



OSHA INSTRUCTION

U.S. DEPARTMENT OF LABOR

Occupational Safety and Health Administration

DIRECTIVE NUMBER: ADM 12-0.4A

EFFECTIVE DATE: August 3, 1998

SUBJECT: Revised OSHA Records Management Program

ABSTRACT

Purpose: This revision provides updated records management procedures on OSHA records, nonrecords and personal papers, regardless of media.

Scope: This instruction applies OSHA-wide.

Reference: The following instructions are referenced in this instruction. OSHA Instructions:
ADM 12.1, OSHA Classification System.
ADM 12.5A, OSHA Compliance Records.
ADM 12-7.2A, Regional and Area Office Records Disposition.
ADM 12-7.3, National Office Records Disposition Schedule

Cancellations: Cancel OSHA Instruction ADM 12.4, OSHA Records Management Program

State Impact: None.

Action Offices: . National, Regional, Area and District Offices.

Originating Office: Office of Management Systems and Organization (OMSO)

Contact: OMSSO, Records Officer (202-219-6320)
N3618 Frances Perkins Building
200 Constitution Avenue, NW
Washington, D.C. 20210

By and Under the Authority of
David C. Zeigler
Director, Administrative Programs

Table of Contents

ABSTRACT	COVER PAGE	
Chapter I	PROGRAM REQUIREMENTS, MANAGEMENT AND RESPONSIBILITIES	1-1
I.	<u>Purpose.</u>	1-1
II.	<u>Scope</u>	1-1
III.	<u>Action Information.</u>	1-1
A.	<u>Responsible Office.</u>	1-1
B.	<u>Action Offices.</u>	1-1
C.	<u>Information Offices.</u>	1-1
IV.	<u>Cancellation.</u>	1-1
V.	<u>Action.</u>	1-1
VI.	<u>Reference.</u>	1-2
VII.	<u>Background.</u>	1-2
VIII.	<u>Major Changes.</u>	1-2
IX.	<u>Program Objectives.</u>	1-2
X.	<u>Authorities.</u>	1-3
XI.	<u>Glossary of Terms.</u>	1-3
XII.	<u>Policy.</u>	1-3
XIII.	<u>Responsibilities.</u>	1-5
A.	<u>Director, Administrative Programs.</u>	1-5
B.	<u>Controlled Correspondence Unit.</u>	1-5
C.	<u>Directors of National Office Directorates and Independent Offices.</u> ...	1-5
D.	<u>Administrators of Regional Offices.</u>	1-5
E.	<u>Area Offices.</u>	1-5
F.	<u>Director, Information Technology.</u>	1-6
G.	<u>OSHA Records Officer.</u>	1-6

	H.	<u>Program and Regional Records Officers.</u>	1-7
	I.	<u>Records Liaison Officers.</u>	1-8
	J.	<u>Supervisors.</u>	1-9
	K.	<u>Files Custodians.</u>	1-9
	XIV.	<u>Approved Filing System.</u>	1-9
Chapter II		FILES MANAGEMENT	2-1
	I.	<u>Purpose.</u>	2-1
	II.	<u>Filing Records.</u>	2-1
	III.	<u>File Stations.</u>	2-1
	IV.	<u>Handling and Safeguarding of Classified Material and Administratively Controlled Information.</u>	2-1
	V.	<u>Files Classification</u>	2-2
	A.	<u>Classification Coding.</u>	2-2
	B.	<u>Determining Codes.</u>	2-2
	VI.	<u>File-Coding Outgoing Documents.</u>	2-2
	VII.	<u>Assembling the File.</u>	2-2
	VIII.	<u>Linking File Elements.</u>	2-3
	IX.	<u>Document Management/Recordkeeping Systems.</u>	2-3
Chapter III		RECORDS DOCUMENTATION:	3-1
	I.	<u>Purpose.</u>	3-1
	II.	<u>Goals.</u>	3-1
	A.	<u>Objectives.</u>	3-1
	B.	<u>Benefits.</u>	3-1
	III.	<u>Documentation Needs.</u>	3-2
	A.	<u>Documentation Requirements.</u>	3-2
	B.	<u>Working Documents</u>	3-2
	C.	<u>Complex Document Requirements.</u>	3-2

IV.	<u>Documentation Determinations.</u>	3-3
V.	<u>Project and Case File Documentation.</u>	3-3
A.	<u>Case Files.</u>	3-3
B.	<u>Project Files.</u>	3-4
VI.	<u>Assembly of Documentation.</u>	3-5
VII.	<u>Official Records, Personal Papers and Nonrecords.</u>	3-5
A.	<u>Official Records.</u>	3-5
B.	<u>Personal Papers.</u>	3-6
C.	<u>Nonrecords.</u>	3-6
Chapter IV	PAPER OR HARD COPY MEDIA RECORDS	4-1
I.	<u>Purpose.</u>	4-1
II.	<u>Categories and Accessibility.</u>	4-1
III.	<u>Required Copies for Paper Records.</u>	4-1
A.	<u>Official File (Yellow or Marked Official File).</u>	4-1
B.	<u>Reading File (Blue or Marked Reading File).</u>	4-1
C.	<u>Supervisory or Other Reading File (Pink or Marked For Purpose).</u>	4-2
D.	<u>CC's, Information Copies or Personal Copy (White or Xerox).</u>	4-2
IV.	<u>Coding Papers.</u>	4-2
Chapter V	ELECTRONIC RECORDS	5-1
I.	<u>Purpose.</u>	5-1
II.	<u>Scope of Electronic Records.</u>	5-1
III.	<u>Identification of Records.</u>	5-1
IV.	<u>Electronic Record Series.</u>	5-1
A.	<u>Identification.</u>	5-1
B.	<u>Retention.</u>	5-2
C.	<u>Backup Copies.</u>	5-2
V.	<u>Electronic Files Operations.</u>	5-2
A.	<u>Organization of Electronic Media.</u>	5-2
B.	<u>Electronic Mail (E-Mail).</u>	5-3

	C.	<u>Current Files</u>	5-3
	D.	<u>Filing Electronic Documents</u>	5-4
Figure 5-1		FILE SYSTEM STRUCTURE	5-4
	E.	<u>Overwritten Files</u>	5-5
	F.	<u>Copied Files</u>	5-5
	G.	<u>Erased Files</u>	5-6
	H.	<u>File Security</u>	5-6
	I.	<u>Status of Files/Data in Active Memory</u>	5-6
	J.	<u>Backups of Files</u>	5-7
	K.	<u>Labeling and Indexing</u>	5-7
VI.		<u>File Types</u>	5-8
VII.		<u>Access to Records</u>	5-8
VIII.		<u>Judicial Use of Electronic Records</u>	5-8
Figure 5-2		JUDICIAL RULES RELATING TO ELECTRONIC RECORDS	5-9
		Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial	5-9
		Rule 1001. Definitions	5-9
		Rule 1006. Summaries	5-9
IX.		<u>Security of Electronic Records</u>	5-11
	A.	<u>Objectives</u>	5-11
	B.	<u>Media Destruction</u>	5-11
	C.	<u>Lack of Security Lockouts</u>	5-12
	D.	<u>Computer Diseases</u>	5-12
X.		<u>Disposition of Electronic Records</u>	5-12
	A.	<u>General Electronic Records</u>	5-12
	B.	<u>Program-Related Database Records</u>	5-12
Chapter VI		MICROGRAPHIC RECORDS	6-1
I.		<u>Purpose</u>	6-1
II.		<u>Micrographic Records Media</u>	6-1
III.		<u>Types of Microforms</u>	6-1
	A.	<u>Varieties</u>	6-1
	B.	<u>Formats</u>	6-1
IV.		<u>Maintenance and Disposition</u>	6-1

	A.	<u>Temporary Records</u>	6-2
	B.	<u>Permanent Records</u>	6-2
	C.	<u>Other Copies</u>	6-2
	D.	<u>Record vs. Non-Record</u>	6-2
	V.	<u>Legal Considerations</u>	6-3
	VI.	<u>Security and Integrity</u>	6-3
Chapter VII		DISPOSITION	7-1
	I.	<u>Introduction</u>	7-1
	II.	<u>Objectives</u>	7-1
	III.	<u>Timely Disposition</u>	7-1
	IV.	<u>Records Disposition Schedules</u>	7-1
	V.	<u>Yearly Review of Records</u>	7-1
	VI.	<u>Disposition of Records in Offices</u>	7-1
		A. <u>Unclassified Records</u>	7-2
		B. <u>Administratively Controlled Material</u>	7-2
		C. <u>Classified Material</u>	7-2
		D. <u>Disposal of Records after Conversion to Another Media</u>	7-2
	VII.	<u>Transfer of Records to the National Archives</u>	7-2
	VIII.	<u>Transfer of Records to Federal Agencies Outside the Department</u>	7-3
		A. <u>Approval Required</u>	7-3
		B. <u>Approval Not Required</u>	7-3
	IX.	<u>Records Donated For Preservation and Use</u>	7-3
		A. <u>Permissible Donations</u>	7-4
		B. <u>Conditions for Donation</u>	7-4
		C. <u>Approval of Donation</u>	7-4
	X.	<u>Nonrecord Materials Disposal List</u>	7-5
		A. <u>Employee Activities</u>	7-5
		B. <u>Extra copies of Security Papers</u>	7-5
		C. <u>Extra Copies of Unclassified Papers</u>	7-5
		D. <u>Letters of General Inquiry</u>	7-5

E.	<u>Mailing Lists</u>	7-5
F.	<u>Notification of Change of Address.</u>	7-5
G.	<u>Personal Files</u>	7-5
H.	<u>Publications.</u>	7-6
I.	<u>Reading Files, Chronological Files, Index Files, and Other Files</u> <u>Used as Cross-Reference Finding Aids.</u>	7-6
J.	<u>Reproduction Materials.</u>	7-6
K.	<u>Routine Reference and Control Papers.</u>	7-6
L.	<u>Routine Transmittal Sheets.</u>	7-7
M.	<u>Stenographic Notes.</u>	7-7
N.	<u>Stocks of Superseded or Obsolete Blank Forms and Processed Documents</u> <u>Preserved for Supply</u>	7-7
O.	<u>Suspense Files</u>	7-7
P.	<u>Work Papers.</u>	7-7
Q.	<u>Working Files.</u>	7-7
R.	<u>Wrappers, Labels, Envelopes, and Routine Routing Slips.</u>	7-8

Chapter VIII RETIREMENT OF RECORDS TO FEDERAL RECORDS CENTERS 8-1

I.	<u>Selecting Records.</u>	8-1
II.	<u>Preparing Records for Transfer.</u>	8-1
A.	<u>Available Containers.</u>	8-1
B.	<u>Obtaining Records Center Boxes.</u>	8-2
C.	<u>Packing Records</u>	8-2
D.	<u>Labeling boxes.</u>	8-3
Figure 8-1	<u>Labeling A Records Box</u>	8-3
E.	<u>Preparing SF-135, Records Transmittal and Receipt.</u>	8-3
F.	<u>Supplemental Records Listing for SF-135.</u>	8-4
G.	<u>Submission of SF-135.</u>	8-5
H.	<u>Accession Number Assignment.</u>	8-5
I.	<u>Shipment of Large Accessions.</u>	8-6
J.	<u>Other Requirements.</u>	8-6
III.	<u>Shipment of Records.</u>	8-6
A.	<u>WNRC or FRC approval.</u>	8-6
B.	<u>Administratively Controlled Materials.</u>	8-6
C.	<u>Classified Materials.</u>	8-6
IV.	<u>Receipt of SF-135 from WNRC or FRC.</u>	8-6
A.	<u>National Office.</u>	8-6
B.	<u>Field Offices.</u>	8-6

V.	<u>Records Reference Service.</u>	8-7
A.	<u>Services available.</u>	8-7
B.	<u>Liaison.</u>	8-7
C.	<u>Routine requests.</u>	8-7
D.	<u>Urgent or Emergency Requests</u>	8-8
E.	<u>Returning Records.</u>	8-8
VI.	<u>Disposition of Records in FRC's.</u>	8-8
A.	<u>Disposition Procedures.</u>	8-8
B.	<u>Agency Notification to FRC.</u>	8-8
C.	<u>Office Address Changes.</u>	8-9
	Figure 8-2 FRC ADDRESSES	8-10
Chapter IX	SECURITY OF CLASSIFIED MATERIAL AND ADMINISTRATIVELY CONTROLLED INFORMATION	9-1
I.	<u>Introduction</u>	9-1
II.	<u>Categories of Classified Information.</u>	9-1
III.	<u>Administratively Controlled Information.</u>	9-1
IV.	<u>Restrictions on Access to Classified Information.</u>	9-1
V.	<u>Standards of Access</u>	9-1
VI.	<u>Other Security Information.</u>	9-2
Chapter X	RECORDS MANAGEMENT REPORTS	10-1
I.	<u>Required Reports.</u>	10-1
II.	<u>Bi-Annual Records Management Report.</u>	10-1
A.	<u>Matters to be Reported.</u>	10-1
B.	<u>Format.</u>	10-2
C.	<u>Submission.</u>	10-2
III.	<u>Records Management Review Reports</u>	10-2
A.	<u>Responsibilities.</u>	10-2
B.	<u>Program Evaluation.</u>	10-2
C.	<u>Areas to be Reviewed.</u>	10-2
D.	<u>Records Management Checklist.</u>	10-2
E.	<u>Report Format.</u>	10-3

	F. <u>Distribution</u>	10-3
Appendix A	E-MAIL RECORDS AND NONRECORDS	A-1
	I. <u>Introduction</u>	A-1
	II. <u>Record Copy Media</u>	A-1
	III. <u>Determining Record Status</u>	A-1
	A. <u>Records</u>	A-1
	B. <u>Nonrecord Material</u>	A-1
	IV. <u>Maintenance of Official Record E-Mail Messages</u>	A-2
	V. <u>E-Mail Official Record Contents</u>	A-2
	VI. <u>Disposition of E-Mail Records</u>	A-2
	VII. <u>Disposition of Nonrecord E-Mail</u>	A-2
	VIII. <u>Privacy Expectations of E-Mail Messages</u>	A-2
	IX. <u>Backup and Disclosure</u>	A-2
	X. <u>Security</u>	A-3
	XI. <u>Recording Members of an E-Mail Distribution List</u>	A-3
	XII. <u>Records Determination</u>	A-3
	A. <u>Definition</u>	A-3
	B. <u>Determining Official Records</u>	A-3
	C. <u>Further Guidelines Step 1</u>	A-4
	D. <u>Further Guidelines Step 2</u>	A-4
Figure A-1	OSHA E-MAIL POLICY SUMMARY	A-4
	XIII. <u>E-mail Record and Nonrecord Examples</u>	A-5
	A. <u>Records</u>	A-5
	B. <u>Nonrecords</u>	A-6
Appendix B	RECORDS MANAGEMENT GLOSSARY OF TERMS	B-1
	I. <u>Definitions</u>	B-1

II.	<u>Abbreviations and Acronyms</u>	B-15
Appendix C	CARE OF ELECTRONIC RECORDS	C-1
I.	<u>General.</u>	C-1
II.	<u>Record Storage Medium.</u>	C-1
III.	<u>Records Labeling.</u>	C-1
IV.	<u>External Labels.</u>	C-1
V.	<u>Internal Labels.</u>	C-2
VI.	<u>Indexing Electronic Records</u>	C-2
VII.	<u>Security.</u>	C-3
VIII.	<u>Disk Maintenance and Care.</u>	C-4
IX.	<u>Environmental Considerations.</u>	C-6
X.	<u>Additional Information.</u>	C-7
Appendix D	COMPARISON OF VARIOUS MEDIA FOR INFORMATION STORAGE AND RETRIEVAL	D-1
Appendix E	RECORDS TRANSFER FORMS	E-1
Figure E-1	SF-135 NATIONAL OFFICE EXAMPLE	E-2
Figure E-2	SF-135 FIELD OFFICE EXAMPLE	E-3
Figure E-3	SF-135 REVERSE	E-4
Appendix F	RECORDKEEPING PRACTICES CHECKLIST	F-1
I.	HOW TO USE THIS CHECKLIST	F-1
II.	CHECKLIST	F-2
A.	RECORDKEEPING PRACTICES	F-2
B.	FILE LESS	F-4

C.	BREAK FILES DOWN	F-5
D.	CASE FILING	F-6
E.	SUBJECT FILING	F-7
F.	ELECTRONIC RECORDS	F-8
G.	TECHNICAL REFERENCE	F-9
H.	DAILY FILING	F-10
Appendix G	CLASSIFICATION OUTLINE	G-1
INDEX		Index-1

Chapter I

PROGRAM REQUIREMENTS, MANAGEMENT AND RESPONSIBILITIES

- I. Purpose.
 - A. This revision of the Records Management Manual provides updated records management procedures dealing with OSHA records and nonrecords, regardless of media.
 - B. The Occupational Safety and Health Administration (OSHA) Records Management Manual:
 - 1. Sets OSHA policy and objectives on records management.
 - 2. Provides OSHA employees a single comprehensive authority on records management for all documentary materials regardless of media.
 - 3. Promulgates guidelines for records management including files management, records documentation requirements, records disposition, records management reviews, maintenance and disposition of classified material, handling and safeguarding of limited access materials including materials subject to the Privacy Act, and the Bi-Annual Records Management Report.
 - 4. Assigns responsibilities to carry out OSHA's records management program.
- II. Scope. This instruction applies OSHA-wide.
- III. Action Information.
 - A. Responsible Office. Office of Management Systems and Organization (OMSO).
 - B. Action Offices. National, Regional, Area and District Offices.
 - C. Information Offices. OASAM Regional Offices.
- IV. Cancellation. Cancel OSHA Instruction ADM 12.4, OSHA Records Management Program
- V. Action. All offices will implement the revised policies and procedures in this manual.

