

DATE: March 11, 1998

TO: DIRECTIVES POINTS OF CONTACT

FROM: HOWARD LANDON /s/
OFFICE OF INFORMATION, RESOURCES AND RECORDS
MANAGEMENT (HR-41)

SUBJECT: DOE G 241.X-1, ELECTRONIC RECORDS MANAGEMENT GUIDE for Use
with 36 CFR Chapter XII - Part 1234

The attached revised Guide, developed by the Office of Information Management (HR-4), is being forwarded for review and comment by your organization. Its purpose is to provide guidance to assist in the implementation of 36 CFR - Part 1234, Electronic Records Management. The revision updates and formally brings into the Directives System guidance that had previously been circulated within the Department's records management community.

Comments on the proposed revision are due by **April 11, 1998**. MAJOR ISSUES and SUGGESTED COMMENTS should be designated as such when submitted. MAJOR ISSUES shall be limited to instances where the directive in its entirety, or one or more of its requirements, would have an adverse effect on DOE policy objectives, mission accomplishment, economy, efficiency, or other management concerns that would preclude its publication. The following procedures shall be followed for the submission of comments:

Headquarters and Field Elements:

Submit comments to Howard Landon, by mail to HR-41, Room 8F-084, FORRESTAL; by facsimile to (202) 586-1972; or by e-mail to howard.landon@hq.doe.gov.

If there are any questions concerning the content of the draft DOE G 241.X-1, contact Mr. Landon at (202) 586-6344. Contact Ms. Gail Cephas at (202) 586-1049 for questions pertaining to the Directives System or the processing of this draft directive.

Attachment

**ELECTRONIC RECORDS
MANAGEMENT GUIDE
FOR USE WITH
36 CFR CHAPTER XII - PART 1234**



U.S. DEPARTMENT OF ENERGY
Deputy Assistant Secretary for Human Resources

Distribution:
All Departmental Elements

Initiated By:
Office of Human Resources and
Administration

ELECTRONIC RECORDS MANAGEMENT

1. **PURPOSE.** This Guide implements 36 Code of Federal Regulations (CFR) Part 1234, “Electronic Records Management,” and provides non-mandatory guidance for the organization, maintenance, and disposition of electronic records. These regulatory requirements may not be disregarded because of any omission, or explanation provided in this Guide. Nothing in this Guide is intended to revoke, modify, change, add, or impose new requirements not otherwise imposed by regulation.
2. **APPLICABILITY.** This Guide is intended for use by all DOE Elements (including their contractors) for electronic records maintenance and disposition.
3. **IMPLEMENTATION.** To implement this Guide, DOE Elements may discontinue electronic records systems currently in place at their respective next scheduled cutoff date. Electronic records lacking scheduled cutoff dates should have such dates established for adoption of the guidelines presented in this Guide.
4. **EXPLANATION OF CHANGES.** DOE is required to establish and maintain an electronic records scheduling program in accordance with 44 United States Code (U.S.C.) 3102, 3301, and 3303 to control the creation and disposition of records accumulated. Accordingly, records disposition schedules are under development for each series of electronic records in DOE or contractor custody. The schedules describe the various electronic records series and provide instructions for their cutoff, retirement to a Federal records center, destruction, or permanent retention. This Guide recommends procedures for the management of electronic records from their creation through their disposition.
5. **REGULATIONS.**
 - a. **Requirements.** 36 Code of Federal Regulations PART 1234, “Electronic Records Management.” contains the primary regulations imposing requirements on the Department’s electronic records. These regulatory requirements may not be disregarded because of any omission, or explanation provided in this Guide. Nothing in this Guide is intended to revoke, modify, change, add, or impose new requirements not otherwise imposed by regulation.
 - b. **Reporting.** This Guide provides information to assist in complying with regulations.

- c. Assistance. For information regarding this Guide, contact Howard Landon, (202) 586-6344.
6. CRIMINAL PENALTIES. In Title 18 U.S.C. Chapter 101, Records and Reports, Section 2071, "Concealment, Removal, or Mutilation," criminal penalties are provided for willful and unlawful concealment, removal, mutilation, obliteration, falsification, or destruction of Federal records.
7. FORMS. Use of the following forms is appropriate:
 - a. "Records Maintenance and Disposition Instructions," DOE F 1324.14 (Optional),
 - b. "Records Transmittal and Receipt" (Standard Form 135), and
 - c. "Request for Records Disposition Authority (Standard Form 115).
8. CLASSIFIED RECORDS. Approved electronic records disposition schedules are required for classified electronic records. Classified information in electronic form is a record. Classification requirements must be followed regarding any aspect of the creation, maintenance, or disposition of classified electronic records. For the security requirements and procedures affecting classified electronic records, see DOE O 471.2, INFORMATION SECURITY PROGRAM; DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL; and their accompanying contractor requirements documents.
9. TRAINING. This Guide should be of use to those interested in obtaining additional information concerning implementation of the regulatory requirements that affect electronic records management. Instructors may also find this Guide useful in supplementing other training provided in this subject matter area.
10. SUMMARY. This Guide consists of five chapters that explain and recommend systems and techniques for use in managing electronic records.

CONTENTS

CHAPTER I, OVERVIEW

1.	Purpose	I-1
2.	Authority	I-1
3.	Implementation and Management	I-1
4.	Summary	I-1
5.	References	I-1
6.	Definitions	I-2

CHAPTER II, CREATION AND RECEIPT

1.	Creation of Electronic Records	II-1
2.	Receipt of Electronic Records	II-2
3.	Authentication/approval	II-3
4.	Submission of Electronic Records	II-3

CHAPTER III, USE AND MAINTENANCE

1.	Records Storage and Maintenance	III-1
2.	Records Retrieval	III-2
3.	Records Protection	III-2
4.	Records Security	III-2
5.	Judicial Use	III-3

CHAPTER IV, DISPOSITION

1.	Inventorying Electronic Records	IV-1
2.	Applying General Records Schedules	IV-1
3.	Scheduling Records	IV-2
4.	Schedules	IV-3
5.	Disposition of Unique Electronic Records	IV-3

CHAPTER V, SPECIAL ISSUES

1.	Legal Admissibility	V-1
2.	Multiple Copies, Revisions, Drafts, and Backups	V-1
3.	Imaging Systems	V-2
4.	Quality Assurance/ Records	V-3
5.	Voice Mail	V-3
6.	Audio/Video Conferencing/Recordings	V-4
7.	Data Portability/Migration	V-4
8.	E-mail Records	V-5
9.	Electronic Record System Documentation	V-8
10.	Information Systems as Records	V-10
11.	Complex Electronic Records	V-11

ATTACHMENT 1, DISPOSITION ISSUES FOR PARTICULAR KINDS OF ELECTRONIC RECORDS	1-1
------------------------------------------------------------------------------------------	-----

CHAPTER I

OVERVIEW

1. **BACKGROUND.** Methods of creating, capturing, editing, maintaining, transmitting, retrieving, and storing Federal records are continuously changing. The result is an increase in the volume—and complexity—of electronically created and stored information. Records can now be found on a variety of electronic media—floppy disks, hard disks, network disk drives, optical disks, and magnetic tapes. Records may include text, graphics, sound recordings, or video recordings generated from a variety of software. Complex records may be composed of multiple computer files stored in multiple locations across the computing environment. The proliferation of electronic information has resulted in electronic copies of record and nonrecord material existing simultaneously on stand-alone workstations, local area networks, and computer system backup tapes.

