA cannot override property law requirements for physical posting of eviction notices.

Many Internet users encounter frustration when important information cannot be saved or printed after downloading from a website. UETA requires that electronic records must be capable of retention by the recipient. If the sender inhibits the recipient from printing or storing the electronic record, the electronic record is not effective.

Electronic transactions pose different security problems than under traditional practices using printed documents or voice telephone conversations. Electronic information is vulnerable to corruption by electronic interference or intentional forgery by hackers. UETA authorizes the use and innovation in security procedures (e.g., encryption) to verify the identity of the sender. UETA makes an electronic record or electronic signature attributable to a particular sender if it was the act of that person. This can be shown in any manner from the context & surrounding circumstances, such as an effective security procedure.

UETA's recognition of electronic signatures differs somewhat from digital signature law and practice, the latter focuses on security and encryption. By contrast, UETA simply permits the substitution of an electronic sound, symbol, or process when the law requires a physical signature if it is attached to or logically associated with a record and used with the intent to sign the record. Electronic signatures may take many forms, including PIN, password, server identification, biometrics, clickwrap using the "I Agree" button or some form of encryption.

Changes and Errors in Electronic Transmissions

Electronic transmissions can be prone to ***errors*** caused by individual users and sometimes are prone to ***changes*** caused by electronic computers or during communication. UETA encourages the use of security procedures to detect and correct changes or errors. In §10, UETA provides that if one party fails to use a security procedure that both parties had previously agreed to use, the conforming party may avoid the change or error if the security procedure would have discovered it and permitted its correction. Other types of changes or errors are resolved by existing contract law under the doctrine of mistake. In an automated transaction with an individual, the party using an electronic agent must give the individual an opportunity to prevent or correct the error. For example, consider an individual who strikes the numeric key "1" to order a single copy of a book from an online bookseller but the "1" key sticks causing "111" to be sent. In such a situation, the electronic agent facility of the online bookseller must send a confirmation screen permitting the individual to review the quantity ordered. This confirmation might be as simple as a box saying "You ordered 111 books, click yes if this is this correct." Without this or some other security procedure, the individual may avoid the contract for the quantity of 111 books.

Restitution is usually required to unwind a mistaken transaction. If UETA gives one party a right to rescind a mistaken transaction, any consideration already received must be either returned, destroyed or follow instructions from the other party. However, a party may be prohibited from rescinding if the consideration was already received and used. For example, it may be impossible not to have use information after it is revealed, information is the consideration received. Once information is received and understood it may be impossible to avoid using or receiving its value and this situation limits the right to avoid the error or change.

Retention of Electronic Records

There are many laws that require various documents be saved as evidence for future use. UETA §12 permits the retention or presentation of electronic records to satisfy these retention requirements if the information accurately reflects the original and it remains accessible for future reference. Accessibility of electronic records becomes problematic over time. Obsolete computer systems become incompatible, accessible only by data recovery experts. Floppy disks are not stable over time and conversion between systems is time consuming and expensive. Nevertheless, electronic records must remain accessible to satisfy legal requirements for retention of electronic records. For example, if a law requires retention of a check, that requirement is satisfied by electronic retention of all information on the front and back of the check. Unless there is a requirement to the contrary, written documents can be discarded once transferred to electronic form.

Automated Transactions

UETA facilitates contracts formed without human intervention or those formed with interaction between a human and an electronic agent. Machines may act as electronic agents and can form contracts. Although human intent is required for contract formation, the use of machines is not fatal because the necessary intent is found in the programming and use of the machine. For example, an anonymous click-through on-line could be effective to create a contract. There are two different scenarios. First, an individual acquires access to a website and uses the information without identifying herself - a legal relationship is not created. By contrast, if the website clearly indicates the information is proprietary and may be used only for certain purposes to which the individual agrees by clicking, a legal relationship would arise.

Sending and Receipt of Electronic Records

The law often requires an inquiry into the time or place that a document is sent or received. For example, the mailbox rule holds a contract is created when the acceptance is dispatched and the UCC requires some notices be delivered to a party's place of business. Electronic records are considered sent when: (1) properly addressed to a system designated by the recipient, (2) are in a form capable of processing by the recipient's system, (3) the information enters a system outside the sender (or sender's agent's) system. Receipt occurs when the record reaches the recipient's designated system & is capable of processing by that system. It is not necessary for the individual recipient to have notice of its receipt. This is similar to the rule that designates it as receipt when the recipient of traditional mail, who never reads a notice but has it in hand, is bound by the receipt. General broadcast messages that are sent to systems rather than individuals are not considered a sending. The key element is whether the sender/recipient has control. UETA §15 does not address proof of time of receipt. In the situation of multiple email addresses, the recipient can designate the e-mail address to be used. When the precise location is an issue, for example in conflict of laws issues, or tax issues, the location is that of the sender or recipient, not the location of information system.