- VI. Reference. The following instructions are referenced in this instruction:
- A. OSHA Instruction ADM 12-0.1, OSHA Classification System
 - B. OSHA Instruction ADM 12-0.5A, OSHA Compliance Record System
 - C. OSHA Instruction ADM 12-7.2A, Regional and Area Office Records Disposition
 - D. OSHA Instruction ADM 12-7.3, National Office Records Disposition Schedule
- VII. Background.
- A. The Federal Records Act of 1950, as amended, in Section 506(b) requires that the "Head of each Federal agency establish and maintain an active Records Management Program." Records Management is an "active, continuing program for controlling the creation, maintenance, use, and disposition of records within an organization to document and transact its business." NARA and GSA provide government-wide oversight in the field of records management.
 - B. A maximum penalty of \$2,000 and/or three years in prison may be imposed for the unlawful destruction or removal of official records (18 USC 2071).
- VIII. Major Changes. This revision has changed the emphasis of OSHA's Records Management Program from paper records to all records. There are new chapters on documentation of policies, procedures, activities and transactions or RECORD KEEPING, paper and other hard copy records, electronic records, audiovisual records, and micrographic records as well as new appendices on care of electronic documentary materials, guidelines for selection of media for RECORD KEEPING, and additional information. The requirement to submit an annual records management report has been changed to biannual submission. The detailed instructions for management of paper records have been lightened to allow offices greater flexibility in managing their paper records.
- IX. Program Objectives. The objectives of the OSHA Records Management Program are to:
- A. Assure compliance with the provisions of Federal law and regulation applying to records management.
 - B. Provide effective control over the creation, RECORD KEEPING (maintenance), use, and disposition of all records regardless of medium.

- C. Ensure that the creation of agency records is at the minimum level necessary for effective program operations.
 - D. Ensure that agency policies, decisions and procedures are accurately and adequately documented.
 - E. Prevent the unnecessary accumulation of records through application of a records disposition program throughout OSHA.
- X. Authorities. The policy and procedures in this manual are issued pursuant to the following:
- A. Federal Records Act of 1950, as amended (44 USC Chapters 29, 31 and 33, as amended).
 - B. Paperwork Reduction Act of 1995, as amended (P.L. 104-13)(44 USC Chapter 35).
 - C. Office of Management and Budget's OMB Circular A-130, Management of Federal Information Resources.
 - D. National Archives and Records Administration's (NARA) Records Management regulations (36 CFR Subchapter B).
 - E. Department of Labor's Records Management Program regulations (DLMS 1, Chapter 400).
- XI. Glossary of Terms. A glossary of common Information and Records Management terms is located in Appendix B.
- XII. Policy.
- A. All records of OSHA, regardless of medium, shall be filed in accordance with an approved filing system, filing scheme or naming convention. (Also see Chapter XV.)
 - B. Paper records shall be filed in accordance with OSHA Instruction ADM 12-0.1 or in accordance with regional filing systems approved by the OSHA Records Management Officer.
 - C. Special records (non-paper) shall be filed in accordance with approved filing schemes or naming conventions as specified in agency directives or, in the absence of specific instructions, as best suits the user's needs.

- D. All records of OSHA, regardless of medium, must be identified and scheduled for disposition on a Standard Form 115, Request for Records Disposition Authority, approved by NARA or, for certain administrative records, approved for disposition in accordance with the NARA-issued General Records Schedules (GRS). Any records not included on an SF-115 or in the GRS are unscheduled records and may not be destroyed until they are scheduled. For additional information about records disposition, refer to Chapter VII, Records Disposition.
- E. Records schedules authorize retirement of records to FRC's. Records will not be sent to an FRC unless they are covered by an item on a records disposition schedule. The media of the records is irrelevant. For additional information about records transfers, refer to Chapter VIII, Retirement of Records to Federal Records Centers.
- F. Only records relating to approved transfers of functions and realignments may be transferred or removed from the agency without an approved disposition schedule.
- G. All actions specified in an approved disposition schedule, including destruction, retirements, transfers, or removals, should be accomplished within 120 days of the scheduled time.
- H. Records system revisions may be made as follows:
 - 1. Revisions to paper or hard copy filing systems (except for subject expansions) shall not be made without the prior approval of the OSHA Records Officer.
 - 2. Revisions to electronic filing systems, naming conventions, etc. shall not be made without the approval of the OSHA Records Officer or the Director, Office of Management Data Systems.
 - 3. Changes to records schedules must be made by the OSHA Records Officer with the approval of NARA.
 - 4. Records not listed for disposition in approved records schedules must be submitted to NARA for approval by the OSHA Records Officer before those records may be destroyed. All unscheduled OSHA records, regardless of medium, must be treated as permanent records. See the NARA regulations at 36 CFR Subchapter B for specific requirements for paper, microform, electronic and other record media.
 - 5. Changes made to filing subjects under authority of this manual do not

apply to directive filing subjects. ONLY classify directives in accordance with the subjects specified in OSHA Instruction ADM 12.1 and not identified as records management subjects.

XIII. Responsibilities.

- A. Director, Administrative Programs. The Director monitors the overall administration of the OSHA Records Management Program.
- B. Controlled Correspondence Unit. The Head, Controlled Correspondence Unit, serves as the Program Records Officer for the Office of the Assistant Secretary.
- C. Directors of National Office Directorates and Independent Offices. Program Directors:
 - 1. Provide oversight for their organization's records management program.
 - 2. Appoint a Program Records Officer to manage, direct, and coordinate all records management activity within the organization. Notify the OSHA Records Officer of the appointment.
 - 3. Appoint Records Liaison Officers in subordinate offices, as needed.
- D. Administrators of Regional Offices. Regional Administrators:
 - 1. Provide oversight for the Region's records management program.
 - 2. Comments on proposed records systems, records schedules, and other records management matters affecting the region.
 - 3. Requests comments from OSHA field organizations on proposed records systems, records disposition schedules, and other records management matters and submits those comments to the OSHA Records Management Officer.
 - 4. Conducts reviews of regional records management practices as part of audits of regional administrative practices.
 - 5. Appoint a Regional Records Officer to manage, direct, and coordinate all records management activity within the region. Notify the OSHA Records Officer of the appointment.
- E. Area Offices. The Area Director shall appoint a Records Liaison Officer to

manage all records management activity within the area and notify the appropriate Regional Records Officer of the appointment.

F. Director, Information Technology. The Director:

1. Implements systems for backing up electronic records that guard against the loss of records information because of equipment defects, human error or theft.
2. Develops controls to prevent the unauthorized alteration or erasure of information in electronic documentary materials that serve as official records.
3. Maintains a complete inventory of all OSHA electronic RECORD KEEPING (computer) systems that are used to process agency records and electronic publications.
4. Determines how electronic records will be maintained to meet operational and archival requirements.
5. Develops and maintains sufficient documentation of programs for all electronic records systems to allow authorized offices to read and retrieve the data from OSHA's electronic records systems.
6. Assures information on magnetic media is destroyed or offered to NARA for retention in accordance with Agency records disposition schedules and the General Records Schedules.
7. Advises the OSHA Records Officer when developing and/or approving new electronic records systems or enhancements to existing systems.
8. Provides descriptions of electronic record systems to the OSHA Records Management Officer including suggested records disposition periods to be used in developing records schedules for electronic records.

G. OSHA Records Officer. The Director, Office of Management Systems and Organization serves as the OSHA Records Officer and:

1. Develops, manages and directs the OSHA Records Management Program.
2. Serves as the OSHA liaison with the Department, NARA, GSA, OMB, GAO, and other agencies on matters relating to records management.

3. Develops agency records management policies, procedures and operations that meet Departmental, OMB and GSA/NARA standards.
4. Issues instructions and other directives implementing agency records management policies, procedures and operations.
5. Conducts surveys and reviews of records management practices and operations including oversight of program and regional management of existing information systems. This includes RECORD KEEPING and records disposition practices.
6. Provides information and assistance to agency officials, employees, and contractors, as appropriate, in records management including RECORD KEEPING and records disposition practices.
7. Technical review of the National Office and Regional Records Management Programs in OSHA is the responsibility of the OSHA Records Officer.
8. For additional information on reviews, refer to Chapter X, Records Management Reports.

H. Program and Regional Records Officers. The designated Program or Regional Records Officer will manage and oversee all records management activities within their organizations. The Program or Regional Records Officer is responsible for:

1. Assuring organizational conformance to all requirements stated in the OSHA Records Management Manual and other records management-related directives.
2. Conducting records management reviews of subordinate offices to determine compliance with the Records Management Manual, records management instructions in other directives and with applicable file systems and records schedules.
3. Reviewing existing manual and automated information systems within their organization to ensure that RECORD KEEPING requirements are met and records disposition is properly accomplished. Proper disposition means:
 - Disposition of records in systems has been authorized.
 - The disposition schedule's instructions have been implemented.

- Any needed revisions of those instructions have been identified.
4. Suggesting changes in this manual, files systems, or records schedules to reflect changes in records operations, organizational functions, work flow, or records disposition needs of their organizations.
 5. Assuring all classified and limited access material including Privacy Act material is properly safeguarded and that the materials are properly disposed when their retention period is completed.
 6. Providing assistance to their organization regarding records management.
 7. Providing the OSHA Records Officer a biannual report of records management activities within the organization including changes in RECORD KEEPING or records disposition.
 8. Notifying the OSHA Records Officer of the appointment of Record Liaison Officers in their organization.
 9. Regional Records Officers serve as liaison with appropriate GSA and NARA regional organizations on records management activities.
 10. Technical review of directorate (including independent offices) or regional records management programs is the responsibility of Program and Regional Records Officers.
- I. Records Liaison Officers. Records Liaison Officers will manage and oversee all records management activities within their organizations. Records Liaison Officers are responsible to:
1. Assure conformance to the OSHA Records Management Manual, records management instructions in other directives and with applicable filing systems and records schedules.
 2. Provide technical assistance to their organization in files management, RECORD KEEPING practices, and records disposition.
 3. Suggest changes in records management directives, filing systems, RECORD KEEPING practices, or records schedules to the Program or Regional Records Officer.
 4. Properly safeguard and provide proper disposition for all classified and

limited access material in their organizations.

- J. Supervisors. Supervisors are responsible for appointing files custodians to manage the files.
 - K. Files Custodians. Files Custodians are responsible for performing files maintenance, RECORD KEEPING and records disposition activities and conforming to the requirements of the OSHA Records Management Manual for all documentary materials under their control, regardless of media.
- XIV. Approved Filing System. The subject-numeric filing system is the filing system mandated for use throughout OSHA, regardless of media.
- A. This system permits arrangement of the primary subject titles in alphabetical sequence while retaining a simple numeric order for the secondary (second) and tertiary (third) subdivisions of the primaries. Regional offices may create quaternary (fourth) subdivisions of primary subjects where necessary. The primary titles are given simple, easily remembered abbreviations where possible, such a PER for Personnel, BUD for Budget and LEG for Legislative and Legal.
 - B. A subject-numeric filing system is based on several major subject groups, each of which is designated by a primary subject abbreviation. The groups currently mandated for use throughout OSHA are contained in OSHA Instruction ADM 12-0.1, OSHA Classification System. Also, refer to Appendix F.
 - C. Exceptions to the use of this system must be approved by the OSHA Records Officer.

Chapter II

FILES MANAGEMENT

- I. Purpose. The purpose of this chapter is to provide a framework for OSHA managers and employees to understand how files should be managed throughout OSHA regardless of media. It makes no difference if records are paper, microforms, electronic, or audiovisuals, certain standards apply to all of them. This chapter delineates those standards.
- II. Filing Records.
 - A. Records should be filed on a regular basis, preferably daily to be sure the information is available for use.
 - B. Records management software may be used to provide a proper framework for managing all records. Electronic systems often use records or document management systems designed for their proper management and disposition. These systems are also available to manage and dispose of hardcopy records.
 - C. Paper, microform and audiovisual records need to be physically placed in their storage location as soon as possible after creation or receipt. Electronic or computer records, whether located in shared memory (in server files) or in hard or removable disks, need to be correctly identified, described and carefully filed in directories or disk files that are properly coded to assure their proper identification.
- III. File Stations. These are specific points where official copies of documentary materials including correspondence, reports, case files, and other documents, regardless of media, are maintained. File stations are usually set up so records of only one media is present. However, some file stations have multi-media collections of records. In these file stations, care must be exercised to be sure that all records, regardless of media, are not inadvertently treated as nonrecord materials. Offices may establish official file stations, as needed, to maintain records of the functions the office performs and identify where records relating to each function are filed, including the record medium.
- IV. Handling and Safeguarding of Classified Material and Administratively Controlled Information. Public access to Government information is in the best interests of a free society. However, classified material (relating to the national defense or conduct of foreign policy) or administratively controlled information (relating to individuals - subject to the Privacy Act - or materials dealing with sensitive activities of the Agency whose disclosure would not be in the public interest) must be protected against

disclosure. Instructions for handling and safeguarding classified material and administratively controlled information are located in Chapter IX.

- V. Files Classification Files classification is mostly about the proper filing and identification of correspondence and related records. Case files are generally self-classifying, but proper classification of correspondence files will require careful management. Paper files are the most critical, followed by electronic files. Regardless of the medium, however, some means must exist to lead the searcher to the files. This means files must be placed where they may be found or, more accurately, CODED in such a way so they may be retrieved.
- A. Classification Coding. Proper identification of records is essential for retrieval. The file code is very necessary for paper records but it is critical for electronic records. File codes in electronic media are usually 8 digits. However, Windows 95, Windows NT and Mac OS allow for longer file name as well as many applications. Using logical, consistent codes for subjects is very important.
- B. Determining Codes. Use the following techniques in determining the correct subject file classification:
1. Read the subject line, if any, first. But remember, this might not be the real subject.
 2. Look for key phrases or familiar terms used in the text and check these against the subject outline.
 3. Note the address and/or originator. The identification of either may help to establish the subject area with which the document is associated.
 4. Refer to previous correspondence referenced in the material to be filed.
 5. Ask technical personnel what subject or function the material deals with.
- VI. File-Coding Outgoing Documents. The originating office will select the subject classification from OSHA Instruction ADM 12-0.1, OSHA Classification System, or from Appendix G. If the proper classification of a document is not readily apparent, contact your program or regional records management officer for clarification or information.
- VII. Assembling the File. Assembly of the filing unit is very important to assure full documentation of Agency policy, decisions, procedures, and transactions. Make sure that each filing unit is complete. The unit contains all incoming or outgoing record copy correspondence plus all background information necessary to fully document the policy,

disclosure. Instructions for handling and safeguarding classified material and administratively controlled information are located in Chapter IX.