Electronic information—and its proliferation—must be managed properly to ensure that electronic records and nonrecords are protected and retained in accordance with approved records disposition schedules. To achieve this goal, records managers should coordinate their programs with originators of electronic records, organizational administrators, program managers, and computer systems managers. The intent is to ensure that all electronic information—including drafts of documents, deleted files, and extraneous copies of records and nonrecord material—are identified and properly dispositioned. The chapters in this Guide address the creation, receipt, use, maintenance, and disposition of electronic records. This information may be useful in developing and implementing professional records management programs.

2. **AUTHORITY.**
 - a. 44 U.S.C. 3101, “Records Management by Agency Heads,” requires the head of each Federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. These records furnish the information necessary to protect the legal and financial rights of the Government and persons directly affected by the agency’s activities.
 - b. 44 U.S.C. 3102, “Establishment of Program Management,” requires the head of each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of the agency’s records.
 - c. 36 CFR Chapter XII - Subchapter B prescribes policies for Federal agencies’ records management programs relating to records creation and maintenance, adequate documentation, and proper records disposition.

- d. 36 CFR 1234, "Electronic Records Management," establishes the basic requirements related to the creation, maintenance, use, and disposition of electronic records.
3. IMPLEMENTATION AND MANAGEMENT. When developing records management programs, records managers should consider the issues and concepts presented in this Guide. Performing program assessments, conducting records inventories, and providing training courses are examples of activities that can benefit from this guidance.
 4. REFERENCES. Guidance from several Federal agencies was used in the development of this Guide. These agencies include the DOE, the National Archives and Records Administration (NARA), the General Services Administration (GSA), and the Office of Management and Budget (OMB). In addition to the references authorizing records management programs (this chapter, Paragraph 2, "Authority"), the following references provide useful information:
 - a. Title 18 U.S.C., Chapter 101, "Records and Reports," Section 2071, "Concealment, Removal, or Mutilation," provides criminal penalties regarding the misuse of Federal records.
 - b. Title 44 U.S.C 2901, "Definitions," Paragraph (2) defines records management.
 - c. 44 U.S.C. 3301, "Definition of records."
 - d. Title 44 U.S.C., Chapter 33, "Disposal of Records," Section 3303, "Lists and Schedules of Records to be Submitted to the Archivist by Head of each Government Agency," provides procedures for the proper disposition of Federal records.
 - e. 36 CFR 1228, "Disposition of Federal Records," provides policies and establishes standards, procedures, and techniques for the disposition of Federal records.
 - f. 36 CFR 1234, "Electronic Records Management," establishes the basic requirements related to the creation, maintenance, use, and disposition of electronic records.
 - g. General Records Schedule (GRS) 20, "Electronic Records," provides disposition authority for certain types of electronic records and specific hard-copy (paper) or microform records that are integrally related to electronic records.
 - h. GRS 23, "Records Common to Most Offices Within Agencies," provides disposition authority for records common to most offices within agencies.
 - i. OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," establishes policy for the management of Federal information resources.

- j. NARA, “Managing Electronic Records” (Instructional Guide Series), contains directions to ensure proper recordkeeping for electronic information systems, including system documentation, such as operational procedures, data integrity controls, database definitions, and computer code documentation.
- k. DOE O 200.1, INFORMATION MANAGEMENT PROGRAM, of 9-30-96, provides policy and requirements for managing information in the Department.
- l. DOE G 1324.5B.1, IMPLEMENTATION GUIDE FOR USE WITH 36 CFR CHAPTER XII SUBCHAPTER B RECORDS MANAGEMENT, of 7-19-96, which provides guidance for the organization, maintenance and disposition of records for the Department of Energy.
- m. “Computer Security Act of 1987” (40 U.S.C. 759; Public Law 100-235) provides for a computer standards program within the NIST, to provide for (among other purposes) Government-wide computer security, and security training for persons involved in the management, operation, and use of Federal computer systems.
- n. U.S. Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards are published to improve the use and management of computers and automatic data processing systems in the Federal Government.

5. DEFINITIONS.

- a. Accession. The transfer of the legal and physical custody of permanent records from an agency to the National Archives.
- b. Administrative Records. Records accumulated by an individual offices that relate to the office’s internal administration or housekeeping activities rather than to its assigned mission functions. In general, these records relate to office organization, staffing, procedures, and communications; expenditure of funds, including budget records; day-to-day administration of office personnel including training and travel; supplies office services, and equipment requests and receipts; and the use of office space and utilities. Administrative records may also include copies of internal activity and workload reports (including work progress, statistical, and narrative reports prepared in the office and forwarded to higher levels) and other materials that do not serve as unique documentation of the office’s programs.
- c. Administrative Value. The usefulness of records in conducting an agency’s current business. Includes fiscal value and legal value, which are analyzed separately when records are evaluated for disposition.

- d. Audiovisual Records. Materials that meet the definition of a Federal record and that are in pictorial or aural form, including still and motion pictures, graphic materials, sound and video recordings, and combinations of media, such as slide-tape productions.
- e. Authentication. The act of attesting that the information contained in a record is a legible, complete, and accurate representation of work performed.
- f. Backup. A copy of a computer file to be used if the original is lost, damaged, or destroyed.
- g. Codebook. In electronic records, a guidebook identifying and explaining the codes used in a computer file or database.
- h. Copy. In electronic records, the result or action of reading electronic data from a source, leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source.
- I. Database. In electronic records, a set of data, consisting of at least one file or a group of files, usually stored in one location, which may be made available to several users at the same time for various applications.
- j. Data File. An organized collection of related data, usually arranged in logical records that are stored together and treated as a unit; related numeric, textual, or graphic information that is organized in a strictly prescribed form and format.
- k. Discoverable. Recorded information that may be obtained by litigation opponent(s).
- l. Disposition. Actions taken regarding records no longer needed in current office space. These actions include transfer to agency storage facilities or Federal records centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives, and disposal of temporary records.
- m. Disposition Authority. Legal approval empowering an agency to transfer permanent records to the National Archives or carry out the disposal of temporary records.
- n. Electronic Records. Any information stored in a form that only a computer can read or process and that satisfies the definition of a Federal record.
- o. E-mail Record. An abbreviation for electronic mail; a message sent or received via an electronic mail system with its transmission/receipt data and attachments and that meets the criteria of a Federal record.