Transferable Records

UETA facilitates electronic negotiable documents but only in the limited areas of the electronic equivalent of paper promissory notes and paper documents of title if issuer of the electronic record agrees that the electronic record should also be an electronic transferable record. UETA does not apply to checks, drafts, investment securities or letters of credit, which may be developed in the future but the banking system is not yet ready for these documents to "go electronic" under UETA.

UETA creates the concept of "control" over an electronic record, which should be the equivalent of "possession" traditionally used in the paper context. Systems must be in place to ensure that the transfer of the record is done in such a manner that there is only one "holder" of the record. The transferable record must remain unique, identifiable and unalterable.

APPENDIX 12 - THE WORLD-WIDE WEB

The World Wide Web

The World Wide Web, (WWW) is a universe of information. The web's existence relies on global networks. The web allows human communication and cooperation by sharing knowledge, and opens this to ordinary people who need no technical skills. By pointing and clicking, just about anyone can find their way through, and even contribute to, this growing base of information that is stored on servers worldwide.

First designed at the physics laboratory, CERN, in 1989, the WWW has spread exponentially, doubling every few months. During 1993 this explosion of available information broke into public awareness. Commercial, educational and government bodies are all rushing to become Web enabled.

Meanwhile, the designers at CERN, and in the many laboratories around the world, who develop web-related code in informal collaboration, have been relying on CERN for coordination, and direction. CERN's charter, however, is for particle physics research, which precludes CERN from funding technology of such a wide application. Companies that are becoming increasingly committed to the web as a way of working and doing business are calling for a central body to define the web, ensure its stability and smooth progression through continued technological innovation.

Tim Berners-Lee

The World Wide Web was really created by Mr. Tim Berners-Lee. In 1989, while he was working at the European Particle Physics Laboratory, he proposed that a global hypertext space be created in which any network-accessible information could be refered to by a single "Universal Document Identifier". In 1990 he proposed that servers be connected together using the available telephone lines. His intention was to permit communications within the High Energy Physics community at first, and to other communities in the summer of 1991.

Between the summers of 1991 and 1994, the load on the first Web server ("info.cern.ch") rose steadily by a factor of 10 each year. In 1992 academia, and in 1993 industry, was taking notice. Mr. Berners-Lee was under pressure to define the future evolution. After much discussion he decided to form the World Wide Web Consortium in September 1994, with a base at MIT in the USA, INRIA in France, and now also at Keio University in Japan. The Consortium is a neutral open forum where companies and organizations to whom the future of the Web is important come to discuss and to agree on new common computer protocols.

The Internet became a part of the World Wide Web when it became apparent that the type and amount of traffic on the Web needed be categorized into separate user communities. The scientific and academic communities were separated from the military and consumer communities. The various communities were formed into what we know today as internets. Each net of users could intercommunicate without interrupting the other nets of users. The control of these communities was given over to the WWW Consortium, who would go on to define the boundaries, parameters and standards governing the WWW.

Aims

The aims of the consortium are as follows:

- To define the World-Wide Web
- To act as a primary point of contact for those expressing interest in the web
- To coordinate the development of the communication standards (network protocols, etc) on which the web is based;
- To ensure that current trends in research are taken into account
- To support, develop and collect public domain software to act as reference implementation of these protocols, etc;
- To promote the use of the web in new domains, especially within education, and interchange between governments, research, and industry.
- To aid especially the less technically developed countries in using the web for the rapid transfer of knowledge, diffusion of culture and as an economic enabler;

Activities

In order to accomplish these aims, the consortium shall manage and support (directly or through subcontract):

- The exchange of information with the public, the press and members, about web-related activities.
- The coordination of technological innovation. Ensure that fragmentation of standards does not occur, and that enhancements will have the required properties of compatibility and scalability, and will represent the leading edge of technology in the field. Define compliance with standards. Act as liaison with general standard bodies.
- The development of specific enhancements to protocols and reference software in response to requests from contributing members. Maintain registries of servers, of organizations providing web-related services, and of web-compatible products.