- V. Files Classification Files classification is mostly about the proper filing and identification of correspondence and related records. Case files are generally self-classifying, but proper classification of correspondence files will require careful management. Paper files are the most critical, followed by electronic files. Regardless of the medium, however, some means must exist to lead the searcher to the files. This means files must be placed where they may be found or, more accurately, CODED in such a way so they may be retrieved.
- A. Classification Coding. Proper identification of records is essential for retrieval. The file code is very necessary for paper records but it is critical for electronic records. File codes in electronic media are usually 8 digits. However, Windows 95, Windows NT and Mac OS allow for longer file name as well as many applications. Using logical, consistent codes for subjects is very important.
- B. Determining Codes. Use the following techniques in determining the correct subject file classification:
1. Read the subject line, if any, first. But remember, this might not be the real subject.
 2. Look for key phrases or familiar terms used in the text and check these against the subject outline.
 3. Note the address and/or originator. The identification of either may help to establish the subject area with which the document is associated.
 4. Refer to previous correspondence referenced in the material to be filed.
 5. Ask technical personnel what subject or function the material deals with.
- VI. File-Coding Outgoing Documents. The originating office will select the subject classification from OSHA Instruction ADM 12-0.1, OSHA Classification System, or from Appendix G. If the proper classification of a document is not readily apparent, contact your program or regional records management officer for clarification or information.
- VII. Assembling the File. Assembly of the filing unit is very important to assure full documentation of Agency policy, decisions, procedures, and transactions. Make sure that each filing unit is complete. The unit contains all incoming or outgoing record copy correspondence plus all background information necessary to fully document the policy,

decision, procedure, or transaction. Official file copies in a suspense or tickler file or those otherwise filed which relate to the subject matter of the file unit must be filed with the unit. Electronic file systems must, at a minimum, provide links between each related document. Electronic files should be arranged to provide a virtual folder that is the key unit containing the electronic documents as if it were an actual folder holding paper copies.

VIII. Linking File Elements. Linking of related materials is essential for documentation and disposition.

- A. Linking records in paper or non-electronic media is usually accomplished by placing related records together in the file. Sometimes in media such as microfilm, the linking is done by electronic indexing systems.
- B. In electronic systems, linking is always done by "tagging" using keywords, file linking as in relational databases, etc. to identify related documentation.
- C. In mixed-media files, the elements retained in electronic, videotaped or audio taped or paper media should be maintained physically in the paper file unit wherever possible. Where, because of size, media constraints, or other storage considerations, electronic or other media documents are maintained in a separate file location, the paper file unit must be annotated (linked) to direct the user to the appropriate additional files.

IX. Document Management/Recordkeeping Systems.

- A. Each file station must maintain its records, regardless of media, in accordance with a plan or system.

The system for paper records is the filing system contained in OSHA Instruction ADM 12-0.1.

Microfilm, photographs, videotapes, audiotapes, etc. will be organized and maintained utilizing a common feature employed in accessing the records. This might be a unit number; such as a photograph number or title, or an inspection number, company name, etc., as best suits the user's needs. Electronic indexing systems are often used to access these records through reference to the common feature used for filing.

Electronic records also must be arranged utilizing a common denominator. Electronic recordkeeping systems do not simply provide a location coding for each segment of the record. They require the system to physically store the record together in one location, something which electronic systems not designed for

recordkeeping purposes, such as E-mail systems and data base systems, among others, do not accomplish. Electronic recordkeeping systems also provide a filing structure as an aid to retrieval and disposition.

- B. Advice and assistance in organizing and managing such systems may be obtained from the OSHA Records Officer, the NARA web site (<http://www.nara.gov/>), and the ARMA Rio Grande Chapter web site (<http://www.flash.net/~survivor/>).

Chapter III

RECORDS DOCUMENTATION.

- I. Purpose. This Chapter provides guidance for the proper and adequate documentation of OSHA policies, decisions, organization, functions, procedures and essential transactions; that OSHA possesses a complete record; and that records are not accidentally destroyed, lost, or removed. This guidance applies irrespectively of the physical form or media used to provide a framework to hold the information or data.
- II. Goals. Agencies are responsible for creating and preserving records that adequately and properly document its policies, decisions, functions, organization, procedures and transactions.
 - A. Objectives. The reasons for documenting what the agency does, how it does it, why, where and who are to:
 1. Protect the legal, financial, and other interests of the Federal government and the people.
 2. Ensure continuity and consistency in administration.
 3. Assist agency officials and their successors in making informed decision.
 4. Provide the information required by the Congress and others for overseeing the agency's activities.
 5. Conform to the requirements of law relating to information disclosure.
 - B. Benefits. By creating and maintaining adequate and proper documentation, an office is able to:
 1. Reconstruct the development of the current management's and predecessors' policies.
 2. Furnish successors with information needed to understand past and current actions.
 3. Leave an enduring record of the office's accomplishments.
 4. Maintain a record of oral decisions and other unusual events. Significant decisions are often made orally by telephone or in conferences or

meetings. Such decisions should be documented in writing. All meetings or conferences should have minutes taken and filed along with a copy of the agenda and all documents that were considered at or resulted from such meetings as well as a record of decisions made.

III. Documentation Needs. The documentation required is dependent upon the complexity of the action, process, etc. being documented.

A. Documentation Requirements. By and large, most documentation requirements will be quite simple. The following examples show basic documentation requirements:

1. A routine request for information requires only the request and a note on the incoming request that the information was sent, assuming a copy of the request is maintained at all.
2. A requisition for supplies or services requires only the requisition including a description of the supplies, equipment or service requested.
3. A travel voucher requires the authorization, receipts and ticket stubs.
4. A purchase order requires the requisition, price quotation, and terms and conditions of the purchase.
5. A receipt for delivery of supplies requires only the receipt copy of the purchase order or requisition.
6. A directive clearance file requires the final clearances and the final original directive or requisition.
7. A policy clearance file (leading to a directive or other policy statement) requires documentation of why the policy is necessary, options considered, substantive drafts and clearances, and final policy statement.

B. Working Documents. Draft or working documents are generally NOT records. However, drafts or working documents which are essential to understanding the development of a policy or procedure are records and must be maintained with the final document or record. Questions should be addressed to the Program or Regional Records Officer.

C. Complex Document Requirements. Some agency actions, procedures, etc. are so complex and involved, that a great deal of documentation is necessary. Examples include public docket files, standards development files and State plan

development and management case files. Where this is the case and the records liaison cannot determine if the 5 "W"s are fully documented (What did the agency do, Who did it, How was it done, Where was it done and Why.), the file custodian or the records liaison should request a determination of the Program or Regional Records Officer regarding the proper documentation for the records.

- IV. Documentation Determinations. Where questions exist as to what constitutes adequate documentation;
- A. The file custodian should request an opinion of the records liaison or the Regional or Program Records Officer (RRO or PRO), as appropriate.
 - B. The RRO or PRO will decide what documentation is necessary for a particular records series if the record series has applicability only in the region or the national office directorate or independent office.
 - C. The RRO or PRO will request that the OSHA Records Officer issue a Documentation Determination when the RRO or PRO is not sure what documentation would be necessary or where the record series is in general use throughout the field or agency.
- V. Project and Case File Documentation. Project and case files can be simple or complex in nature. Their documentation needs are usually more complex than correspondence files and are more likely to contain multi-media materials. Documentation of case files and projects is very important in any organization. Case files and projects serve to identify and document at a point in time what the Agency is doing and how it is doing it.
- A. Case Files. Case files relate to a specific person, organization, process, or transaction, have a definite beginning and ending, consist of two types of records: Essential documentation and short-term documentation.
 - 1. Essential documentation is that which documents specific actions taken and decisions made. For example, a procurement case file's essential papers would include the purchase order, requisition, cost and performance information showing the goods or services purchased were sufficient to do the job at the lowest cost to the government, and other similar documentation.
 - 2. Short-term documentation, including working papers or copies, relates to materials that are not essential to show the history of the case file, materials that may be summarized in the essential documentation, or materials that are otherwise of little value. Usually this documentation is disposable when no longer needed for active case file management or

when the case is closed.

B. Project Files. Project files are a variation of case files. Projects usually are detailed studies of a particular matter and usually result in the preparation of formal findings, reports, or another type of product such as a manual, procedure, handbook, and the like. Projects often cover an extended period of time. Projects deal with important aspects of an agency's work to improve or change the manner in which that work will be carried out, what work is accomplished, the organization in which that work is carried out, and in several other ways. Projects provide useful documentation of the past history of an agency including policies, procedures, practices, and other activities; and show which were successful and which ones were unsuccessful and why.

1. Essential Documentation. Documentation characteristic of project files include some or all of the following:

- Project Proposals or Requests. These are developed internally or received from another source. They include contracts for consultants.
- Approvals.
- Feasibility Studies, if desired.
- Project Statements, Action Plans, and Other Similar Documentation. Shows what is to be accomplished, assigns personnel, and responsibilities.
- Interim Project Documentation. Includes status reports, meeting or committee reports, memoranda to the file, memoranda of telephone or face-to-face conversations, correspondence relating to the study or project (except transmittal letters), and the like.
- Final Reports. Reports, manuals, handbooks, procedures, and the like required after the fact finding and analysis phases have been completed.
- Project Implementation Reports. Includes implementation results and presentation scripts and materials, if any.
- User Guides or Instructions, if any.
- System Documentation Flow Charts.

when the case is closed.

B. Project Files. Project files are a variation of case files. Projects usually are detailed studies of a particular matter and usually result in the preparation of formal findings, reports, or another type of product such as a manual, procedure, handbook, and the like. Projects often cover an extended period of time. Projects deal with important aspects of an agency's work to improve or change the manner in which that work will be carried out, what work is accomplished, the organization in which that work is carried out, and in several other ways. Projects provide useful documentation of the past history of an agency including policies, procedures, practices, and other activities; and show which were successful and which ones were unsuccessful and why.

1. Essential Documentation. Documentation characteristic of project files include some or all of the following:

- Project Proposals or Requests. These are developed internally or received from another source. They include contracts for consultants.
- Approvals.
- Feasibility Studies, if desired.
- Project Statements, Action Plans, and Other Similar Documentation. Shows what is to be accomplished, assigns personnel, and responsibilities.
- Interim Project Documentation. Includes status reports, meeting or committee reports, memoranda to the file, memoranda of telephone or face-to-face conversations, correspondence relating to the study or project (except transmittal letters), and the like.
- Final Reports. Reports, manuals, handbooks, procedures, and the like required after the fact finding and analysis phases have been completed.
- Project Implementation Reports. Includes implementation results and presentation scripts and materials, if any.
- User Guides or Instructions, if any.
- System Documentation Flow Charts.

2. Short-Term Documentation. Possible types of working or non-essential documentation in case files include:
 - Voluminous collections of cards, questionnaires, interview notes, summary sheets, and other background materials involved in gathering and tabulating data.
 - Short-lived correspondence or documentation such as transmittal letters and other materials dealing with the routine administration of the case. This documentation has no more value than general correspondence-type transitory documentation.

VI. Assembly of Documentation.

- A. The record copy of correspondence, reports, studies, etc. must have all attachments, enclosures, background information, etc. filed together (stapled or otherwise fastened together for paper records) or otherwise have their location identified especially where different media are involved.
- B. Records where the official record copy is dispersed into different media. For example, the report or correspondence is in electronic media, attachments are video tapes under separate cover and background information is in hard copy or paper media. Regardless of the media, they are still all records; some are paper, some are audiovisuals and some are electronic. They are ONE record with parts of that one record in different media.
- C. Electronic media records are "assembled" by linking them together or identifying the locations of individual files to the record.
- D. The office MUST have a complete record in the official record copy. The unauthorized destruction, alienation, loss, or theft of official records of the United States is a crime. Do not think the designated record copy is the only official agency record. It isn't if another copy more completely documents agency policy, procedures, actions, transactions and the like.

VII. Official Records. Personal Papers and Nonrecords.

A. Official Records.

1. These are materials made or received either in pursuance of Federal law or in connection with the transaction of public business. Official records are public records and belong to the office rather than to the officer. Correspondence designated "personal," "confidential," or "private," but

relevant to the conduct of public business, is nonetheless an official record subject to the provisions of Federal law pertinent to the maintenance and disposition of such records. The removal of official records from Federal control is unlawful and subject to criminal penalties.

2. Those materials, created or accumulated by management officials, which deal with job-related activities are considered records of the Agency. They include but are not limited to materials relating to program policy and procedures development and implementation, appointment calendars, schedules, copies of awards, congratulations, invitations, thank you's and regrets, and the like which provide evidence of the official's job-related activities.
3. "Management officials" refer to the Assistant Secretary, Deputy Assistant Secretary, Executive Assistants, Program Committee Chairpersons (such as NACOSH), National Office Directorate and Office Directors and Deputies, Regional Administrators and Deputies and Area Office Directors and Assistant Directors.

- B. Personal Papers. Personal papers cover material pertaining solely to an individual's private affairs and do not affect the conduct of agency business. Personal papers, like records, may be in any media. Examples of personal papers include personal copies of personnel actions, employee copies of earning and leave statements, diaries, journals and other personal information that are not prepared or received in the process of transaction Government business.
- C. Nonrecords. Nonrecord materials often have many of the characteristics of records but they do not serve to document significant activities of the agency. These materials usually are not included in files as documentary evidence. Nonrecords include technical reference files, working files, convenience files (Not reading files), tickler files (another copy exists in the office) and similar information that does not document the work of the agency. Refer to Chapter VII for additional information.

Chapter IV

PAPER OR HARD COPY MEDIA RECORDS

- I. Purpose. This Chapter provides guidance for the proper maintenance and use of paper or hard copy records to assure they fully document OSHA policies, procedures and activities, are a complete and true record and are not accidentally destroyed, lost, given away or removed.
- II. Categories and Accessibility.
 - A. Paper records are usually harder to access than computer-generated records unless the volume of paper files is small. Because of the relative difficulty searching paper records, paper record systems usually contain either a computerized cross-reference or a paper-based cross-reference copy.
 - B. Paper records fall into a wide variety of subjects. However, they can be said to generally fall into 2 general categories: Correspondence or subject-related documentation and case file documentation. (For an explanation of these categories, refer to Chapter III).
- III. Required Copies for Paper Records. Make the first three copies for all paper records. The colors specified are optional. However, the purpose of the copies must be recognizable. The record copy must be either yellow or marked as the record copy. An exception may be made when records are produced on laser printers.

Note: When an electronic indexing system is in use, only the official record copy must be maintained.

 - A. Official File (Yellow or Marked Official File). This is the official file which includes all attachments, related incoming correspondence, background materials. In short, everything related to the subject. This copy can be either in a central area or in your possession. IF IT IS IN YOUR POSSESSION, IT IS STILL A RECORD, not your personal copy. If you have a personal copy separate from the official file copy and it is more complete than the official file copy, YOU HAVE THE OFFICIAL FILE COPY.
 - B. Reading File (Blue or Marked Reading File). This is usually a chronological file which is a cross-reference finding aid to the official file copy (the yellow copy unless a "personal" copy is more complete). The reading file copy tells where the official file copy is located by coding in the upper right corner (either the file code if the material is in the central file [subject or case] or, if the file is held elsewhere,

the name of the subject or case file and the name of the person having custody of the official file copy).

- C. Supervisory or Other Reading File (Pink or Marked For Purpose). The office or official supervising the office maintaining the record copy usually receives a reference copy of correspondence.
- D. CC's, Information Copies or Personal Copy (White or Xerox). Information copies are usually copies on letterhead paper (an "official" hard copy) sent to someone in another agency or in the private sector. This copy does not contain any drafters' legends. The personal copy might actually be the official file copy depending if the official file copy or the personal file is more complete and contains the complete history of the subject file or case.

IV. Coding Papers.

- A. Place the appropriate file code on the Upper Right Corner in Red ink or pencil on All copies. (OSHA's file classification subjects are found in OSHA Instruction ADM 12.1, OSHA Classification System, are outlined in OSHA Instruction ADM 12.4, Records Management Manual, Appendix D, Subject Outline for OSHA Instruction ADM 12.1, OSHA Classification System.)
- B. Mark the appropriate file coding, in red ink or pencil, on the upper right corner of the material.
- C. File the copies in the appropriate folder or other location.
- D. Maintain a listing of all filing categories used in your office. This list will help you retrieve materials and will help you classify records consistently.