- p. File Layout. In electronic records, the arrangement and structure of data in a file, including the sequence and use of its components.
- q. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures.
- r. Media. The physical forms of recorded information, including film, computer disks, computer tapes, and any other materials on which information can be recorded.
- s. Nonrecord. U.S. Government-owned informational materials excluded from the legal definition of records. Includes extra copies of documents kept only for convenient reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibition. Also called nonrecord materials.
- t. Permanent Records. Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes.
- u. Record. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business. Records are preserved or are appropriate for preservation by an agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the value of their information.
- v. Recordkeeping. The act or process of managing records from their creation, or receipt, through their processing, distribution, organization, storage, and retrieval to their ultimate disposition.
- w. Recordkeeping Requirements. As used by NARA, statements in statutes, regulations, directives, or other issuances specifying the records to be created or received and maintained.
- x. Records Management Program. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

- y. Records Schedule. A document providing authority for the final disposition of recurring or nonrecurring records. Also called records disposition schedule, records control schedule, and records retention schedule.

CHAPTER II

CREATION AND RECEIPT

The way in which human-readable records are created does not pose an issue for future use because no special device or knowledge is required to read them. The opposite is true of machine-readable electronic records. Creation of electronic records is dependent on the software application, hardware, operating system, media, and file formats that make up the computer system in use. Therein lies the special nature of electronic records in records management. Records managers should be concerned with, and help employees understand that, the methods used to create records and the documentation of the system that created the records are important and will dictate the requirements for retrieving, reading, and using records in the future.

1. CREATION OF ELECTRONIC RECORDS.

- a. Types of Electronic Records. Electronic records may be created as text, data, or images. They may be produced in a variety of media and file formats. Proper records management planning and control of these variables should ensure ongoing preservation and usability of records in electronic form.
- b. Two Main Groups. Electronic records can be described as either magnetic or optical media. Magnetic media are written and read using a magnet. Optical media use lasers. Examples are provided in the two columns below:

Magnetic Media

- 3.5-inch diskettes
- 5.25-inch disks
- magnetic tape
- tape cartridges
- magnetic cartridge

Optical Media

- CD-ROM
- Optical tape cartridge
- 12- and 14-inch disc platters
- 3.5-inch optical diskettes

- c. Current Media. Although the media listed above are currently in use, new media and formats are constantly being created and adopted and existing ones dropped. Users, computer operations administrators, and records management personnel should constantly reevaluate electronic media to determine its continued suitability for business or archival purposes. Each medium has a different life span, and records may need to be transferred to a new medium or format to ensure the information remains accessible.
- d. Selection. Proper selection of software, media, and file formats for the creation of electronic records will ensure that records can be adequately read, retrieved, and duplicated until they are no longer needed. Instructions and information for retrieval

and/or preservation must be documented to ensure long-term readability. Such information might include the physical and technical characteristics of the records, hardware and software platforms required to read the records, form of the data, and any other technical information needed to read or process the records.

- e. Text-Data Files. Text-data files are computer-readable files storing simple text characters that can be displayed or printed, usually in American Standard Code for Information Interchange (ASCII). Other computing standards for text characters exist, but are less common, such as the Extended Binary Coded Decimal Interchange Code (EBCDIC) used on some mainframe computer systems.
- (1) ASCII. Electronic documents created or stored with ASCII text can only be enhanced with additional embedded ASCII text characters (tags) to add to the document some basic display features, print formatting, or search capability. These tagged text file formats include Hypertext Markup Language (HTML) and Standard Generalized Markup Language (SGML). Electronic documents stored as text files are less dependent on a particular computer application software to view or print the document than electronic documents stored as binary data files.
 - (2) Binary Data Files. Binary data files are computer-readable files that store data formatted as 1s and 0s in a manner that requires a specific application software to display, print, or use the data in the file. Data can be stored in binary data files by word processors, spreadsheets, databases, graphics programs, or document imaging systems in either proprietary or non-proprietary data formats. Types of binary data file formats include Rich Text Format (RTF), Computer Graphics Metafile (CGM), Portable Document Format (PDF), and Tagged Image File Format (TIFF).
- f. Computer System Documentation. To ensure the long-term viability of electronic records created by computer software, computer system documentation will need to be available to anyone who might need to read or recreate the record. In addition, imaging systems that use optical disk media for records storage and contain permanent records for accessioning into NARA should conform to NARA standards. NARA regulations, directives, bulletins, and handbooks stating current policies can be obtained from NARA prior to developing or purchasing an imaging system that will contain permanent records.

2. RECEIPT OF ELECTRONIC RECORDS.

- a. Custody. In the Federal contracting environment, the custody of electronic records is frequently reassigned from one organization to another in the course of closing or changing contracts. Electronic records received but not created by an organization should follow the same guidelines as those created by the organization. However,

receiving organizations not involved in creation of the system or the records have no control over the methods used to create the records. If electronic records received have inadequate documentation, or if they require a hardware or software platform that is unavailable or obsolete, the records are rendered useless. The value of the records should be compared against the cost of obtaining or recreating software and hardware to enable the records to be read and used.

- b. E-mail Records. Internal e-mail policies, procedures, and systems for managing e-mail as records should be designed to accommodate e-mail messages received from outside. Such messages should not be treated any differently than internally generated messages. If an e-mail message received from outside meets the definition of a Federal record, it should be handled as a Federal record within the organization's internal system.
3. AUTHENTICATION/APPROVAL. All records requiring authentication must be dated and either signed, initialed, stamped, or otherwise attested to their authenticity. Authentication is a confirmation that the record is accurate, complete, and appropriate to the actions taken. For paper records, authentication is usually easy to verify because most forms of hard copy record authentication are visible on the front of the record. Methods of authenticating electronic records, however, are more varied. These methods include, but are not limited to the following:
 - a. Hard Copy. Authentication of a hard-copy document that accompanies the electronic media. This hard-copy document can be a transmittal or information sheet containing information about the electronic record that can be used for identifying, retrieving, or indexing.
 - b. Label. Authentication of a label attached to the media.
 - c. Signature Link. Linking of a digital signature to the electronic file/document.
 - d. Authentication. Design of a unique location-specific procedure for authentication of electronic records.
 4. SUBMISSION OF ELECTRONIC RECORDS. In organizations employing centralized files, electronic records should be submitted as follows:
 - a. Indexing Requirements. Electronic records should have sufficient accompanying information to allow correct indexing of the records. The records should have an external label affixed, or include documentation that contains the following:
 - names or narrative description of the information submitted;
 - date the information was generated;
 - names of person or organization that generated the information; and

- identifying numbers or codes, such as serial or volume number.
- b. Additional Documentation. Electronic records submitted should include all available documentation including any special instructions for retrieval or preservation, physical and technical characteristics of the records, hardware and software platforms required to read the records, a description of the form of the data, and any other technical information needed to read or process the records.
- c. Duplicates. Electronic records should be submitted in duplicate so that records maintenance personnel can place one copy in storage and have one copy available for retrieval. Generally, records maintenance personnel will not have hardware and software to read or duplicate electronic records. It should be a requirement that users submitting electronic records are responsible for providing any equipment necessary to read and process the records.
- d. Missing Documentation. Generally, electronic records submitted in compliance with the above criteria will be accepted by records maintenance personnel. On the other hand, records maintenance personnel should not accept records with insufficient information until that information is provided.
- e. Preservation Responsibility. Records maintenance personnel who accept an electronic record also accept responsibility for continued preservation of the record. Appropriate policies, procedures, and standards should be developed to ensure the media are properly stored, including but not limited to proper environmental storage conditions for temperature and humidity; cleaning, rewinding, retensioning, and recopying magnetic tapes; migration; and periodic checking of the electronic records to identify and rectify any degradation.