Technical design is coordinated by the consortium, but decisions will be made by rough consensus among participants in open discussions taking place over the networks and, when deemed appropriate, at physical meetings. The board of the consortium, and if necessary, the president will rule in the case of arbitrary decisisions, or impasse.

APPENDIX 13 - MEDIA STANDARDS

Section 1: ANSI/AIIM Standards, Technical Reports, and Guidelines (4/2000)

ANSI/AIIM MS52-1991 - *Recommended Practice for the Requirements and Characteristics of Original Documents Intended for Optical Scanning*
ANSI/AIIM MS53-1993 - *Recommended Practice; File Format for Storage and Exchange of Image; Bi-Level Image File Format: Part 1*
ANSI/AIIM MS54-1993 (R1999) – *Symbols for Various Functions of Document Handling Equipment*
ANSI/AIIM MS55-1994 - *Recommended Practice for the Identification and Indexing of Page Components (Zones) for Automated Processing in an Electronic Image Management (EIM) Environment*
ANSI/AIIM MS58-1996 - *Standard Recommended Practice for Implementation of Small Computer Systems Interface (SCSI-2) (X3.131-1994)*
ANSI/AIIM MS59-1996 - *Media Error Monitoring and Reporting Techniques for Verification of Stored Data on Optical Digital Data Disks*
ANSI/AIIM MS60-1996 - *Electronic Folder Interchange Datastream*
ANSI/AIIM MS61-1996 - *Application Programming Interface (API) for Scanners in Document Imaging Systems*
ANSI/AIIM MS66-1999 - *Metadata for Interchange of Files on Sequential Storage Media Between File Storage Management Systems (FSMSs)*
ANSI/AIIM TR1-1988 (A1992) – *Guidelines for Metrics*
ANSI/AIIM TR2-1998 – *Glossary of Document Technologies*
ANSI/AIIM TR15-1997– *Planning Considerations, Addressing Preparation of Documents for Image Capture*
ANSI/AIIM TR17-1989 – *Facsimile and Its Role in Electronic Imaging*
ANSI/AIIM TR19-1993 – *Electronic Imaging Display Devices*
ANSI/AIIM TR21-1991 – *Recommendations for the Identifying Information to be Placed on Write-Once-Read-Many (WORM) and Rewritable Optical Disk (OD) Cartridge Label(s) and Optical Disk Cartridge Packaging (Shipping Containers)*
ANSI/AIIM TR25-1995 – *The Use of Optical Disks for Public Records*
ANSI/AIIM TR26-1993 – *Resolution as it Relates to Photographic and Electronic Imaging*
ANSI/AIIM TR27-1996 – *Electronic Imaging Request for Proposal (RFP) Guidelines*
ANSI/AIIM TR28-1991 – *The Expungement of Information Recorded on Optical Write-Once-Read-Many (WORM) Systems*
ANSI/AIIM TR29-1993 – *Electronic Imaging Output Printers*
ANSI/AIIM TR31:1-1992 – *Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems Part 1: Evidence*

ANSI/AIIM TR31:2-1993 – *Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems Part 2: Acceptance by Government Agencies*

ANSI/AIIM TR31:3-1994 – *Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems Part 3: Implementation*

ANSI/AIIM TR31:4-1994 – *Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems Part 4: Model Act and Rule*

ANSI/AIIM TR32-1994 – *Paper Forms Design Optimization for Electronic Image Management (EIM)*

ANSI/AIIM TR33-1998 – *Selecting an Appropriate Image Compression Method to Match User Requir*ements

ANSI/AIIM TR34-1996 – *Sampling Procedures for Inspection by Attributes of Images in Electronic Image*

Management (EIM) and Micrographics Systems

ANSI/AIIM TR35-1995 – *Human and Organizational Issues for Successful EIM System Implementation*

ANSI/AIIM TR38-1996 – *Compilation of Test Target for Document Imaging Systems*

ANSI/AIIM TR39-1996 – *Guidelines for the Use of Media Error Monitoring and Reporting Techniques for the Verification of Information Stored on Optical Digital Data Disks*

ANSI/AIIM TR40-1995 – *Suggested Index Fields for Documents in Electronic Image (EIM) Environments*