Chapter V

ELECTRONIC RECORDS

- I. Purpose. This Chapter provides guidance to assure OSHA electronic records fully document OSHA policies, procedures and activities, are a complete and true record and are not accidentally destroyed, lost, given away or removed.
- II. Scope of Electronic Records. Electronic documents, spreadsheets, databases, graphics and similar data may be records, just as paper documents may be records. Any materials created on computers using word processing, spreadsheet, database or other programs may be records. The existence of these records on diskettes, hard drives, compact disks or other storage device, doesn't mean they may be destroyed when desired. The National Archives, at 39 CFR Part 1234, has set out regulations, including standards, governing the creation, maintenance and use, and disposition of electronic records, including permanent retention electronic records.
- III. Identification of Records. The introduction of microcomputers into offices has worked a great reevaluation of exactly what types of materials constitute records. At heart, a record is not paper or any other physical form.
 - A. A record is information. That record can be ink on paper - it can also be magnetic code on tape or disk. Electronic records can be identified by the use made of the electronic information.
 - B. Electronically created information in electronic mail systems, business graphics systems, digitized voice mail systems, office electronic message and calendaring systems, management information systems, and decision support systems may also be records.
 - C. The information must be reviewed and analyzed to determine if it is record or non-record material. Pending determination, electronic information must be considered to be records except for those types of information which consist of non-record materials. Eliminating them from consideration as records will leave those materials which are records and must be preserved until the end of their scheduled retention period.
- IV. Electronic Record Series.
 - A. Identification. Electronic records, like other records, are identified by common characteristics which are used to group them into specific categories or subjects. These categories or subjects are called record series. Specific record series can consist of financial records, administrative correspondence, program

correspondence, inspections, laboratory testing results and the like.

B. Retention.

1. The retention for automated records in a specific records series generally is the same as for related paper or non-automated records. While this is generally true, there are some exceptions. A record series is most usually linked to an item on a records disposition schedule or on the General Records Schedules.
2. The electronic data may be considered a copy of a hard copy or paper record. If a hard copy or paper record is not maintained, then the electronic copy is the record copy. The sole exception to this is permanent retention records.
3. Electronic media copies of permanent records must have a specific retention period in a records disposition schedule or they must be treated as a permanent electronic record.

C. Backup Copies. One record series that is limited only to electronic records is backup copies. These are not duplicate copies of the record. These are old versions of the record. For example, the old version of a word processing or spreadsheet file after the file has been updated. The old version is a record if there is valuable information in the old outdated version. Old versions of database programs used to draft and develop standards or regulations may contain valuable information.

V. Electronic Files Operations. Electronic records require strict controls on their identification, maintenance, retrieval, use and disposition. Electronic media is very sensitive and may be easily misplaced, destroyed or erased, or disclosed by accident.

Electronic records generally constitute their own finding aid. Use of cross-reference files, similar to the "blue" copy of paper records, is unnecessary and will not be done.

A. Organization of Electronic Media. Different computer operating systems organize and index data on electronic media in different ways.

1. Various functions may affect the status and integrity of records created on the computer. Saving the file currently in memory is one of these functions. A new record must be saved or recorded on the proper medium or it will be lost when the computer is turned off. Saving the previous version of a file is another specified function because the previous version is often erased and replaced with the new one. Copying and erasing files

on the computer may have a direct impact on electronic record integrity.

2. It is important for users to keep in mind that they may be creating, manipulating, and deleting official government records.

B. Electronic Mail (E-Mail). For additional information, refer to Appendix A, E-Mail Determinations

1. E-Mail messages, including attachments may be record or Nonrecord documentation. An e-Mail message must be analyzed, like any other documentary material, to determine its record status. (Refer to the records definition in Appendix B and the criteria for making records decisions and determinations in Chapter III.)
2. Where the message is determined to be of record character, does a paper copy exist?
 - a. If a paper copy was not made, the electronic message is a record and must be saved off the e-Mail system. It must be safeguarded by being placed in a "security directory or file" so it will not accidentally be destroyed.
 - b. If a paper copy was made, the paper copy is the record and the electronic copy may be destroyed.
3. The record of the e-Mail message, whether paper or electronic, must contain a record of the addressees and the sender and the date sent. If deemed necessary by the sender, the record must also include the date opened by the addressees or received by the addressees in their mailbox, if supported by the system.
4. If the e-Mail message is a record and if it is NOT covered by a records schedule item, it is an unscheduled record.

C. Current Files. Many computer systems will save information to a named file when requested. Some systems wait for a command to save a file; others save periodically; still others save based on quantity, such as a full page of text. Automatic file saves are also possible to many systems. Users must know how the system works to save files. Every user should think about how the computer's file save feature will affect the work created. For example, the user may not want to always change the old version of an application or data file and may also never want to destroy the previous version of a file. The user must think very carefully and determine if destroying the file version will destroy a record that must be

maintained to document agency policy, procedure, and the like.

D. Filing Electronic Documents

1. The directory and sub-directory structure used to file documents should be similar to the file system contained in OSHA Instruction ADM 12-0.1 used to file paper documents.
2. Electronic documents and paper documents relating to the same or similar functions should be filed using the same or similar subjects. A memo relating to inspections would be filed under Compliance 2 for paper records. Electronic memos relating to the same subject could be similarly filed. The directory structure could be similar to the following:

Figure 5-1
FILE SYSTEM STRUCTURE

Paper Record Filing Structure	Electronic Record Filing Structure
Filing Cabinet Drawer	C:\ files_98
CPL COMPLIANCE FY-98	cpl_98
CPL 2 Inspections FY-98	2_insp
Individual File	Individual File

3. The electronic records could be filed in the sample directory structure on the right. Be sure each directory title includes the year.
4. Nonrecords could be filed in a folder labeled "Nonrec" or simply destroyed and not filed at all.
5. Assignment of the disposition period from the appropriate disposition schedule can be made to each folder. The directory title provides the year the documents were created. The subject classification will provide the disposition. Assure the proper retention period is applied to each document (file) in the directory or subdirectory at the time it is "filed" to assure proper disposition.
6. Continue adding files to the appropriate directory or subdirectory for the remainder of the year.

7. At the end of the year, add another set of directories only correct the titles of the new directories to reflect the new year.
 8. When the files in a particular directory have reached the end of their disposition period, simply erase the directory. The files in the directory will be deleted from the file directory or the disk. If complete and total erasure of the file from the media is necessary, obtain and use a commercially available overwrite utility program to repeatedly overwrite the file .
- E. Overwritten Files. When a file already exists on a specific medium, such as a diskette, under a specific filename/extension, e.g., "SAMPFILE.DBM," a revision of that file may replace the old file. The last revision of a saved file may take over the exclusive use of the filename/extension. Two or more files with identical names would confuse the computer and the user.
1. Some microcomputer systems render the old file "transparent" to the user. The old file still exists on the electronic medium, but the file's name has been removed from the directory and the file has become inaccessible to the user. However, the file still exists on the file medium and can be accessed with the right know how and software.
 2. Some systems allow the conversion of the old file into a backup file. It allows not only the current version of the file but a last previous version backup file. Previous versions will then become transparent to the user. The backup file will usually have the same file name but a different extension. The last previous version backup file will be accessible to the user but the previous backup versions will not be accessible to the user although the data is still on the media.
- F. Copied Files. Most computer file-copying functions have a clear problem area with a direct impact on record integrity. The problem is rooted in the file-overwrite concept outlined in paragraph c. above.
1. When a file is saved and then copied to another file on a hard disk or to a diskette, two copies of the file will exist with identical filenames and extensions. As the working copy of the file is modified and saved, it may also be copied to another location at the end of each update cycle. Two versions of the file are always available: the current one and its predecessor. This file multiplication can continue indefinitely as long as file space is available.

2. The problem in file management arises when the copy procedure accidentally occurs in the wrong direction. A systems user may make backup copies onto a floppy disk or loads a backup copy from a floppy to the hard disk. Then the latest copy of a file is replaced with the preceding version of the same file. Loss of valuable information, formats, editorial changes, author time, and editing can result. If the most recent copy of the file can be reconstructed, the user wastes time and experiences frustration. If it cannot be reconstructed, the damage can be incalculable.
- G. Erased Files. When a user erases a file by filename, there is normally no problem with file integrity. There is no doubt the user intended to destroy the file. If the computer system actually erases the file, there is no problem with file integrity. However, many systems do not erase the file, they merely erase the filename from the system directory. This allows the space occupied by the file to be used to store other files since the system recognizes that space is available for a new file.
- H. File Security.
1. In most instances of file erasure, pressing the "delete" key is acceptable to delete files.
 2. Users should be aware that in most cases of electronic erasure of files, only the directory entry is erased while the file is still on the medium and may be accessed by anyone employing the requisite commercially available file recovery software. Just because the computer says Privacy Act, policy determination, FOIA-exempt, trade secret and other limited access records have been erased does not mean they cannot be relatively easily retrieved from the medium. Users must be sure that classified and limited access materials on magnetic media cannot be retrieved by unauthorized persons.
 3. If your computer contains sensitive information and you need to remove the information from your computer, contact OMDS for assistance in removing the files or in obtaining the proper software to allow you to fully erase the files yourself.
- I. Status of Files/Data in Active Memory. Electronic records generally have less stability than paper or microform records. Users should frequently make backup copies of their files to support the integrity of the electronic records. The credibility and often the legal acceptability of information in electronic records is directly related to the documented procedures for preserving the electronic record's integrity and to periodic reports on the regular practice of those procedures. Regardless of whether backup copies are made automatically,

administrative backup procedures should be established. Standardized procedures are the keys to effective control.

J. Backups of Files. All microcomputer systems allow backing up files, programs or the entire hard drive. Backups should be done to assure the information on the computer is safeguarded against accidental loss. Backups typically save the file, program or entire hard drive on the computer to another location, usually another directory for file or program backups or to another drive on a LAN for system backups. Contact OMDS for information on system backups.

K. Labeling and Indexing.

1. External Labels. Labels are essential for using electronic records. Labels intended for use on floppy disks (on the paper jacket) should include the name or abbreviation of the originating office, diskette title, begin and end dates, software application (such as Lotus, WordPerfect, dBASE, etc.), and the type of computer it was produced on. Computer generated magnetic tape labels should include the volume/serial number, the name of the sponsoring program office, and the data set names. Access restrictions should also be placed on the label.
2. Internal Labels. Document, file and directory naming conventions for internal labels should be easily understandable and standardized so that authors and their colleagues or successors can find and use information stored on disks or tapes. Labeling, naming and filing conventions should be simple. One simple but effective system is to file similar documents created during a set time period in the same place such as on the same labeled floppy or in the same directory on a hard disk.
3. Indexing. Indexing is a relatively simple (although more complex than labeling) way to find electronic documents if a filing system is not used. Indexing of documents by offices is optional.

An indexing system should require the document creator to indicate the name of the document, the addressee, the date, and the identifier of the disk on which it is stored. An abstract of the document may also be useful.

The index can be printed out, stored in magnetic media on appropriate application software, on index cards or using some other method. The amount and complexity of information in the electronic files will determine if indexing is necessary and, if so, what kind of labeling and indexing system is needed.

For additional information and assistance, contact your Regional or Program Records Officer.

- VI. File Types. Electronic records may be said to fall into three main categories: Word processing, spreadsheets and databases. These categories define the relative value of electronic records or data. The records in each category may also span the range from trivial to permanent, depending on the subject and worth of the material in the electronic system.
- A. Generally, information which is part of a system where the information may be manipulated or massaged, rearranged, or otherwise changed in presentation, format, etc. is more valuable as data than information which is not subject to manipulation.
 - B. While administrative function data bases are treated as extra copies of hard copy records, program data bases are not. Even if a program data base duplicates program records, that data base is a record and cannot be considered a non-record copy of the hard copy or paper record.
 - C. Word processing, spreadsheets and indexes generally do not have information in them which must be maintained simply because it is in electronic form. Information in word-processing and spreadsheet programs has equal value to the hard copy output of those programs.
- VII. Access to Records. This paragraph deals with an area of great importance for the use of electronic records: "Who has access to the information in electronic records and under what circumstances?" The Freedom of Information Act (FOIA) and the Privacy Act have as great an impact on access to electronic records as they do on hard copy or paper records. The Electronic Communications Privacy Act covers access to electronically transmitted information. The FOIA provides public access to information on Federal government activities. The Privacy Act pertains to records kept on individuals and requires Federal agencies to prevent the misuse of data about individuals and ensures a person's right to know the purpose and use of information assembled regarding him. The Electronic Communication Privacy Act pertains to the intentional interception, use or disclosure of electronic communications and the penalties for interception, use or disclosure.
- VIII. Judicial Use of Electronic Records. This is an important area with many implications for the use of electronic records: The rationale, procedures and rules for authenticating electronic records for judicial actions.
- A. Legal standards for the acceptability of records other than paper records as evidence have been slow to evolve. The Federal Rules of Evidence provide a

guide to admit records with a variety of contents and forms into evidence in the courts. However, each judge is free to admit or dismiss evidence on the basis of the court's independent evaluation.

- B. The court must have evidence that the records are trustworthy. They must clearly and accurately relate the facts as originally presented or in summary form.
- C. Electronic records, however, contain systemic vulnerabilities not found with paper records. Additional evidence must be presented to assure the court of their trustworthiness. The Federal Rules of Evidence (Title 28 of the U.S. Code) serve as the primary guide for evidence submitted to a Federal court. The three rules that relate to electronic records are Rule 803(6) and (8) in Article VIII, Hearsay, and Rule 1001 and Rule 1006 in Article X, Contents of Writing, Recordings, and Photographs. (See Figure 5-1.)
- D. Electronic records may be acceptable to the courts. The way in which electronic records are created places them at greater risk than paper records. Ensuring the trustworthiness of an electronic record has added importance. The following reliability or trustworthiness concerns are intended to provide a framework for the user to assure his records are acceptable.
 - 1. The user may be required to present evidence the equipment was working properly on the day the computer record was prepared. A computer operations log indicating the absence of any malfunctions is generally adequate.
 - 2. Output errors frequently result from errors in the initial data entry. Procedures for verifying or proofreading data entered into the system should be in documented.
 - 3. The reliability of computer records is enhanced if an accurate audit trail is provided to indicate the sequence of events followed in processing the data and the methods used to prevent loss of data.
 - 4. Software reliability is important in demonstrating reliability of the data. Errors in data can occur from errors in programs. The user may be required to present evidence related to the development and testing of programs. In this event, contact the office responsible for program development or implementation.

Figure 5-2

JUDICIAL RULES RELATING TO ELECTRONIC RECORDS

Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

(6) Records of regularly conducted activity

A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

(8) Public records and reports

Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed

pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (~) in civil actions and proceedings and against the Government in criminal cases, factual finding resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

Rule 1001. Definitions

For purposes of this article the following definitions are applicable:

(1) Writings and recordings

"Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(2) Photographs

"Photographs" include still photographs, X-ray films, video tapes, and motion pictures.

(3) Original

An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

(4) Duplicate

A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original.

Rule 1006. Summaries

The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

5. Computer printouts prepared in the ordinary course of business are perceived as having higher trustworthiness than printouts prepared for

trial. However, if the user can show an adequate audit trail leading to data creation and merely a time lag before printing. No adverse consequences should result.

6. An increasing number of records are being created and utilized electronically without conversion to paper and without ever receiving formal signatures. Electronic record generation makes affixing a signature difficult from a technical standpoint and undesirable from a records management standpoint. Solutions include maintaining two files; one electronic and one paper, authentication programs for electronic signatures, or simply doing away with signatures on many documents.
7. Records disposition schedules have an important bearing on court proceedings. They limit the time an agency must provide records to a court. The fact that a record is scheduled helps prove the record was produced as a regular practice of the agency. Lack of a records schedule authorizing disposition could be construed as showing the record was not produced during the regular course of business. Federal courts accept the defense that records are not available since they have been disposed in accordance with an approved records disposition schedule.

IX. Security of Electronic Records. Security for the electronic records created, used and stored on microcomputer or personal computer (PC) systems has become an important issue. Mainframe computer systems have traditionally had considerable protection but PC systems have not because they have been treated as single-user devices. Due to this traditional treatment, the security weaknesses of PC systems may threaten the confidentiality, integrity or availability of electronic information.