CHAPTER III

USE AND MAINTENANCE

It is important that the integrity of all Federal records be maintained throughout their life cycle. Capturing information electronically imposes new requirements for the records including their handling, use, and maintenance in the office, which must occur concurrently with the protection of their integrity. The basic records management principles applied to paper records can be applied to electronic records.

1. RECORDS STORAGE AND MAINTENANCE.

- a. Necessary Criteria. Appropriate media and systems for storing Federal records throughout their life cycle should—
 - (1) permit easy retrieval in a timely fashion;
 - (2) facilitate distinction between record and nonrecord material;
 - (3) retain records in a usable format until final disposition/destruction occurs;
 - (4) meet requirements for accessioning permanent records into the National Archives;
 - (5) include a data migration plan for each series; and
 - (6) facilitate records authentication and verification.

- b. Factors to Consider. Before selecting a storage medium or converting from one medium to another, the following factors should be considered:
 - (1) The authorized life of the records, as determined during the scheduling process.
 - (2) The effort necessary to maintain the records.
 - (3) The cost of storing and retrieving the records over the life of the media or record.
 - (4) The record's density.
 - (5) The access time to retrieve stored records.

- (6) The portability of the medium; i.e., selection of a medium that will run on equipment offered by multiple manufacturers and that will allow transfer of the information from one medium to another (e.g., from optical disk to magnetic tape).
 - (7) Whether the medium meets current applicable Federal Information Processing Standards.
 - (8) The length of time that storage is required. Floppy disks are not recommended for the exclusive long-term storage of permanent or unscheduled electronic records.
 - (9) Established procedures for external labeling to ensure that all authorized users can identify and retrieve information stored on diskettes, removable disks, or tapes
 - (10) Conversion of storage media to provide compatibility with current hardware and software to ensure that information is not lost because of changing technology or deterioration. Before conversion to a different medium, a determination should be made that the authorized disposition of the electronic records can be implemented after conversion.
 - (11) Backing up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. (This is sometimes called "making a copy.") Duplicate copies of permanent or unscheduled records should be maintained in storage areas physically separated from the storage location of the records that were copied.
2. RECORDS RETRIEVAL. All electronic records should be retrievable throughout their life cycle. All authorized users of the system should be able to retrieve desired documents through some means, such as an indexing or text search system. Key fields should be uniquely identified and properly indexed to ensure records can be retrieved accurately.
 3. RECORDS PROTECTION. To ensure they are accessible and readable until their disposition, all electronic records should be protected to ensure their integrity and to check for deterioration.
 4. RECORDS SECURITY. Implementation and maintenance of an effective records security program should incorporate the following:
 - a. assurance that only authorized personnel have access to electronic records,
 - b. backup and recovery of records to protect against information loss,

- c. assurance that appropriate personnel are trained to protect sensitive or classified electronic records,
 - d. minimum risk of unauthorized alteration or erasure of electronic records, and
 - e. assurance that electronic records security is included in computer systems security plans prepared pursuant to the Computer Security Act of 1987 (40 U.S.C. 759 note).
5. JUDICIAL USE. Electronic records may be admitted in evidence to Federal courts for use in court proceedings if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the system management controls imposed upon the system. Implementation of the following procedures will enhance the legal admissibility of electronic records:
- a. documenting that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach;
 - b. substantiating that security procedures prevent unauthorized addition, modification, or deletion of a record and that those procedures protect the system against such problems as power interruptions;
 - c. identifying the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records; and
 - d. coordinating all the above with legal counsel and senior staff.

CHAPTER IV

DISPOSITION

One of the most effective techniques for managing all records (including electronic records) is scheduling them for disposition. Use of DOE F 1324.14, "Files Maintenance and Records Disposition Instructions," is recommended. This form describes records series as either temporary or permanent. Temporary means the records are disposable after a certain fixed period. Permanent records are records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes. The term "disposition" refers to what happens to the records when they are no longer needed for current business and includes, but is not limited to, transfer of eligible records to Federal records centers, transfer of permanent records to the National Archives, and disposal of temporary records. To prescribe disposition for electronic records, their electronic information system should be analyzed and described.

1. INVENTORYING ELECTRONIC RECORDS. An aggregate collection of information about information systems constitutes an information systems inventory. This is the first step in the disposition process. Information pertinent to determining the disposition of an information system follows:
 - a. name of the system;
 - b. system control number;
 - c. program supported by the system;
 - d. purpose of the system;
 - e. data input and sources;
 - f. major output(s);
 - g. information content;
 - h. hardware/software environment;
 - I. system managers;
 - j. location of documentation needed to read and understand the files (code books and file layouts);
 - k. restrictions on access and use;
 - l. authorized disposition of the information as determined by the General Records Schedules or a NARA-approved Standard Form 115, "Request For Records Disposition Authority";¹
 - m. disposition authority citation;
 - n. location and volume of any storage media containing identical information;
 - o. identification of person conducting the inventory;
 - p. date of inventory;

¹ Information systems not covered by a schedule should be indicated as, then indicate "Unscheduled" and include a recommended disposition.

- q. data/application owner; and
 - r. data/application organization.
2. APPLYING GENERAL RECORDS SCHEDULES. After compiling an inventory of electronic information systems, the next step is to determine whether the information in any system is covered by disposition instructions in the General Records Schedules (GRS) issued by NARA, the NARA-approved DOE Administrative Records Schedules (ADM), the NARA-approved DOE Program Records Schedules (PRO), or site-specific records schedules.
3. SCHEDULING RECORDS.
- a. Unscheduled Records. Some records with enough value to warrant permanent preservation in the National Archives are not covered in existing schedules. Other records with only a temporary value are also not covered in existing schedules. These records are referred to as “unscheduled” records. To obtain authorization for the disposition of unscheduled electronic records, an SF 115 is submitted to NARA for approval. When scheduling records for disposition, the following factors should be considered:
 - (1) data sets and files included in the system;
 - (2) hard-copy inputs and outputs;
 - (3) processing, subset, and special format files created and used in the system;
 - (4) documentation describing and defining the system and the data in it;²
 - (5) determination of the values inherent in the records.³
 - b. Standard Form 115. An SF 115 should be prepared after it has been determined how long the data needs to be maintained, and after any additional legal requirements affecting disposition have been identified.
 - c. Potentially Permanent. As is true for most hard copy records, most electronic records do not warrant permanent preservation in the National Archives. The following are examples of some potentially permanent electronic records:

² This technical documentation is a valuable record that should be retained for the life of the system.