Section 2: ANSI/ISO Standards

ISO 10089 - *Rewritable 130 mm Magneto-Optical*
ISO 10090 - *Rewritable 90 mm Optical Disk.*
ISO 10149 - *Information Technology - Data Interchange on Read-Only 120 mm Optical Data Discs*
ISO 10922 - *Recommendations for Identifying Information on Optical Disk Package Labels.*
ISO 11560 - *Magneto-Optical Recorded WORM.*
ANSI X3.213 *86 mm Rewritable Optical Disk Cartridge Using the Discrete Block Format (DBF) Method.*
ISO/IEC 10090 *90 mm optical disk cartridge rewritable and read only for information interchange.*
ISO/IEC 9171-1 *130 mm optical disk cartridge, write once, for information interchange - Part 1: unrecorded optical disk cartridge.*
ISO/IEC 9171-2 *130 mm optical disk cartridge, write once, for information interchange - Part 2: Recording format.*
ISO/IEC 10089 *130 mm rewritable optical disk cartridge for information interchange.*
ISO/IEC 11560 *130 mm rewritable optical disk cartridge write-once, using the magneto-optical effect for information interchange.*
ANSI X3B11/91-120 *WORM application using MO media*
ISO/IEC DIS 13481 Data interchange on 130 mm optical disk cartridges - Capacity: 1 gigabyte per *cartridge.*
ANSI X3.211-1992 *130 mm Write-Once Optical Disk Cartridge using Continuous Composite Serve, RLL 2,7 Encoding and LDC.*
ANSI X3.212-1992 *130 mm Optical Disk Cartridge Using the Magneto-Optical Effect and Continuous Composite Servo Forma*t.
ANSI X3.214-1992 *130 mm Write-Once Optical Disk Cartridge Using Sampled Servo and 4/15 Modulation.*
ANSI X3.220-1992 *Digital Information Interchange - 130 mm Optical Disk Cartridge Using the Magneto-Optical Effect for Write-Once Functionality.*
ANSI X3.191-1991 *Recorded Optical Media Unit for Digital Information Interchange - 130 mm Write-Once Sampled Servo RZ Selectable-Pitch Optical Disk Cartridge.*
ISO/IEC JTC1 *Information Interchange on 300 mm Optical Disk Cartridges of the Write Once, Read Multiple (WORM) Using the CCS Method.*
ISO/IEC 10885 *356 mm optical disk cartridge for information interchange - write once.*
ANSI X3.200-1992 *356 mm Write Once Optical Disk Cartridge for Information Interchange.*
ANSI X3.191-1991 -*Recorded, Unrecorded Characteristics of 130 mm Optical Disk Cartridges Using Sampled Servo and RZ Modulation.*
ANSI X3.200-1992 - *Unrecorded and Recorded Characteristics of 130 mm Optical Disk Cartridges of the WORM Type Using the Magneto-optic Effect.*

ANSI X3.200-1992 – *Recorded and Unrecorded Characteristics of 356 mm (14-inch) Optical Disk Cartridges.*

ANSI X3.211-1992 –*Recorded, Unrecorded Characteristics of 130 mm Optical Disk Cartridges Using Continuous Composite Servo, RLL 2, 7 Modulation and LDC Error Correction.*

ANSI X3.212-1992 – *Recorded and Unrecorded Characteristics of 130 mm Magneto-optic Rewritable Media.*

ANSI X3.213-1992 –*Unrecorded and Recorded Characteristics of 86 mm Rewritable, Read-Only Optical Disk Cartridges Using the Discrete Block Format (DBF).*

ANSI X3.214-1992– *Recorded, Unrecorded Characteristics of 130 mm Optical Disk Cartridges Using Sampled Servo and 4/15 Modulation.*

ISO 9171/1 – *130 mm (5.25-inch) Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Unrecorded Optical Disk Cartridge.*

ISO 9171/2– *130 mm (5.25-inch) Optical Disk Cartridge, Write Once, for Information Interchange, Part 2: Recording Format.*

ISO 12024 – *Permanence of Information Recorded on CD-ROM.*

ISO 12037 – *Recommended Practice for the Expungement, Deletion, Correction or Amendment of Records on Optical Write-Once-Read-Many (WORM) Systems. .*

ISO/IEC 13346 – *Volume and File Structures for Optical Media.*

ELECTRONIC RECORDS MANAGEMENT HANDBOOK

(The Great Seal of the State of California)

Gray Davis
Governor
STATE OF CALIFORNIA

Aileen Adams
Secretary
STATE AND CONSUMER SERVICES AGENCY

Barry D. Keene
Director
DEPARTMENT OF GENERAL SERVICES