A. Objectives. Successful electronic records security requires a balance among the following objectives:

1. Confidentiality of personal, proprietary or otherwise sensitive electronic records handled by the system.
2. Integrity and accuracy of electronic records and the processes associated with them.
3. Accessibility of electronic records systems and the electronic records or services they support.

B. Media Destruction.

1. Magnetic media, such as disks, diskettes and tapes, that contain sensitive,

classified, Privacy Act or FOIA-exempt electronic records should not be discarded in regular waste containers, given to other organizations for reuse, or declared excess property. They should be cleared by degaussing and reusing or rendered useless by shredding or burning.

2. Defective or damaged magnetic media used for sensitive, classified, Privacy Act or FOIA-exempt records should be degaussed at least twice before being returned to the vendor.
3. Periodically defragment your hard drives and erase the free or empty space on the hard drive.

C. Lack of Security Lockouts. Most PC's and application software does not isolate or lock out unauthorized users from systems, application and data files. This can be especially troublesome on local area networks (LAN's). Some database systems do provide security to data files. However, many of these lockout features may be circumvented by knowledgeable users or intruders. Without security lockouts, users cannot be prevented from accessing or modifying parts of the records system and intended security for the information may be circumvented. This may be alleviated somewhat by the institution of security procedures regarding access to the hardware.

D. Computer Diseases. Computers attached to LAN's and other computer communications or network systems are particularly vulnerable to computer viruses. These nasty little programs usually attach themselves to systems or execution programs. Some also attach to the boot sector of disks and diskettes. All computers are vulnerable to computer diseases. To avoid problems with loss of data or impaired computer function, computers should be protected by antivirus programs to detect and destroy the virus.

X. Disposition of Electronic Records. Disposition of electronic records must be done in accordance with approved records disposition schedules, either GRS or agency-initiated. For additional information on disposition, refer to Chapter VII.

A. General Electronic Records. Electronic records in data processing systems, spreadsheet systems, graphic systems, administrative databases, and the like may be disposed of in accordance with the disposition authority affecting the paper or non-automated copies of the information. The General Records Schedules provide the authority to dispose of the above-mentioned automated records. Information or data in program-related databases is an exception.

B. Program-Related Database Records. These automated records must be specifically approved for disposition. If they have not been approved for

disposition specifically as automated records, they may not be destroyed. This includes database records which have been completely automated and hard copy or paper is no longer produced. These records are considered by NARA to be new records series and must be re-approved for disposition. Database records include data files for application software such as Access, Foxpro, FileMaker, dBASE, RBase, and Informix. (For data base records dealing with ADMINISTRATIVE subjects, see paragraph A., above).

Chapter VI

MICROGRAPHIC RECORDS

- I. Purpose. This Chapter provides guidance to assure OSHA records fully document OSHA policies, procedures and activities, are a complete and true record and are not accidentally destroyed, lost, given away or removed.
- II. Micrographic Records Media. Microforms are a medium which uses a reduced-size positive or negative image on film to record information.
- III. Types of Microforms. Microforms generally come in four varieties of film and four file formats. Microforms are increasingly being replaced by Compact Disk technology for active information storage. They are increasingly being used for archival or long-term inactive storage.
 - A. Varieties. There are several varieties of microforms:
 1. Silver-halide (like camera film).
 2. Diazo (blue background with clear areas for information).
 3. Vesicular (gray background with foggy information areas).
 4. Updatable (images may be added and some versions allow deletion of images).
 - B. Formats. There are several microform file formats are:
 1. Roll film (a roll of film similar to 16 mm camera rolls).
 2. Fiche (usually similar to a 4 by 6 or 5 by 8 inch card).
 3. Microfilm jacket fiche (like a fiche except with "channels" of clear plastic over a plastic base which are designed to hold roll film). The film usually relates to the same case or subject as a unit record.
 4. Aperture cards (similar to a tab card usually with one large image, usually a picture or drawing). This card is not in general use any longer. It is usually used for architectural drawings or blueprints.
- IV. Maintenance and Disposition. In the past, information was microfilmed to save space

and increase file integrity. The materials microfilmed, because of the high cost of preparation and filming, were records with either permanent or at least very long retention periods. Today, microforms are usually used for reference materials such as catalogs and records such as general correspondence, case files, and converted long-term or permanent electronic records..

- A. Temporary Records. The use of microform records does not present any records maintenance or disposition problems for records assigned a disposition period of less than 30 years. The records may be filmed and maintained in any environment using any file format and film variety. The disposition of such microfilm records is made in accordance with the instructions of an approved records disposition schedule. If the schedule was approved for paper or another record medium, except automated records, and the microform copy replaced the paper or other medium copy, the disposition period may be applied to the microfilm copy. For microform records having a retention period of 30 years or more, apply the standard for permanent microform records outlined below.
- B. Permanent Records. Permanent retention microform records have certain restrictions placed on their creation, maintenance and use, and disposition since microforms are fragile over time. They cannot be guaranteed more than 30 years unless stringent precautions are taken to preserve them. The National Archives, at 36 CFR 1230, has set out regulations, including standards, governing the creation, maintenance and use, and disposition of microforms, including permanent retention, microforms.
- C. Other Copies. Extra copies of microform records are non-record copies and may be discarded as non-records consistent with security requirements. Microform copies of permanent records in another medium must be handled differently. Because permanent records are for permanent retention and may be accidentally lost, all copies of them in other medias must be listed on records disposition schedules to be eligible for disposition. If a microform copy of a permanent paper record, for example, exists and is not listed on an approved records disposition schedule, it may not be destroyed but must be maintained as if it were a permanent record until it is listed for disposition on a records disposition schedule.
- D. Record vs. Non-Record. Microforms used in offices that are:
 - 1. Created or accumulated by those or other offices to document OSHA policies, procedures, transactions, and the like are records and must be disposed in accordance with an approved records disposition schedule.
 - 2. Accumulated by OSHA offices to be used as reference sources such as

magazines or journals reproduced on microforms by commercial enterprises are non-records and may be disposed of when they are no longer needed.

- V. Legal Considerations. Microforms, to be admissible in court, must meet the requirements of the evidence rules outlined below.
- A. Each roll, fiche, etc., must contain a statement that the filming is done in the routine course of business (Filming is always done for the record series in question and the routine followed in filming, editing, etc, is followed for all records in that series.), the date filmed or beginning and ending dates filmed if the file format is fiche, and the name of the filmer.
 - B. The filmer and/or custodian must certify that the record is complete and records have not been deleted in the routine course of business. Images have not been deleted except in accordance with an approved records disposition schedule.
- VI. Security and Integrity. Like other records, the security of limited access materials must be protected and the integrity or accuracy and completeness of the records must not be compromised. Microform records must be maintained and handled with special care since the record is miniaturized and is fragile. Accidents do happen to records. This can be a problem since miniaturized records are not readily identifiable as the information cannot be read directly by eye but must be enlarged by optic or video systems.

Chapter VII

DISPOSITION

- I. Introduction. Disposition means the disposal (destruction), retirement, transfer, or conversion (to another media) of records.
- II. Objectives. The objectives of records disposition are to:
 - A. Provide for the permanent retention of records necessary to document Agency:
 1. Organization and administrative development.
 2. Policies and procedures.
 3. Substantive functions.
 - B. Maintain a sound disposition program through proper control of records.
 - C. Promote a prompt reduction in the volume of records not eligible for destruction by retirement to an FRC.
 - D. Provide for the prompt and systematic destruction of records having no further value.
- III. Timely Disposition. Systematic records retirement or disposal is essential if materials needed for current operations are to be retrieved quickly and easily. Files clogged with unneeded material are difficult to use as well as expensive to operate.
- IV. Records Disposition Schedules. All existing Agency records disposition schedule items dealing with administrative and program function records remain in effect.
- V. Yearly Review of Records. Before the end of each fiscal year, file custodians will review all files in their custody, and segregate the inactive records which will be eligible for retirement, disposal, or other disposition at the end of the fiscal year. The usual time to make these determinations is the month of August. The simplest method of segregating files is to group them by category: Nonrecord, records of limited retention, and permanent records. Electronic records eligible for retirement or transfer should also be marked or otherwise identified.
- VI. Disposition of Records in Offices.

- A. Unclassified Records. Destroy in accordance with the applicable item of a records disposition schedule. No precautions need be taken regarding recovery of the records unless they are administratively controlled material.
- B. Administratively Controlled Material.
 - 1. Dispose of Administratively Controlled Information including material subject to the Privacy Act (does not include classified materials) on the basis of subject content and the applicable item of a records disposition schedule. However, the METHOD of disposition must be by tearing into small pieces (shredding), burning, or other means preventing recovery of the information.
 - 2. The destruction must be witnessed by an OSHA employee if it is performed by a non-Federal entity such as a city government, private paper pulper, and the like. Destruction carried out by another Federal agency need not be witnessed.
- C. Classified Material. Dispose on the basis of subject content and the applicable item of a records disposition schedule. However, the METHOD must be in accordance with the provisions of DLMS 2, Chapter 300, Paragraph 380.
- D. Disposal of Records after Conversion to Another Media. Do not dispose of records that have been converted to another media until disposition approval has been granted by the OSHA Records Officer.

VII. Transfer of Records to the National Archives.

- A. Direct transfers of records usually consist of older records (more than 25 years old), possibly valuable records no longer being created, or records which must be safeguarded such as master copies of computer tapes, microfilm rolls, motion pictures, and similar records. Generally, most permanent records are offered to NARA after storage in the WNRC or FRC as provided in approved Agency records disposition schedules. However, permanent retention electronic records are usually transferred as soon as possible after the cutoff.
- B. Direct transfers must be made in writing to the OSHA Records Officer for review and approval. The OSHA Records Officer will send a request to the Departmental Records Officer for review and submission to NARA.
- C. The transfer letter must include the following information:

1. Identification of the subject matter.
2. Date span of the records.
3. Statement of how the records were used.
4. If they are not textual records, their physical characteristics such as motion pictures, sound recordings, video records, cartographic records, computer tapes, microfilm cartridges or fiche, and the like.
5. Volume of the records.
6. Arrangement of the records.
7. Existence of indexes or other finding aids, if any, and if they are included in the offer.
8. Physical condition of the records (excellent, good, poor).
9. Statement of any restrictions on use, such as security classifications or Privacy Act restrictions.

VIII. Transfer of Records to Federal Agencies Outside the Department.

- A. Approval Required. Advance written approval is required when the ownership and custody of records are to be transferred from OSHA to a Federal agency outside the Department, except as stated in paragraph 2, below. Request approval from the OSHA Records Management Officer and include the volume of records (cubic feet), a full description of the records, and the reason for the transfer. The records may be transferred after written approval is received.
- B. Approval Not Required. Advance written approval is not required when:
 1. The records are loaned for official use.
 2. The records are transferred to a FRC or the WNRC.
 3. The transfer of records or functions, or both, is required by a statute, Executive Order, Presidential or Departmental reorganization plan, or specific determinations made thereunder.

IX. Records Donated For Preservation and Use.

- A. Permissible Donations. Disposable records may be donated to an institution, a corporation, or a person. Requests for records may come from State and local historical societies or archival institutions. Only records that have been authorized for destruction and have reached the destruction date may be donated. If the authorization has not occurred or the destruction date has not been reached, the donation amounts to illegal destruction of records and, as such, the donor may be subject to criminal penalties.
- B. Conditions for Donation. Donations are made under the following provisions:
1. It must be agreed, in writing, that the records will not be sold to third parties.
 2. Transfer to the applicant is made without cost to the Government.
 3. Do not donate records containing information the revelation of which is prohibited by law or which would be contrary to the public interest.
 4. No transfer to a foreign government is made unless it demonstrates that it has an official interest in the records.
 5. No transfer to a person is made unless the records involved are directly pertinent to the custody or operation of properties acquired from the Government such as buildings, machines, vessels, plants, or other items of real or personal property.
- C. Approval of Donation. All requests for proposed donations of OSHA records to non-Federal custody must be submitted to the OSHA Records Management Officer for review and approval. The OSHA Records Management Officer will submit the request to the Department Records Officer for review. The Department Records Officer will report the donation to NARA. The request must show:
1. The operating unit of OSHA that created the records or had custody of them.
 2. The name and address of the recipient of the records.
 3. Descriptive data about the records: Series identification with inclusive dates, the records disposition schedule and item number(s) or other disposal authority.

X. Nonrecord Materials Disposal List.

This list describes items which may be destroyed as nonrecord material. Although these items are useful in daily operation and may appear to acquire record character because they are involved in daily activities, they do not serve to document the procedures, practices, or operations of the Agency. These materials may be disposed of at any time.

- A. Employee Activities. Materials documenting employee activities (such as employee welfare activities, credit union activities, savings bond drives, charitable fund drives, and public interest notices and activities) are not involved with Agency mission or support functions. They are nonrecord and may be disposed of at any time, unless otherwise stated in records disposition schedules.
- B. Extra copies of Security Papers. These copies may be destroyed as nonrecord material. Method of destruction is the same for extra copies of these papers as with official copies.
- C. Extra Copies of Unclassified Papers. Because the official files contain the record copies for documentation purposes, extra copies are nonrecord and may be disposed of at any time, unless otherwise specifically provided for in records disposition schedules.
- D. Letters of General Inquiry. These letters do not involve substantive questions and, when answered, complete the cycle of correspondence and have no further value. Examples: Requests for and transmittals of publications, photographs, and the like. Destroy when reply is made or information is furnished. OPTIONAL METHOD: Return letters to the originator along with the requested material.
- E. Mailing Lists. These include individual cards or computerized lists and may be destroyed when obsolete.

EXCEPT: When documenting distribution of a record such as a letter or memo or an e-mail record.
- F. Notification of Change of Address. Destroy when the change has been made in the records.
- G. Personal Files. Files maintained by an individual for the personal management of his affairs and including documents such as travel papers, travel vouchers, employee copies of time or leave records, employee copies of personnel actions, salary and allowance papers, and the like, already documented in official files. If they are forgotten by a departed employee, they may be mailed to the employee's forwarding address. If the employee does not want them, the materials may be

destroyed as nonrecord material.

EXCEPT: Offices may require individual travelers to attach original travel voucher receipts to the travel voucher. Employees should maintain copies to meet their needs.

H. Publications. Books, circulars, catalogs, trade journals, periodicals and other library-type materials which are given general public or Government wide distribution and which require no action and are not part of an official file are nonrecords. All such published materials may be destroyed when superseded, obsolete, or otherwise not needed.

EXCEPT: Newspapers and magazine clippings and abstracts from them pertinent to Agency programs or which document Agency missions should be combined with Agency files. All reference aids and expendable published material should be reported as excess property.

EXCEPT: Publications originated by your office. These are covered in the Agency filing and records disposition systems.

I. Reading Files, Chronological Files, Index Files, and Other Files Used as Cross-Reference Finding Aids. Index files are made up of extra copies of correspondence, letters, and memoranda, arranged by date, number, or organizational element. Reading or chronological files are arranged by date and are used as cross-reference filing aids. Since these files constitute duplication of subject matter already in official files, cross-reference and index files should be destroyed as nonrecord material.

EXCEPT: Reading or chronological files are official records when they: 1) are the Assistant Secretary's reading file, 2) index files that are an integral finding aid to the record (electronic index files are valuable in themselves and may be records), or 3) where no record copy files are maintained by the office.

J. Reproduction Materials. These include any device which performs the function of causing production of printed copy, such as mimeograph stencils, hectograph or ditto masters, ozalid, multilith, or offset plates. Destroy upon completion of the production job. If it is anticipated that a reprint will be needed, they may be retained for that purpose.

K. Routine Reference and Control Papers. These include job control records, status cards, routing slips and the like used for control purposes. Dispose when work is

completed or when no longer needed for operating purposes.

L. Routine Transmittal Sheets. These include letters or memorandums transmitting materials and either contain no information of value or cease to possess value after the material has been received by the recipient. Destroy after the recipient has received the material transmitted.

M. Stenographic Notes. This material, including filled notebooks, recording discs from stenographic machines, and steno tape recordings are of no value when the text has been satisfactorily transcribed and may be destroyed at that time.

EXCEPT: Those produced by advisory or other committees and hearings are records. Those which are not transcribed are records.

N. Stocks of Superseded or Obsolete Blank Forms and Processed Documents Preserved for Supply. Destroy when obsolete or superseded.