³ Values are based on the usefulness of records in documenting fiscal, legal, administrative, emergency operating, and rights and interests uses.

- (1) electronic records that replace records scheduled as permanent in another medium;
 - (2) automated indexes to permanent records;
 - (3) unique and important scientific and technical data resulting from observations of natural events or phenomena or from controlled laboratory or field experiments;
 - (4) management data that have Government-wide coverage or significance;
 - (5) socioeconomic data on such topics as trade, education, health, or behavior;
 - (6) natural resource data related to land, water, minerals, or wildlife;
 - (7) data that document military or civilian operations during times of war, civil emergency, or natural disaster;
 - (8) political or judicial data related to such topics as elections, special investigations, or court proceedings;
 - (9) cartographic data used to map the earth's surface, other planetary bodies, or the atmosphere; and
 - (10) national security and international relations data that document such activities as strategic or foreign policy assessments, foreign public opinion, or international negotiations.
4. SCHEDULES. Once a proposed disposition for the unscheduled records of an electronic information system has been approved by NARA, the disposition authority and approved disposition become part of either of the two types of Departmental records schedules—ADM and PRO—, or site-specific records schedules.
5. DISPOSITION OF UNIQUE ELECTRONIC RECORDS. See Chapter V for disposition regarding unique information management issues.

CHAPTER V

SPECIAL ISSUES

Records managers should coordinate the effort among records creators, records recipients, and computer systems management organizations to ensure that records are maintained and protected in accordance with approved record schedules. Records managers should ensure that site-level policies and procedures are developed to protect and ensure accessibility of electronic documents.

Certain actions involving electronic records may have a direct, significant impact on the integrity and authenticity of those records. It is important to know that regardless of its record status, any electronic document, draft, copy, backup, image, and voice mail message is potentially “discoverable” and may be admissible in court.

1. LEGAL ADMISSIBILITY.

- a. Creation/Receipt. When effective recordkeeping practices are implemented, computer-based records pose no greater legal problems than do paper or micrographic records, unless statutes or regulations specifically require records to be in paper format. If the only record is electronic, procedures should be established and followed so that (1) the date of the record can be determined, (2) the date of any alterations will be automatically recorded by the system, and (3) it will be evident that the document was authorized to be issued (“signed”).
- b. Use and Maintenance. System documentation and procedures should sufficiently document the system’s credibility as an accurate representation of work performed. (See also Paragraph 9. of this chapter, “Electronic Record System Documentation.”) Electronic records must be used and relied on in the normal course of business. Training and procedures should support the normal use of electronic records and be kept current, as should system documentation and disposition. Additionally, regular, independent assessments of electronic records and the system maintaining them need to be performed. Procedures should include how and what records are entered, retrieved, used, maintained, dispositioned, and audited, reflecting what occurs in the normal course of business.
- c. Disposition. Retention and disposition of electronic records must adhere to NARA-approved records schedules.

Note: Records eligible for disposition that have been identified as necessary for a legal process may not be disposed of until the legal process has been resolved.

2. MULTIPLE COPIES, REVISIONS, DRAFTS, AND BACKUPS.

- a. Use and Maintenance. It is important to use and maintain the most recent version of an electronic record or nonrecord because multiple, prior iterations of an electronic document can exist on local hard drives, network drives, floppy disks, and other electronic storage media, causing confusion.
- b. Disposition. When scheduling electronic records for disposition, the records manager should ensure the following are considered and reflected in local policy and practice:
 - (1) Determining the retention period for drafts that do not become finalized (e.g., until no longer needed; report issued; disposition of final version), as well as drafts of issued versions.
 - (2) Ensuring that all copies are scheduled.
 - (3) Establishing a routine schedule for deleting working and system backups and deleting prior iterations of documents.
 - (4) Establishing a routine schedule for degaussing, or overwriting, erased disk files by using appropriate disk utilities. This is increasingly important for all computer systems to prevent business risk.
 - (5) Ensuring that each linked information source is properly dispositioned to consider the approved retention period of the documents to which they are linked. (See this chapter, Paragraph 11, "Complex Electronic Records," for additional information.)

Compound documents may contain links to various information sources rather than the actual information itself. Documents can be compiled from various "boiler-plate" information sources. These sources may be stored in different word processing documents, database files, spreadsheets, and sound files, each of which might reside on a different computer system. For example, purchase requisitions may be compiled from signature files, vendor name and address files, requisitioner name and address files, and parts and inventory files, which may be stored in diverse locations accessible via a network.

Note: In high-security environments, users should be aware that deleting a file does not necessarily remove the data or information from the medium; it may only remove the file name and extension from the directory of files. The space occupied by classified files should be degaussed and overwritten or the medium physically destroyed to prevent unauthorized re-creation of the file.

See Attachment V-1, for additional discussion of disposition issues for particular kinds of electronic files.

3. IMAGING SYSTEMS.

- a. Creation/Receipt. If the paper (or other media) originals are retained after imaging, the “best evidence rules” will generally indicate that the original copy remains the record copy for legal purposes. The storage medium selected—i.e., Write Once Read Many (WORM), re-writable optical disk, tape, magnetic disk—should be appropriate for the records retention and Quality Assurance (QA) requirements, and should include policies, procedures, and training that support and enforce record preservation and integrity. Preparation of originals for scanning is essential to ensure readable, complete, and accurate imaging.. Before equipment and software applications are selected, the physical characteristics of the originals being imaged must be considered, including color, textual, and pictorial content of the originals, in order to make a true and accurate imaged copy of the original. Site legal counsel should be consulted regarding the admissibility of the scanned images.
- b. Use and Maintenance. Provisions should be established, documented, and managed for migrating images forward as applications, imaging equipment, and storage media advance.

Note: See Paragraph 7 of this chapter, “Data Portability/Migration.”

- c. Disposition. Storing files with varying disposition dates on one disk or tape requires management of disposition. In the case of WORM drives, disposition management will require recopying records that are not due for disposition onto new storage media so that the other files can be disposed of, whether for transfer or destruction. Removing the index pointers to the imaged files will not destroy an image. The image itself must be removed from the storage media, or the storage media must be physically destroyed.

4. QUALITY ASSURANCE RECORDS.

- a. Creation/Receipt. It is important to understand the creation and duplicate copy requirements established for the site.
- b. Use and Maintenance. Likewise, it is important to understand and implement any special, local site storage requirements designated for QA records. It is not recommended that single storage be used for electronic, QA records.
- c. Disposition. Ensure that disposition of all copies of QA records takes place.

5. VOICE MAIL.

- a. Creation/Receipt. Generally, a voice mail system is not considered to be a recordkeeping system. Should a voice mail message be determined to be a record, the user should document the message in a more stable and appropriate recordkeeping system. For example, the content of the voice mail message can be recorded on paper, or in an electronic file, either as a “note to file” or in a confirming note or memorandum to the sender of the voice mail message; this record can then be entered into the recordkeeping system.
- b. Use and Maintenance. Users should be aware of the voice mail application’s capabilities regarding deletion of unread, skipped, and stored voice mail messages, and whether a deleted message can be recovered. If this information is not widely disseminated in a policy or procedure development of such a policy should be considered. Included in such a policy should be the site’s policy regarding privacy of voice mail messages and the circumstances in which an individual’s voice mail may be retrieved by someone other than the individual.
- c. Disposition. If a voice mail message is determined to be a record, the recorded message may be deleted once the content has been properly documented in a regular recordkeeping system.

6. AUDIO/VIDEO CONFERENCING/RECORDINGS.

- a. Creation/Receipt. Audio and/or video recordings may be considered a record if the content of the recording meets the definition of a record as found in 44 U.S.C. 3301. If it is anticipated that the content of a recording will be a record, the necessary actions must be taken to properly identify the recording, the date it was made, etc.
- b. Use and Maintenance. Recordings should be maintained under proper conditions (e.g., in a temperature/humidity-controlled storage environment) to ensure preservation and accessibility of recordings during the approved retention period.
- c. Disposition. The recording of a video conference or teleconference may be disposed of if—
 - a video conference or teleconference is recorded for note-taking purposes only, and
 - the visual and auditory content is fully transcribed to a document (electronic or otherwise), and
 - the document is solely relied upon as a record of the meeting, and
 - this reliance is reflected in the site’s records schedule

7. DATA PORTABILITY/MIGRATION.

- a. Creation/Receipt. As software and equipment continues to improve, change, become obsolete, or be replaced with other software and/or equipment, it is necessary to ensure that electronic records created using the superseded software and/or equipment are readable, and accessible, throughout the records' approved retention period. This requires records managers, users, system administrators, and other interested individuals to make provisions to upgrade, convert, or otherwise move the electronic documents into the new equipment/software environment at the time that the new software/equipment is put into service. Likewise, quality control provisions should be part of the process to ensure the upgraded, converted, or moved electronic records are readable, accessible, and unaltered once they reside in the new software and/or equipment.
- b. Use and Maintenance. Records managers and users should develop processes, including periodic records compliance audits, for ensuring compliance with the standards for storing electronic documents as those standards develop and change. Such standards may address use of the following:
 - a particular directory/folder structure,
 - a network drive rather than a local drive,
 - a particular universal format like Portable Document Format (PDF).
- c. Disposition. Even though electronic documents may not be accessible or readable by an individual user or group of users after upgrade of equipment or software, others may be able to access and read those documents. Records managers and users should ensure the former versions of the electronic documents are destroyed once the documents reside in the new software/equipment to avoid the potential for unauthorized disclosure of the content of the documents.

8. E-MAIL RECORDS. E-mail messages are considered Federal records according to the same criteria established for other Federal records. Accordingly, the same records management principles and guidelines that apply to paper and other non-electronic records apply to e-mail. E-mail records are subject to the same information protection and security issues as other Federal records in other media. In addition, the dynamic communication environment of e-mail, with potential copying and wide distribution of information, makes it very important that standard records management procedures and recommendations be followed by all creators and users of e-mail. Each organization's records management guidelines and procedures should specifically address the important issue of e-mail records. E-mail users (senders and receivers) should distinguish between record and nonrecord materials, properly preserve the records, and promptly dispose of nonrecords as soon as they have fulfilled their purpose.

a. Creation and Receipt.

- (1) A Record. The user generally decides whether an e-mail message and/or attachments is a record. The user must base the decision on the 44 U.S.C. 3301 definition and local guidance and explanatory material provided by records management personnel. As with other records, the decision process focuses on the information, not the media. Each organization must implement specific programs to ensure that users are properly trained to determine the record or nonrecord status of any e-mail messages. The appropriate two-part question to answer is, "Should this message be included in the appropriate records series as necessary documentation for a transaction, and is maintenance of its specific records series the responsibility of the user's organization"?
- (2) Distinguish. All e-mail users should be provided with sufficient information, guidance, and training to distinguish Federal records from nonrecords and to apply appropriate retention and disposition practices. Many nonrecords are retained solely for convenient reference, not to document transactions in a records series.
- (3) Training. Training programs for e-mail users should address the following:
 - (a) how to identify or create e-mail records that are appropriate or necessary for retention purposes;
 - (b) how to distinguish between record and nonrecord messages and/or attachments;
 - (c) the similarities for recordkeeping purposes between e-mail records and records transmitted by mail or fax systems;
 - (d) the need for describing and instructing users regarding the e-mail hardware/software used on-site;
 - (e) how technology should be used to best meet recordkeeping requirements (e.g., how to set up electronic "folders" to match record series/file titles);
 - (f) how to establish site-specific procedures for producing a complete record of the message, plus transmission data and receipt, if in use at the site;
 - (g) site-specific requirements for record creation, and;
 - (h) site-specific requirements and/or outside compliance orders for training methods and documentation.

b. Use and Maintenance.

- (1) Storage Options. The recordkeeping system should allow e-mail records to be retrieved in a useable format. The three general storage options are—
 - the e-mail system itself;
 - a separate electronic recordkeeping system; and
 - paper or non-electronic media.
 - (2) Person Responsible. The person who has created, received, or acted upon a message/attachment that is a record is responsible for ensuring that it enters the recordkeeping system. A non-record may be deleted without entering it into the system.
 - (3) Transaction Documents. Messages belong in a record series when they document transactions in a records series that the user's organization is responsible for maintaining. The responsible person should first note that an e-mail message constitutes a transaction document; second, he/she should ensure that the message is placed in the official record series for that type of record. The record will then be available to other authorized users. The records series file could be paper or electronic. Whichever it is, the record series should be described, maintained, and disposed of according to the established file instructions on DOE Form 1324.14, "Records Maintenance and Disposition Instructions." Each organization should implement specific procedures for performing this activity.
 - (4) Personal E-mail Folders. Generally, personal e-mail "folders" for storing messages should not be part of an official record system. E-mail is password-protected and is available increasingly on a user's workstation only. Others do not have easy access to the information
- c. System Backups. System backups are intended to restore computer system operations and are not adequate for records storage and archival purposes. They should not be used for a records series retention.
- d. System Backup Tapes. System backup tapes or media should be destroyed according to established rotation schedules. Temporary records should never be kept longer than the retention period in the records disposition schedules for the records series contained in the backup files because if the record exists, it is discoverable. Deleting or thoroughly erasing this information at specific intervals will reduce possible business risk, cost due to misuse of information, and compromise of protected information. This records retention consideration also applies to personal backups on floppy disks.
- e. Message Meta Data. E-mail message records should include transmission and receipt data, as needed for adequate and proper documentation of transactions. Transmission

data is part of an e-mail record and should be included wherever necessary for complete documentation of significant transactions. Incidentally, this related data is appropriate record information, whether non-electronic or electronic. As meta information, it includes sender's name, dates and times transmitted, names of recipients, and subject. If a return receipt is requested, the verification of that receipt including time received is also part of the record. If an e-mail record is sent to a "group," the names of the individuals in that group at that point in time should be available. For large corporate groups, such as "all employees," the organization that maintains the group may be assigned responsibility for keeping a record of who was in that group at any point in time.