O. Suspense Files. These are extra copies of documents which serve as reminders of action due on a certain date or other indicators of a chronological or sequential character which do not acquire a record character from this function. They may be destroyed when action is completed.

EXCEPT: Where the record copy is used as the suspense copy.

P. Work Papers. Rough drafts, notes, figures and calculations, and the like, which an individual uses in preparation of a letter, report, or other finished product may be disposed of when the product is satisfactorily completed and approved.

EXCEPT: Those necessary for a complete understanding of the finished product or that are needed to fully document decisions, calculations and the like.

Q. Working Files. Folders which contain notes, reference material, duplicates of papers in official files, and other related papers used by individuals in day-to-day operations in their work are nonrecord. These are papers of temporary or transitory value which are primarily used as reference or background material but retention of which is not required as supporting evidence of an official policy, administrative or program operation or procedure, or transaction. They may be destroyed at the discretion of the individual who created them.

EXCEPT: That necessary for a complete understanding of the finished product or are needed to fully document decisions and the like.

- R. Wrappers, Labels, Envelopes, and Routine Routing Slips. Destroy immediately. EXCEPT: Envelopes which list the time and/or date of mailing and/or show the time and date of receipt when necessary to document a file, such as sealed bid envelopes documenting a contract file, may be retained with the file.

Chapter VIII

RETIREMENT OF RECORDS TO FEDERAL RECORDS CENTERS

- I. Selecting Records. Records are identified in approved records schedules as being eligible for retirement to an FRC
 - A. Records should be transferred to FRC's in annual blocks whenever possible. File custodians should survey their files NO LATER THAN AUGUST 31 of each year, identify those inactive records which will be eligible for retirement on SEPTEMBER 30 and separate them by disposition schedule item. The schedule item will identify those records eligible for retirement. A minimum of one (1) cubic foot (one box) per accession is required to initiate retirement. One accession equals the records disposable under one item on a records disposition schedule and dated in a particular fiscal year. Records are maintained by calendar, leave, or fiscal year depending on the type of record.
 - B. Make a note of the media of the records you propose to retire.
 - C. Do not send nonrecords to the FRC. (See Nonrecord Disposal List, Paragraph B of this Chapter.)
 - D. Do not send records with less than 1 year retention remaining before destruction to the FRC. All requests for exemption must be accompanied by a complete justification statement.
 - E. The accessioning paperwork (SF-135) should be sent to the FRC at least three weeks before the end of the fiscal year.
- II. Preparing Records for Transfer.
 - A. Available Containers.
 1. Standard containers. The box used to transfer records to the FRC is the records center box or carton measuring 14-3/4 x 12 x 9-1/2 inches. Each carton holds approximately 1 cubic foot of records. This box is available from GSA stores and warehouses.
 2. Nonstandard containers. Special boxes are available for retiring special kinds of records such as index cards; microfiche, and magnetic tape. Contact the FRC concerning use of these boxes before retiring the records.

B. Obtaining Records Center Boxes.

1. Letter- and Legal-size record containers. There is one letter and legal size record box available.

<u>National Stock Number</u>	<u>Description</u>	<u>Unit of Issue</u>
8115-00-117-8249	Box, Record (Tuck - bottom) 14-3/4 x 12 x 9-1/2 inches	25 per bundle

2. Other size record containers. There are several boxes available for retiring special kinds of records. Contact the FRC for acceptable boxes.

C. Packing Records.

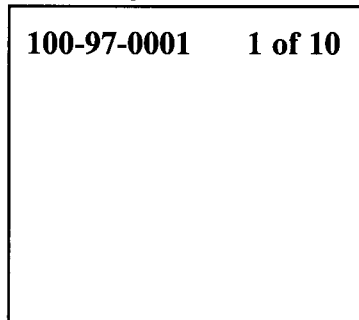
1. Remove nonrecords and records eligible for destruction from the records to be transferred.
2. Group and identify the records to be transferred into records series. A series consists of those records grouped under an item on a records disposition schedule, and (for subject files) created or accumulated or (for case files) closed or terminated in any one year.
3. Without disturbing the existing filing arrangement of the record series, pack the records firmly in the box. To make future references easier, records should not be packed so tightly as to hinder withdrawal. Do not mix records belonging to different records series or with different retention periods in the same box.
4. Face all folders in the same direction in the box. Place them upright in the box. Do not pack file guide cards. Letter-size files are placed facing the end of the box while legal-size files are placed facing the side of the box.
5. Fill each box completely, but leave adequate space for reference purposes..
6. When records will be interfiled after shipment, pack the reserved space in the box with wadded paper. Make note of the box on the SF-135.
7. Wrap oversize and undersize records, such as bound volumes, ledgers, maps and charts, microforms, and fragile items like glass plate negatives

as directed by the FRC which will receive the records.

8. Contact the FRC for instructions to transfer electronic media records such as magnetic tape, tape cartridges, compact disks and the like.

- D. Labeling boxes. Write the accession number, box number and a brief description, as indicated below, on one end of each box with heavy crayon or marker pen. If the box does not have a printed space provided, place the information on the unstitched front (narrow side) of the box. Number boxes in numerical sequence, beginning with box number 1, for each accession. For example: Box 1 of 10. For an example, refer to Figure 8-1 below.

Figure 8-1
Labeling A Records Box



1. The records must face the end of the box showing the accession number.
 2. Make the accession and box number 1 to 2 inches in height.
 3. The FRC may have additional requirements for labeling boxes.
- E. Preparing SF-135, Records Transmittal and Receipt. Prepare an SF-135 for every group of records transferred to an FRC and for historical or otherwise valuable records transferred directly to the National Archives. See Figures 12 and 13. Use SF-135A, Records Transmittal and Receipt (Continuation), as continuation sheets when necessary. Follow the instructions on the reverse of the SF 135 when completing the form. The following are special instructions for completion.
1. Block 2: "Agency Transfer Authorization."
 - a. All Washington Metropolitan Area offices will leave this block blank for completion by the OSHA Records Officer.

b. Field offices will enter the signature and title of the Records Liaison Officer.

2. Block 5: "From". Enter the office and complete mailing address of the OSHA Records Management Officer for offices located in the Washington Metropolitan Area or the address of the transferring field office. The office name and mailing address of the OSHA Records Officer are:

OSHA Records Officer
DOL, OSHA, Office of Management Systems
and Organization
Room N3618 Frances Perkins Bldg.
200 Constitution Ave, N.W.
Washington, D.C. 20210

3. Block 6: "Records Data". This block contains all the information necessary for the FRC to identify, approve, and service the records while they are in FRC storage. Before listing any groups of records, provide the following information in column (f) of the SF-135:

- The office where the records are located including a complete mailing address.
- Provide a records identification statement containing:
 - Agency; program, and office transferring the records.
 - Organizational entity which originally created and/or accumulated the records if different from transferring office.
 - Summary of the types of records, including inclusive dates.
 - Records media code.
- Each series of records (Disposal Schedule Item Number) must be listed in separate accessions on the SF-135. Do not list two separate year's records under the same accession. For a complete explanation of how to complete block 6, refer to the reverse of the SF-135.

F. Supplemental Records Listing for SF-135.

When preparing the SF-135, the transferring office will complete a supplemental

listing of the records being transferred.

1. Washington Metropolitan Area Offices will furnish the original of the Supplemental Records Listing when submitting the SF-135. The listing will be filed with the Agency copy of the SF-135 by the OSHA Records Management Officer.
2. The originating field office will maintain the listing with their copy of the SF-135 (Agency file copy).
3. The Listing is an item by item or folder by folder itemization of each box. All items on the SF-135 are covered by a file system must be cross-referenced into that file system by identifying the file system and by placing the appropriate file codes on the SF-135.

G. Submission of SF-135.

1. Submit the original and two copies of the SF-135:
 - Washington Metropolitan Area offices will submit the SF-135 to the OSHA Records Management Officer. Include a copy of the Supplemental Records Listing.
 - Field offices will submit the SF-135 to the appropriate FRC. If desired, regional offices may screen SF-135's before submission to an FRC. Do not send a copy of the Supplemental Records Listing to the FRC. Inquire if the FRC has any additional requirements for shipping or receiving records.
2. Retain the third copy of the SF-135 as a suspense copy. A confirmation copy will be returned to the originating office by the FRC.

H. Accession Number Assignment.

1. The appropriate FRC will assign accession numbers for each series of records for field offices.
2. The OSHA Records Management Officer will assign accession numbers for offices in the Washington Metropolitan Area.
3. For offices located in Washington, D.C., Maryland, Virginia, and West Virginia, the Philadelphia Regional Office will assign accession numbers. These numbers are available each year for assignment by the Regional

Office. The block of numbers assigned to Region III is:

100-(Fiscal Year)-0300 to 0399

- I. Shipment of Large Accessions. When an accession of 500 cubic feet or more is to be sent to the WNRC or FRC, the director of the WNRC or FRC must receive written notification at least two weeks before the records are actually shipped to allow for allocation of space and manpower.
- J. Other Requirements. The FRC may have additional requirements for shipment of records. Contact your local FRC.

III. Shipment of Records.

- A. WNRC or FRC approval.
 - 1. If the WNRC or FRC approves the transfer, the WNRC or FRC will return the SF-135 indicating approval to transfer the records and may complete block 6(j) indicating the location of the first box in each series of records.
 - 2. The WNRC or FRC will return the SF-135 to the OSHA Records Management Officer or the originating field office, as appropriate, indicating the records may be transferred.
- B. Administratively Controlled Materials. Seal boxes containing administratively controlled information including Privacy Act materials. Escort by OSHA personnel is not necessary during shipment. Use of special postal services such as Registered or Certified Mail is also not necessary.
- C. Classified Materials. Follow those provisions of DLMS 2, Chapter 300, Security Regulations, dealing with transmission of classified materials including information classified as TOP SECRET, SECRET, or CONFIDENTIAL.

IV. Receipt of SF-135 from WNRC or FRC.

- A. National Office. The WNRC will send the accessioned SF-135 to the OSHA Records Officer for Washington Metropolitan Area offices. A copy of the SF-135 will be sent to the transferring office.
- B. Field Offices. The FRC will send the accessioned SF-135 to the transferring field office which will maintain the Agency record copy. The transferring field office will send a copy of the accessioned SF-135 to the Regional Records Officer.

V. Records Reference Service.

A. Services available. The following services are provided for retired records:

1. Find and return one document, an entire box, several boxes, or an entire shipment.
2. Duplicate, under certain circumstances, a document or set of documents.
3. Review and furnish information contained in the records.

B. Liaison. Responsibility for all requests for reference service and return of material should be assigned to one person in the transferring office. In this way, desired control of retired records can be achieved and maintained.

C. Routine requests.

1. WNRC. All Washington Metropolitan Area offices and other offices serviced by the WNRC will contact the WNRC directly for retrieval of desired records. Only the directorate which originally sent the records to the WNRC is authorized to remove records from the FRC.
2. FRC. Field offices will submit requests for transferring records directly to the appropriate FRC. Only the transferring office is authorized to remove records from the FRC.
3. Request Form. Make the request on Optional Form (OF) 11, Reference Request - Federal Records Centers. Complete one OF-11 for each record (document, folder, or box) requested. See Figure 15.
4. Information Needed. Provide the following information:
 - a. Name and location including room number and street address of requesting office.
 - b. Name and telephone number of person requesting records (contact).
 - c. Accession number, FRC location codes, and Agency box numbers shown on the SF-135.
 - d. Description of records including type of record, title or name, and year created or accumulated (see the SF-135), and any other

information deemed useful in locating the records.

- e. Whether it is a permanent or temporary withdrawal. Requests for permanent withdrawal must be in writing. Offices making permanent withdrawal of records from a FRC must send a copy of the OF-11 to the OSHA or the Regional Records Management Officer, as appropriate, for filing with the SF-135.

- D. Urgent or Emergency Requests. The National Office directorate or field office which transferred the records will submit urgent or emergency requests directly to the WNRC or FRC by telephone. Provide the same information required for routine requests.
- E. Returning Records. Offices will return records directly to the WNRC or FRC. Enclose a copy of the OF 11 with the records.

VI. Disposition of Records in FRC's.

- A. Disposition Procedures. Transferring records to a records center is not a substitute for disposing of them in the office. Records that have served their function, are no longer needed for administrative, fiscal, or legal purposes and have reached the end of their disposition periods should be destroyed.
 - 1. Notice to Agency. When records retired to a records center are eligible for destruction, the OSHA office shown in Block 5 of the SF-135 is sent a NA Form 1301, Notice of Intent to Dispose of Records, NA Form 1300, Agency Review for Contingent Disposal, or other equivalent form at least 90 days before the scheduled destruction date.
 - 2. Agency Approval to Dispose of Records Located in FRC's.
 - a. Only the OSHA or Regional Records Management Officer may approve destruction or further retention of records.
 - b. When an office receives a NA-1300, NA-1301 or equivalent, forward the form to the OSHA or Regional Records Management Officer, as appropriate.
- B. Agency Notification to FRC. The OSHA or Regional Records Management Officer will notify the records center when the retention period will be extended. No notification is necessary if destruction is approved with the NA 1301 or

equivalent since the records center will automatically destroy the records after 90 days have elapsed since the NA 1301 or equivalent was sent to the Agency.

- C. Office Address Changes. The Agency must be sure that records are not inadvertently destroyed due to office relocation or closing and that the NARA disposition notice is received. When an OSHA field office closes or relocates, the Regional Records Management Officer will notify the FRC and provide a new contact address and a list of the affected accessions.

Figure 8-2

FRC ADDRESSES

FRC Address	Phone, Fax and E-mail	Area Served and Comments
Washington National Records Center 4205 Suitland Road Suitland, MD 20746-8001	Phone: 301-457-7000 E-mail: center@suitland.nara.gov Fax: 301-457-7117	Headquarters offices: District of Columbia, Maryland, and Virginia. Federal field operations in Maryland, Virginia, and West Virginia.
Anchorage FRC NARA, Pacific Alaska Region 654 West Third Avenue Anchorage, AK 99501-2145	Telephone: 907-271-2443 E-mail: archives@alaska.nara.gov Fax: 907-271-2442	Some agencies in Alaska.
Atlanta FRC NARA, Southeast Region 1557 St. Joseph Avenue East Point, GA 30344-2593	Telephone: 404-763-7477 E-mail: archives@atlanta.nara.gov Fax: 404-763-7033	Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee
Bayonne FRC NARA's Northeast Region Building 22 Military Ocean Terminal Bayonne, NJ 07002-5388	Telephone: 201-823-7241 E-mail: center@bayonne.nara.gov Fax: 201-823-5432	New Jersey, New York, Puerto Rico, and U.S. Virgin Islands. This FRC's nonclassified holdings are moving to Lee's Summit FRC. The Bayonne FRC will close by April 1999.
Boston FRC NARA, Northeast Region 380 Trapelo Road Waltham, MA 02154-6399	Telephone: 781-647-8100 E-mail: archives@waltham.nara.gov Fax: 781-647-8460	Maine, New Hampshire, Vermont, Massachusetts, Connecticut, and Rhode Island.
Chicago FRC NARA, Great Lakes Region 7358 South Pulaski Road Chicago, IL 60629-5898	Telephone: 773-581-7816 E-mail: archives@chicago.nara.gov Fax: 312-353-1294	Illinois, Minnesota, and Wisconsin.
Dayton Federal Records Center NARA, Great Lakes Region 3150 Springboro Road Dayton, OH 45439-1883	Telephone: 937-225-2852 E-mail: center@dayton.nara.gov Fax: 937-225-7236	Ohio, Indiana, and Michigan
Denver FRC NARA, Rocky Mountain Region Building 48, Denver Fed. Center Denver, CO 80225 P. O. Box 25307 Denver, CO 80225-0307	Telephone: 303-236-0804 E-mail: center@denver.nara.gov Fax: 303-236-9297	Colorado, Montana, New Mexico, North Dakota, South Dakota, Utah, and Wyoming.
Fort Worth FRC NARA, Southwest Region 501 West Felix Street, Building 1 Fort Worth, TX 76115-3405 P. O. Box 6216 Fort Worth, TX 76115-0216	Telephone: 817-334-5525 E-mail: archives@ftworth.nara.gov Fax: 817-334-5621	Arkansas, Louisiana, Oklahoma, and Texas

Figure 8-2

FRC ADDRESSES (Continued)