- f. Security. E-mail systems need to incorporate security measures to protect against unauthorized alterations or deletions.
- g. Access to E-mail. E-mail is not completely confidential or private. Supervisors may have the right to read an employee's e-mail in certain circumstances (e.g., during absences). A network or systems administrator may need to access employees' e-mail for technical reasons.
- h. Classification. Approved records disposition schedules are required for classified documents. Classified documents are also records. Classification requirements must be strictly adhered to regarding the creation, maintenance, or disposition of classified records (including classified electronic records). For security requirements and procedures affecting classified records, see DOE O 471.2, INFORMATION SECURITY PROGRAM; DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL; and their accompanying contractor requirements documents. Information classification and protection procedures and guidelines are mandatory for use of an e-mail system involving classified records.

- Notes:
- (1) Simple deletion of a message does not actually erase or destroy the message, and specific requirements apply.
 - (2) Additional organizational and systems procedures may apply to some nonclassified systems.

- i. Disposition.
 - (1) E-mail records should be retained and disposition made according to approved records schedules.
 - (2) Depending on the content, some e-mail messages may be unscheduled records. As the term "unscheduled" implies, unscheduled records are not authorized to be destroyed.

- (3) Avoid retaining records beyond the approved retention period provided for in an approved records schedule.
 - (4) Nonrecords may be deleted from computer systems without filing a copy for record purposes. Many e-mail messages are nonrecords. Other examples of nonrecords include copies of memoranda or letters that were received for information rather than action; messages or attachments for whose retention the individual is not responsible; or messages that have only temporary value (such as the message that an insignificant meeting has been moved from the morning to the afternoon).
9. **ELECTRONIC RECORD SYSTEM DOCUMENTATION.** Documentation is required for any computer system that electronically transmits records to a recordkeeping system or stores and manipulates electronic records. For any legal or regulatory purpose, system documentation will substantiate and demonstrate consistent and systematic use of the system, in accordance with established requirements. To protect an organization in the event of litigation, it is imperative to show that all reasonable requirements were successfully met in the implementation and operation of electronic records systems. To that end, the level of detail in the documentation should be commensurate with the importance of the application and records series being considered. The following information should be addressed when documenting systems or related activities or processes that involve the generation of electronic records.
- a. **System Purpose and Scope.** Describe the system's purpose, function, and operation. Identify the records that are to be maintained as electronic records and those that are not to be included in the scope of the system.
 - b. **Operating and Technical Specifications.** Describe the operational and technical specifications used for developing or procuring the system, and provide complete copies of the operating manuals purchased with the system or developed for the application.
 - c. **Testing and Validation.** Document the testing, test results, and validation program or method used to evaluate the system's compliance with design or procurement specifications. Include the method by which any program changes are implemented and verified for proper system operation.
 - d. **Data Dictionary.** For database applications, document the following in the data dictionary for all data and summary fields: data element name, description, field type, field size, and method for validation.
 - e. **System Links to Other Systems.** Identify all links and network configurations used to receive, use, or exchange data with other computer systems. Include the names of

other systems and describe the information exchanged and how that information is exchanged.

- f. Disaster Planning. For disaster prevention and recovery plans, describe how records access downtime is minimized and what alternative methods, if any, are available when experiencing minor failures up to and including catastrophic failures. These plans should describe potential hazards, preventive measures taken, and procedures to follow in the event of a disaster. System access controls preventing unauthorized modification of the information should be included in the disaster prevention section. These plans should be reviewed and tested periodically for adequacy; any deficiencies identified should be promptly corrected.
 - g. Future System Migration or Upgrade. Document how future migration or upgrade plans for the system will be handled. Address how hardware, software, or operating system upgrades or obsolescence will be handled while simultaneously continuing to properly retain and maintain the records until their authorized disposition. Satisfactory evidence that data migration will be successful can be demonstrated by testing. During testing, data should be transferred to other systems or file formats to demonstrate that the transfer works. This will ensure that the data configuration can be maintained for as long as it is required to be retained.
 - h. Operational Procedures. Procedures should be approved and in effect for all system operations including data entry, correction, modification, or deletion; database administration; and modifications to, and testing of, the software.
 - i. Quality Control and Quality Assurance. To ensure data accuracy and integrity, plan for and describe the quality control and quality assurance measures or procedures to be implemented. To verify compliance with all programmatic and procedural requirements, plan for the type and frequency of internal and independent assessments to be performed.
 - j. Training. Document user training to show that users are qualified to enter, retrieve, modify, or delete data in the system and to perform any system database administration functions. Also, document general user training to enable users to extract necessary information and to interpret the information in support of decision-making processes.
10. INFORMATION SYSTEMS AS RECORDS. Information systems or databases are complex, dynamic data processing environments. In these environments, information undergoes a variety of logical and numerical processes to provide multiple system users with up-to-date, relevant, on-line, structured and unstructured information. Organizational systems may include payroll, budget and accounting, records indexing, inventory, scheduling, computer-aided design and drafting (CADD), and three-dimensional modeling. These information systems consist of one or more numerical, textual, or graphical files containing data elements subject to a variety of rules and relationships with other fields, files, and even systems. These systems can reside on a variety of computer platforms

ranging from stand-alone personal computers to group or Departmental servers, including mainframes.

- a. Formerly the Nonrecord Copy. In the past, due to the complexities and logistics involved, many organizations considered information systems by themselves to be the nonrecord copy, and the copy itself was retained and used for information purposes only. The signed, hard-copy forms authorizing data to be updated or changed and the specific, periodic printouts—paper, computer output to microfilm (COM), or laser disk (COLD)—were considered to be the records. Some organizations considered the records to be the hard-copy printouts or screen prints of requested ad hoc reports summarizing the data contained in the system. The database itself, however, was not considered to be “record” information.
- b. Electronic Information Systems Designated as “Records.” The following guidelines should be considered in planning for the implementation and maintenance of an information system as “the record copy” or as “record” information, as opposed to its use as “an extra copy for information only” (i.e., for convenient reference only) consider the following guidelines:
 - (1) Assemble a project implementation team drawing on, at a minimum, computer, technical, legal, business/operation, regulatory, and records experts. Additional resources or support may include computer security personnel and representatives of upper management, such as, the chief executive officer (CEO) or chief information officer (CIO).
 - (2) Provide complete system documentation to substantiate consistent and systematic use of the system for any legal or regulatory purposes. The level of detail in the documentation should reflect the importance of the application being studied. (See this chapter, Paragraph 9, “Electronic Record System Documentation.”) Depending on the specific functions and importance of the application being planned, address the following considerations in the documentation:
 - (a) Evaluate and document the record media balance to be used; that is, determine how much of the data in the information system will be used as the record copy, in lieu of traditional paper records. Records management organizations or implementation teams should evaluate the value of data contained in the system and determine which information is better retained electronically rather than as hard copy. Data that can be disposed of “when no longer needed” or “when superseded” could reasonably be expected to be kept electronically. Data that requires a long retention period or documented authorizations and signatures may need to be documented in a hard copy. Periodic status reports can be prepared and generated to capture specific data elements and then printed to paper, microfilm, laser disk, or

even magnetic tape. This practice may help prevent some of the electronic storage and long-term retention and management issues involved with retaining the database as a record.

- (b) Determine the types and importance of decisions likely to be made using the on-line information system, and determine what documentation is or will be necessary to support those decisions in the future. Recognize also that the user's ability to generate ad hoc reports may result in information being seen in a variety of different contexts, more so than if they were made available through standard, system-generated reports. If that is the case, the system manager should determine how to maintain that electronically retained information. To do this, he/she should determine—
- whether each addition, modification, deletion, or system query should be tracked in a transaction log or audit trail along with periodic snap-shots;
 - how far back a transaction log/audit trail should be maintained; and
 - what information should be maintained in the log (e.g., user identification, before data, after data, and date and time of change).

The project implementation team should decide how often, and for how long, complete system backups should be maintained, while ensuring that they are not retained longer than authorized for the system records. The team should decide when, if necessary, users or system administrators are required to save ad hoc queries and query results as hard copy records rather than relying on system transaction logs or backups.

- (c) Evaluate requirements for accessing and manipulating data to meet future retrieval needs. Periodic ASCII reports may meet the business and regulatory retention needs.

11. COMPLEX ELECTRONIC RECORDS. Complex electronic records are composed of multiple computer files to be viewed on a computer screen. Printing these records on paper may result in a loss of some of the records' content. These complex electronic records are a subset of electronic records and include the following: multimedia documents such as electronic files that combine both text and video, dynamically linked documents such as text files with active links to electronic spreadsheets, HTML documents sometimes known as "Home-pages or Web pages," and three-dimensional CADD models. These records present relatively new issues for records and information managers and require special care to manage electronically. The following guidelines are intended to aid organizations in managing these types of records:

- a. Multimedia Combined Documents. Multimedia documents that combine two or more record types in a single record are best used for record series with short retention periods, or simply as “information only” documents. The viability of maintaining these records for long retention periods is uncertain particularly as software and hardware evolves. Record copies could be managed more easily if stored as separate records, rather than as combined multimedia records.
- b. Linked Records. Linked records are records that automatically extract information from another electronic file; for example, a word processing report that automatically extracts and displays selected financial data from a budget spreadsheet. Through the use of linked files, one file can be automatically updated when the linked file is changed. This situation would invalidate records that require retention periods longer than “until superseded.” Therefore, care must be taken that the information to be extracted is either copied and pasted into the record file, or the file from which data is extracted is protected from being changed or revised. In the first case, copying and pasting data eliminates the need for maintaining the second file as part of the record. In the latter case, any time a component of a set of linked files is changed, the entire set must be saved as a new revision, if required by an approved records disposition schedule. This maintains a revision audit trail for the record.
- c. Hypertext Documents. Hypertext documents are files that contain embedded links that allow a reader to select new information by pressing the mouse button while the cursor is on the link. This results in a jump to another view of the same document or a jump to an entirely new document on the same server or some other designated server anywhere in the world. At this time it is recommended that Web pages on an Internet Server be viewed as “information only” documents and not records. Record copies of Web information should be stored in a separate recordkeeping system for as long as is required by approved records disposition schedules.
- d. Design Models. Three-dimensional CADD models can be used to represent the design of facilities, structures, systems, equipment, or components. They can produce the traditional two-dimensional drawings necessary for construction and maintenance of an item. Engineering design changes can result in the model being updated electronically without the need for printing two-dimensional drawings ,but these changes will be there when a hard copy is requested. Record managers should work with the appropriate engineering and construction organizations to decide how the record information should best be managed. Options include electronic or hard copy management. Electronic management would require taking and storing electronic snapshots of the model and tracking the individual changes electronically between snapshots so that the model can be reconfigured for any point in time. Hard-copy management could require printing out paper or computer-output-to-microfilm (COM) of the two-dimensional drawings along with each subsequent revision. A mix may include direct computer-output-to-laserdisc (COLD) or scanning the paper or aperture cards into a more traditional imaging system.

- e. Similarities. The general issues and concerns for managing complex electronic records are the same as for simple electronic records or even paper and microfilm. Records managers should work with appropriate organizations to establish and document the policies and procedures for transferring the records to a new custodian. Consideration should always be given to access frequency, information format, technology migration, and long-term retention issues, such as software and hardware upgrades. These issues should be balanced by the relative importance of the application and the record series.

ATTACHMENT 1

DISPOSITION ISSUES FOR PARTICULAR KINDS OF ELECTRONIC RECORDS

1. Overwritten Files. When a file already exists with a specific filename and extension, revisions to that file may replace the old file. The old file is still stored on the medium, but it is inaccessible to the user. (Technically advanced users with the proper commercially available utilities may still gain access to the file.)
2. Erased Files. Files that have been erased directly by the user generally have no problem with record integrity. However, the operating system may only delete the file's name from the directory and leave the data on the medium while waiting for the space on the hard disk or floppy disk to be reused for another file.
3. Copied Files. As files are created, saved, and copied to another medium (e.g., from the hard disk to a floppy disk), two copies of the file exist with the same file name and extension. If the copy process is repeated using a different floppy disk, multiple prior iterations of the file exist. If it becomes necessary to restore a file from a backup floppy disk, it is important to use the most recently revised floppy disk file; use of an earlier but unrevised floppy disk will result in loss of data and time when the error is discovered.
4. Backup Files. Some software applications create backup files with the same name but a different extension to identify it as a backup file. These backup files may be recaptured without the need for special utilities. Unless the medium is degaussed or the backup file is erased and its file space either reused or degaussed, the old file may still be resident on the medium.