FRC Address	Phone, Fax and E-mail	Area Served and Comments
Kansas City FRC NARA, Central Plains Region 2312 East Bannister Road Kansas City, MO 64131-3011	Telephone: 816-926-6272 E-mail: archives@kansascity.nara.gov Fax: 816-926-6982	Iowa, Kansas, Missouri, and Nebraska
Lee's Summit FRC NARA, Central Plains Region 200 Space Center Drive Lee's Summit, MO 64064	Telephone: 816-478-7089 E-mail: sean.murphy@kccave.nara.gov Fax: 816-478-7625	New Jersey, New York, Puerto Rico, and the U.S. Virgin Islands. Nonclassified holdings formerly held by Bayonne FRC.
Laguna Niguel FRC NARA, Pacific Region 24000 Avila Road, First Floor-East Entrance Laguna Niguel, CA 92677-3497 P. O. Box 6719 Laguna Niguel, CA 92607-6719	Telephone: 714-360-2641 E-mail: center@laguna.nara.gov Fax: 714-360-2624	Arizona, southern California, and Clark County, Nevada
New York City FRC NARA, Northeast Region 201 Varick Street New York, NY 10014-4811	Telephone: 212-337-1300 E-mail: archives@newyork.nara.gov Fax: 212-337-1306	New Jersey, New York, Puerto Rico, and the U.S. Virgin Islands
Philadelphia (Center City) FRC NARA, Mid Atlantic Region Ninth and Market Streets Philadelphia, PA 19107-4292	Telephone: 215-597-3000 E-mail: archives@philarch.nara.gov Fax: 215-597-2303	Delaware, Maryland, Pennsylvania, Virginia, and West Virginia.
Philadelphia (Northeast Philadelphia) FRC NARA, Mid Atlantic Region 14700 Townsend Road Philadelphia, PA 19154-1096	Telephone: 215-671-9027 E-mail: center@philadelphia.nara.gov Fax: 215-671-8001	Delaware and Pennsylvania
Pittsfield FRC NARA, Northeast Region 10 Conte Drive Pittsfield, MA 01201-8230	Telephone: 413-445-6885 E-mail: archives@pittsfield.nara.gov Fax: 413-445-7599	Certain Federal agencies located throughout the United States
San Francisco FRC NARA, Pacific Region 1000 Commodore Drive San Bruno, CA 94066-2350	Telephone: 650-876-9009 E-mail: center@sanbruno.nara.gov Fax: 650-876-9233	Northern California and Nevada (except Clark County), and for selected Federal agencies in Hawaii and the Pacific Ocean area.
Seattle FRC NARA, Pacific Alaska Region 6125 Sand Point Way NE Seattle, WA 98115-7999	Telephone: 206-526-6507 E-mail: archives@seattle.nara.gov Fax: 206-526-4344	Idaho, Oregon, and Washington and selected Federal agencies in Alaska, Hawaii, and the Pacific Ocean area.

Chapter IX

SECURITY OF CLASSIFIED MATERIAL AND ADMINISTRATIVELY CONTROLLED INFORMATION

I. Introduction

This chapter supplements Department of Labor Manual System (DLMS) Volume 2, Chapter 300, Security Regulations, which governs the classification, declassification, and safeguarding of classified records in the Department. This chapter also provides guidelines covering the security of administratively controlled information including Privacy Act information.

II. Categories of Classified Information.

Official information which requires protection in the interest of national security is limited to three (3) categories of classification. These classifications, in descending order of importance, consist of TOP SECRET, SECRET, AND CONFIDENTIAL. No other marking may be used to classify national security information, including military information, except as provided by statute.

III. Administratively Controlled Information.

Administratively Controlled Information is information which must not be released for public dissemination. This includes FOIA-exempt information, Privacy Act restricted information, and other information to which access is restricted such as individual medical records, trade secrets and other private or restricted company information.

IV. Restrictions on Access to Classified Information.

- A. The possession or knowledge of classified information shall be confined to persons whose specific official duties require such information and who have security clearance to the level of the material. People are not authorized to gain knowledge of classified information by virtue of their grade or position alone.
- B. An employee NOT having security clearance must not accept, receipt for, read, or knowingly discuss classified information.

V. Standards of Access.

Administratively Controlled Information and Classified Information must be protected so

unauthorized persons do not gain access to the information. Hard copy materials should be maintained in locking file equipment or safes, as appropriate. Electronic information must limit access through password, encryption or other appropriate means to deny access to unauthorized persons. The materials should not be left unattended. Depending on the sensitivity of the information, a log of access and file access or checkout procedures may be needed to safeguard the information.

Authorized access must be limited to those with a need to know the contents of the information

VI. Other Security Information.

Contact the OSHA Security Officer, Office of Administrative Services, for additional information on security concerns involving classified or administratively controlled information.

Chapter X

RECORDS MANAGEMENT REPORTS

I. Required Reports.

The Office of Management Systems and Organization requires information to determine the effectiveness of the OSHA Records Management Program. Two reports are necessary to gather this information:

- A. Bi-Annual Records Management Report.
- B. Records Management Review Reports.

II. Bi-Annual Records Management Report.

Regional and Program Records Management Officers must prepare a biannual report of the records management activities occurring in the organization. The report covers the period October 1 through September 30 of each even numbered year.

A. Matters to be Reported.

1. Number of records management reviews conducted including organizations reviewed and locations. Include copies of review reports if not previously furnished (Includes records management portions of more complete administrative reviews).
2. Copy of the Records Management Checklist for every organizational component. (Refer to Appendix F.)
3. Records management training provided employees.
4. Significant problems encountered in the area of records management practices and operations, but not included in review reports, and solutions implemented.
5. Suggested changes to the Records Management Manual, file systems, disposition schedules, and the like.
6. Updated lists of Records Management Liaison Officers.
7. Other items of interest.

- B. Format. Prepare a narrative report in memorandum form and style.
- C. Submission. Program and Regional Records Management Officers will submit the report to reach the OSHA Records Officer by October 31 of each even numbered year.

III. Records Management Review Reports

Records management reviews are conducted to assist offices in performing their functions more effectively through use of common sense records management practices.

- A. Responsibilities. It is the responsibility of the reviewer to provide guidance on:
 - 1. Files practices or operations in all media.
 - 2. Implementation and operation of records systems including file systems and records disposition schedules.
 - 3. Transfer of records to Federal records centers and other records transfers.
 - 4. Other records management areas.
- B. Program Evaluation. Reviews are useful to help evaluate the OSHA Records Management Program. Reviews point out areas which may not be fully understood by OSHA employees, and indicate unclear or conflicting directives or instructions, or may indicate the program is not being implemented. The reviews and their findings, recommendations, and other information point out new directions for the program and indicate where changes need to be made to improve the program.
- C. Areas to be Reviewed. The review should cover, at a minimum, the areas of records control and reduction, file classification, recordkeeping and use, records classification practices, use of finding aids, filing practices, disposition practices, reference services, workload, file documentation, filing equipment and supplies, space and workflow, and training.
- D. Records Management Checklist. The Checklist contains questions concerning all the areas listed in paragraph 3 above. Additional questions may be asked and additional areas may be explored at the option of the reviewing official. The Checklist provides the basis for writing a review report. See Appendix F, Records Management Checklist.

- E. Report Format. Records review reports will include the following information:
1. Date of report.
 2. Name, title, organization, and address of reviewing official.
 3. Field or National Office offices reviewed including addresses.
 4. Inclusive dates of each review.
 5. Principal contact in each office or organizational component reviewed.
 6. Volume of records on hand in the office before and after the review.
(Cubic feet for paper or hard copy records, linear feet for audio and video tape, linear feet for computer tape, and kilobytes or megabytes for other electronic records.)
 7. Total volume of records destroyed during review.
 8. Total volume of records transferred to FRC's during review.
 9. Numbers and types of filing equipment on hand.
 10. Information on records management practices in offices reviewed.
 11. Findings. Refer to Records Management Review Checklist.
 12. Recommendations. Refer to Records Management Review Checklist.
 13. Summary and closeout conference.
 14. Follow up action including progress reports required, if any.
- F. Distribution. Provide copies of the report to:
1. OSHA Records Officer.
 2. Office reviewed.
 3. Directorate Director for the office if the office is located in the National Office.
 4. Regional Records Officer for field offices reviewed.

Appendix A

E-MAIL RECORDS AND NONRECORDS

I. Introduction

- A. This appendix covers the creation, maintenance, use, and disposition of e-mail records and nonrecords. A summary of the policy is included below as a reference aid.
- B. Office automation has changed how records are created, used, and stored. Electronic mail messages and attachments, like any other document in an agency's possession, may be official records.
- C. Technology requires senders and receivers of e-mail messages to make recordkeeping decisions regarding the record or nonrecord status. The decision to retain and place paper documents in the file has always rested with the creator or recipient of the document. The advent of e-mail merely requires the e-mail creator or receiver to make an immediate decision regarding the record status of an electronic document.

II. Record Copy Media. OSHA offices will maintain the record copy of e-mail records in paper form or in another media but not in electronic form. E-mail systems are not electronic recordkeeping systems and neither the Department nor OSHA has electronic recordkeeping systems for LAN's in place; therefore, e-mail records will not be maintained in electronic media.

III. Determining Record Status.

- A. Records: The sender and each recipient will determine if a particular e-mail message is an official record. Use the guidelines listed in paragraph XII below to determine if an e-mail message is an official record. Examples of record e-mail messages are located in paragraph XIII. See Appendix B for a definition.
- B. Nonrecord Material: All documentary material, e-mail messages and enclosures, that do not meet the definition of an official record are nonrecords. Examples of nonrecord e-mail messages are located in paragraph XIII. See Appendix B for a definition.

- IV. Maintenance of Official Record E-Mail Messages. The e-mail message must be printed out by the user and maintained in the file with other similar records. Optionally, the user may maintain the record copy in another media such as microfilm or CD-ROM.
- V. E-Mail Official Record Contents. The sender of an e-mail message that is determined to be an official record must preserve the following information in the files:
- The e-mail message.
 - Any attachments.
 - A list of recipients if they are not individually listed on the message. Includes any groups.
 - Return receipt notifications if determined by the sender to be needed for documentation.
- VI. Disposition of E-Mail Records.
- A. E-mail messages that are official records will be destroyed or transferred to a Federal Records Center in accordance with an approved Agency Records Schedule or the General Records Schedules, as appropriate.
 - B. Agency records schedules cover records specific to that agency (i.e., inspection case files, standards development files).
 - C. The GRS cover records common to most Federal agencies (i.e., retirement registers, time and attendance sheets). Absence of a records schedule covering the e-mail message does NOT mean the message is nonrecord.
- VII. Disposition of Nonrecord E-Mail. E-mail messages that are nonrecords should be promptly deleted by the user when no longer needed. This improves system efficiency by releasing valuable disk space for other messages.
- VIII. Privacy Expectations of E-Mail Messages. OSHA e-mail messages, either official record or nonrecord, are produced or received using Federally-owned property and, as such, are the property of the agency, not the individual employee. Employees should have no expectation of privacy in their e-mail messages.
- IX. Backup and Disclosure. Each e-mail system has a security backup procedure where a "snap-shot" is taken of the data on the system, usually after business hours. Backups permit the retrieval and re-creation of messages in the event of a system failure. Information found on backup tapes is subject to subpoena, discovery proceedings, and

requests filed under the Freedom of Information Act (FOIA) and Privacy Act. Messages in an e-mail system are public documents subject to disclosure.

X. Security. Users should recognize that the e-mail system used by them or their recipient may not afford proper protection for sensitive, classified, or other restricted information. Users should consult with the appropriate systems administrators to determine what steps (passwords, encryption, etc.), if any, can be taken to ensure information security before using e-mail for this type of message.

XI. Recording Members of an E-Mail Distribution List. The members of a distribution list that does not appear on an e-mail record must be included with the record.

- If the e-mail system allows viewing and/or printing of the members of a list, like the OSHANET or the Department's Employee Computer Network (ECN), print and attach the members list to the message.
- If the system does not allow printing the list, the LAN administrator or other designated employee is responsible for maintaining current e-mail distribution lists and making them available to all e-mail users at the National Office organization or field location for the system. Users will obtain lists from the LAN administrator or other designated employee and attach the appropriate listing to the e-mail record.
- Non-record e-mail materials may be destroyed at the user's discretion.

XII. Records Determination.

A. Definition. According to 44 U.S.C. 3301, the term 'records', "includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them."

B. Determining Official Records. Use the guidelines below in determining if an e-mail message is an official record. Examples of records and nonrecords are located in paragraph XIII.

1. Official records provide documentation on agency policies, procedures, actions, processes and decisions and document the "who, what, where, and why" of the policy, procedure, action, etc.

2. If the message does not document policy, procedure, action, processes or decisions or is not the best or only documentation, then it is not a record but is a nonrecord.
- C. Further Guidelines Step 1. If the sender or receiver still cannot determine records status, consider the following further guidelines. If the answer to 1. is "yes" and either 2. or 3. is "yes," the message is an official record which must be safeguarded as evidence of the agency's mission and functions just as any other record in paper or electronic form.
1. Does the message tell what agency policies, procedures, actions, processes and/or decisions have been made, are being considered or will be considered for adoption or implementation in the future?
 2. Does the message provide information which is not available in another copy or form in your office?
 3. Does the message provide the best documentation of the policy, procedure, etc. in your office?
- D. Further Guidelines Step 2. If the user is not sure of records status after considering paragraphs B. and C. above, apply the following additional guidelines.
1. If the message should be filed in accordance with the OSHA Classification System (OSHA Instruction ADM 12-0.1), or would normally be filed in a case file, subject file, or chronological file, it is probably an official record.
 2. If the message can be destroyed, retired, or transferred in accordance with an approved Agency records schedule or the National Archives-issued General Records Schedules, it is an official record.
 3. If the information is necessary to protect the financial, legal, and other rights of the Government and persons affected by Government actions, the message is a record.

Figure A-1

OSHA E-Mail Policy Summary

- A. E-mail messages are public documents subject to disclosure unless specifically exempt.
- B. E-mail messages are the property of the agency, not the individual. Do not have an expectation of privacy in your e-mail messages.
- C. E-mail systems are usually not secure. Contact your system administrator to determine how to protect sensitive or restricted access information.
- D. Determine if an e-mail is record or nonrecord.
- E. Records must be safeguarded and maintained in a record-keeping system (Printed on paper and placed in the official files).
- F. E-mail records must preserve several elements in the file:
 - 1. The e-mail message.
 - 2. Attachments.
 - 3. Recipient list for recipients listed on message as groups, not individuals.
 - 4. Return receipt notifications, if needed.

XIII. E-mail Record and Nonrecord Examples. Following are some examples of records and nonrecords. These examples are based on general ideas of records vs. nonrecords. They are not limited only to electronic communications but apply to documentary materials in all media.

- A. Records.
 - 1. Documentary material discussing proposed policy.
 - 2. Documentary material announcing the date a report is due.

3. Documentary material requesting comments on a draft policy.
4. Copy of requisition requesting services or supplies attached to an e-mail.
5. Responses with substantive changes from other offices to a draft.
6. Documentary materials containing information not maintained elsewhere in the office and relating to office functions.
7. Originating office copies of documentary materials circulated for approval, comments or action. Also includes materials received by the office and circulated for approval, comments or action.
8. Responses to a draft containing substantive changes from other offices.
9. Office responses to a draft from another office and containing substantive changes.
10. Copy of a memo received from another office related to this office's functions.
11. Original of a publication prepared by your office.
12. Downloaded Internet information documenting your office's functions.
13. Documentary material publicizing a health fair, equipment show, or other official activity when sponsored by the office.
14. Suggestive e-mail sent from within the office which might be cause for a grievance, suit, etc.

B. Nonrecords.

1. Work-related materials that do not contain unique information or were not circulated for approval, comment, or action such as meeting reminders, telephone messages and the like.
2. Copies of documents (information copies) that are maintained solely for convenience of reference.
3. Copy of a requisition received from another office for information.
4. Copy of a memo received from another office not related to this office's

functions.

5. Documentary material for information noting that a draft is being circulated for comment but not asking you to respond.
6. Documentary material announcing a health fair.
7. Documentary material relating to a person's personal business.
8. Copy of a publication, not original artwork.
9. Downloaded Internet files not documenting your office's work.
10. Suggestive e-mail received from outside the organization.
11. Copy of a requisition received from another office for information.
12. Copy of a memo received from another office not related to this office's functions.
13. Copies of general announcements or bulletins (blood drive, holiday party, town hall meeting, etc.).
14. Messages of a non-work related nature (car pool arrangements, lunch plans, etc.).

Appendix B

RECORDS MANAGEMENT GLOSSARY OF TERMS

This glossary was prepared to provide agency personnel a common understanding and meeting ground for records management concepts and practices. Section I provides definitions of terms. Section II lists selected abbreviations and acronyms, along with their meanings.

- I. **Definitions.** These definitions provide information and explanations for many common-use terms in records and information management. While this listing is not meant to be all-encompassing, it should provide sufficient information for continuity and commonality of thought for fruitful information exchange and discussion.

ACCESSION. (1) A group of records related to one or several functions disposable under one item of a disposal schedule and usually created or accumulated during the same year. (2) Transfer of historical or other "permanent" retention records to NARA or of temporary retention records to a Federal records center. *See also* **BLOCK (1)**, **PERMANENT RECORDS**, **RETIREMENT**, **TRANSFER**.

ACCESSION NUMBER. A number assigned to identify shipments of records sent to the Federal Records Centers or to NARA.

ACTIVE RECORDS. *See* **CURRENT RECORDS**.

ADEQUACY OF DOCUMENTATION. The standard of sufficiently and properly recording actions and/or decisions so that the record of the conduct of Government business is complete and accurate to the extent required to document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and that is designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. *See also* **DOCUMENTATION (1)**, **RECORDKEEPING REQUIREMENTS(1)**, **RECORDS CREATION**.

ADMINISTRATIVE RECORDS. Records, regardless of medium, relating to budget, personnel, supply, and similar housekeeping, or facilitative, functions common to most agencies, in contrast to program records. *See also* **PROGRAM RECORDS**.

ADMINISTRATIVELY CONTROLLED INFORMATION. Privacy Act, FOIA exempt, privileged, trade or business secrets or other non-security-classified information sometimes bearing designations, such as "Administratively Controlled Information", "For Official Use Only," "Restricted Private Company Information," and the like, to prevent its unauthorized disclosure. *See also* **CLASSIFIED INFORMATION**, **DISCLOSURE-FREE EXTRACT**.

APPRAISAL. The process of determining the value and thus the disposition of records based upon their administrative, fiscal, legal, evidential, informational, and research value. Includes their arrangement and relationship to other records..

ARCHIVES. The noncurrent records of an organization preserved because of their continuing, or enduring, value.. *See also* **PERMANENT RECORDS**.

ARCHIVING. Creating a backup copy of computer files, especially for long-term storage.

AUDIOVISUAL RECORDS. Records in pictorial or aural form, regardless of format. Includes still photographs (or still pictures), graphic arts (posters and original art), motion pictures, video recordings, audio (or sound) recordings, and related records. *See also PHOTOGRAPHIC RECORDS.*

AUTOMATED DATA PROCESSING (ADP). Systematically performing a series of actions with data by using automatic machines, primarily electronic digital computers. Also, called automatic data processing. Often used as a synonym for electronic data processing (EDP). *See also DATA PROCESSING, ELECTRONIC RECORDS.*

AUTOMATED INFORMATION SYSTEM. An information system that usually involves the use of a computer. Often used as a synonym for an electronic records system. *See also ELECTRONIC RECORDS SYSTEM.*

BLOCK. (1) One or more chronological segment of cutoff, or closed, records that are in the same series and are dealt with as a unit for disposition purposes. *See also ACCESSION, CUTOFF, PERMANENT RECORDS, TRANSFER.* (2) In electronic recordkeeping, a grouping of data stored as a unit on an external storage medium and dealt with as a unit by the computer for input or output.

CASE FILES. The grouping together of records, regardless of media, which document a specific action, event, person, company, place, project, organization, or other matter. The contents of case files are restricted to records dealing only with the specific item for which the file was established, from its inception to its close.

CASE WORKING FILES. Background or support files, such as worksheets, questionnaires, rough notes, calculations, or drafts, used to prepare or analyze case file documents. Often bulky when in paper form. *See also WORKING FILES.*

CENTRAL FILES. Files accumulated by several offices or organizational units and maintained and supervised in one location. They are most effective in small organizations. Also called centralized files. *See also DECENTRALIZED FILES.*

CHRONOLOGICAL (CHRON.) FILES. *See READING FILES.*

CLASSIFICATION. (1) the process of determining the sequence or order in which to arrange documents, assigning a file category in a manual or automated filing system and identifying documents with that category. *See also FILING SYSTEM.* (2) The process or result of identifying records containing national security information. *See also CLASSIFIED INFORMATION, DECLASSIFICATION.* (3) The designation of documents which should not routinely be made available to people outside the agency and includes Privacy Act and FOIA Exempt materials. Also known as Administratively Controlled Information. *See also ADMINISTRATIVELY CONTROLLED INFORMATION, DISCLOSURE-FREE EXTRACT.*

CLASSIFIED INFORMATION. Records or information requiring, for national security reasons, safeguards against unauthorized disclosure and have been classified as **CONFIDENTIAL**, **SECRET** or **TOP SECRET**. *See also ADMINISTRATIVELY CONTROLLED INFORMATION, DECLASSIFICATION.*

CODING. (1) The process of putting abbreviated file designations on documents. *See also FILE CODES.* (2) Converting data to a form that a computer can process.

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).

COMPUTER-ASSISTED LOCATOR (CAL) SYSTEM. A computer system that keeps track of documents as

they circulate through an agency.

COMPUTER OUTPUT MICROFILM (COM). Microfilm containing data converted and recorded directly from a computer. Generally used in place of hard copy printouts. *See also MICROIMAGING SYSTEMS.*

COMPUTER PRINTOUT. *See PRINTOUT.*

CONVENIENCE FILES. Nonrecord copies of correspondence, completed forms, and other documents kept solely for ease of access and reference. *See also READING FILES, TECHNICAL REFERENCE FILES, WORKING FILES.*

COPY. (1) A reproduction of the contents of an original document, prepared simultaneously or separately and usually identified by function or by method of creation. (2) In electronic recordkeeping, the action or result of reading data from a source, leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source.

CORRESPONDENCE. Letters, postcards, memorandums, notes, telecommunications, E-mail and any other form of addressed communication that are sent and received. *See also GENERAL CORRESPONDENCE FILES.*

CREATION. *See RECORDS CREATION.*

CURRENT RECORDS. Records necessary to conduct the current business of an office and therefore generally maintained in office space and equipment. *See also NONCURRENT RECORDS, SEMICURRENT RECORDS.*

CUSTODY. Guardianship, or control, of records, including both physical possession (physical custody) and legal responsibility (legal custody), unless only one is specified. It may include legal title or ownership of the records except where an agency is only providing storage space for the records, such as in a Federal records center.

CUTOFF. Breaking, or ending, files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal or transfer in complete blocks and, for correspondence files, to permit the establishment of new files. Cutoff is also called file cutoff or file break. *See also BLOCK (1).*

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. *See also INFORMATION, MACRODATA, MICRODATA.*

DATA BASE. In electronic recordkeeping, a set of data, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users at the same time for various applications.

DATA BASE MANAGEMENT SYSTEM (DBMS). A software system used to access and retrieve data stored in a data base.

DATA FIELD. A specific area of an electronic record allocated for a particular category of data, usually one data element, such as a name. *See also LOGICAL RECORD, RECORD LAYOUT.*

DATA FILE. An organized collection of related data, usually arranged into logical records that are stored together and treated as a unit by a computer. Used in contrast to text documents that may be recorded on electronic media.

DATA PROCESSING (DP). Systematically performing a series of actions with data. May be done by manual, mechanical, electromechanical, or electronic (primarily computer) means. Often used interchangeably with automated data processing (ADP). *See also AUTOMATED DATA PROCESSING (ADP).*

DAY FILES. *See READING FILES.*

DECENTRALIZED FILES. A type of file plan under which each element of an organization maintains its files at the point of reference. *See also FILE PLAN.*

DECLASSIFICATION. The process or result of determining that information no longer requires classification for national security reasons. *See also CLASSIFICATION (3), CLASSIFIED INFORMATION.*

DELETING. The process of permanently removing, erasing, or obliterating recorded information from a medium, especially a magnetic tape or disk, which then may be reused. In electronic recordkeeping, sometimes called scratching or erasing. *See also DESTRUCTION.*

DESTRUCTION. The major type of disposal action. Methods of destroying records include burning, pulping and selling, or salvaging the record medium. *See also DELETING, DISPOSAL, DISPOSITION.*

DETAIL FILES. *See TRANSACTION FILES (2).*

DIGITAL AUDIO TAPE (DAT). *See AUDIOVISUAL RECORDS, ELECTRONIC RECORDS.*

DIRECT ACCESS. The process of retrieving data from memory or a storage device by going directly to a particular location, usually as specified by an address, without reading any other data. Also called random access. Used in contrast to sequential, or serial, access. *See also SEQUENTIAL ACCESS.*

DIRECTIVE. An organized system of documents communicating policy and procedure.

DISCLOSURE-FREE EXTRACT. A copy of a record that excludes all exempted information; that is, information deleted or otherwise concealed under provisions of the Freedom of Information Act (FOIA) or the Privacy Act. Also called a public use file. *See also ADMINISTRATIVELY CONTROLLED INFORMATION.*

DISPOSABLE RECORDS. *See TEMPORARY RECORDS.*

DISPOSAL. The destruction or occasionally donation to an eligible person or organization of temporary records after their retention periods expire. *See also DESTRUCTION, DISPOSE, DISPOSITION, FINAL DISPOSITION, TEMPORARY RECORDS.*

DISPOSE. To destroy temporary records. *See also DISPOSAL, FINAL DISPOSITION.*

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. *See also DISPOSAL, DISPOSITION PERIOD, FINAL DISPOSITION, LIFE CYCLE OF RECORDS, RETIREMENT, SCHEDULED RECORDS, SCHEDULING, TRANSFER, UNSCHEDULED RECORDS.*

DISPOSITION AUTHORITY. Legal approval empowering an agency to transfer permanent records to NARA or carry out the disposal of temporary records or the agency's approval of disposition instructions for nonrecord materials.

DISPOSITION PERIOD. The length of time that records are maintained by an agency before a final disposition action. *See also DISPOSITION.*

DOCUMENT. Recorded information regardless of physical form or characteristics. Often used interchangeably

with record. *See also NONRECORD MATERIALS, RECORDS.*

DOCUMENTARY MATERIALS. A collective term for records and nonrecord materials that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording. *See also FILES, MEDIUM, NONRECORD MATERIALS, RECORDED INFORMATION, RECORDS.*

DOCUMENTATION. (1) The act or process of substantiating by recording actions and/or decisions. *See also ADEQUACY OF DOCUMENTATION.* (2) *See DOCUMENT.* (3) Records, generally in paper form, required to plan, develop, operate, maintain, and use electronic records and software including system specifications, file specifications, codebooks, record layouts, user guides, and output specifications. *See also MASTER FILES, PROCESSING FILES.*

DOCUMENTATION REQUIREMENTS AND STANDARDS. *See RECORDKEEPING REQUIREMENTS.*

ELECTRONIC DATA PROCESSING (EDP). *See AUTOMATED DATA PROCESSING (ADP).*

ELECTRONIC MAIL. The process or result of sending and receiving messages via telecommunications links between computer terminals. Also called E-Mail.

ELECTRONIC RECORDKEEPING. The creation, maintenance and use, and disposition of records created and stored using a computer. *See also RECORDKEEPING, RECORDKEEPING REQUIREMENTS.*

ELECTRONIC RECORDS. Records stored in a form that only a computer can process. Also called machine-readable records or ADP records. *See also AUTOMATED DATA PROCESSING (ADP), OPTICAL DISK, RECORDS.*

ELECTRONIC RECORDS SYSTEM. Any electronic information system that produces, processes, and/or stores records by grouping them in a logical and orderly manner thereby facilitating use and disposition. Often called an automated information system. *See also AUTOMATED INFORMATION SYSTEM.*

EMERGENCY-OPERATING RECORDS. That type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. *See also VITAL RECORDS.*

ERASING. *See DELETING.*

ESSENTIAL RECORDS. *See VITAL RECORDS.*

FACILITATIVE RECORDS. *See ADMINISTRATIVE RECORDS.*

FACSIMILE or FAX. A method or device for transmitting an exact copy of a document, drawing, photograph, etc. via telephone or radio for reproduction elsewhere.

FEDERAL RECORDS. *See RECORDS.*

FEDERAL RECORDS CENTER (FRC). Records centers located regionally and serve as the repositories for semiactive permanent or temporary Federal records.

FICHE. *See MICROFICHE.*

FILE. (1) An accumulation of records or nonrecord materials arranged according to a plan. (2) A unit, such as a folder, microform, or electronic medium, containing such records or nonrecord materials. (3) Storage equipment,

such as a filing cabinet. (4) *See DATA FILE. See also FILING, RECORD UNIT.*

FILE CODES. Numbers or symbols used to abbreviate lengthy file titles. *See also CODING (1).*

FILE COPY. *See COPY (1), RECORD COPY, RECORDS.*

FILE CUTOFF. *See CUTOFF.*

FILE LAYOUT. The arrangement and structure of data in a file, including the sequence and size of its components. *See also RECORD LAYOUT.*

FILE PLAN. A plan designating the physical location(s) where files are to be maintained. The plan may also include the specific types of files to be maintained, and the organizational element(s) having custodial responsibility. *See also FILING SYSTEM.*

FILE STATION. A location at which records are maintained for current use in an organization. It may be centralized or decentralized. *See also FILES, FILES CUSTODIAN, NONRECORD MATERIALS, RECORDS.*

FILE SERIES. *See SERIES.*

FILE STRUCTURE. The format of fields within a data record.

FILE TYPES. Categories or classes of files. Include case, case working, general correspondence, chronological or reading, transitory correspondence, convenience, and technical reference files, along with vital records and special records. Each of these types is defined in this glossary.

FILE UNIT. *See RECORD UNIT.*

FILES. (1) A collective term usually applied to all records and nonrecord materials of an office or agency. *See also DOCUMENTARY MATERIALS, MASTER FILES, NONRECORD MATERIALS, RECORDED INFORMATION, RECORDS.* (2) In electronic records, a collective term for data files. *See also DATA FILE, MASTER FILES.*

FILES CUSTODIAN. The individual in charge of files at a file station in an office or storage area. Often used interchangeably with records custodian.

FILES INVENTORY. *See INVENTORY.*

FILES MANAGEMENT. Applying records management principles and techniques to filing practices in order to organize and maintain records properly, retrieve them rapidly, ensure their completeness, and make their disposition easier. *See also RECORDS MANAGEMENT.*

FILES OPERATIONS. *See FILES MANAGEMENT.*

FILING. Putting documents into their place in accordance with a plan, or filing system. *See also FILE, RECORDS MAINTENANCE AND USE.*

FILING FEATURE. A characteristic by which a document is filed and found, such as a number, date, title, name, or subject.

FILING SYSTEM. A set of policies and procedures for organizing and identifying files or documents to speed their retrieval, use, and disposition. Sometimes called recordkeeping system.

FINAL DISPOSITION. The end of the records life cycle in which temporary records are disposed of and permanent records are transferred to the National Archives. *See also DISPOSAL, DISPOSE, LIFE CYCLE OF RECORDS, PERMANENT RECORDS, SCHEDULED RECORDS, TEMPORARY RECORDS, UNSCHEDULED RECORDS.*

FINDING AIDS. Indexes or other lists, whether manual or automated, that are designed to make it easier to locate relevant files or retrieve information. *See also INDEX.*

FOLLOW UP FILES. *See SUSPENSE FILES.*

FOR OFFICIAL USE ONLY. *See ADMINISTRATIVELY CONTROLLED INFORMATION.*

FORM. (1) *See MEDIUM.* (2) A document with a fixed arrangement of captioned spaces designed for entering and extracting prescribed information. Categories of forms include internal, interagency, public use, standard, and optional. (3) Input screens used to enter data or information on a computer, usually into a database.

FORMAT. (1) The shape, size, style, and general makeup of a particular record. (2) The arrangement of data for computer input or output, such as the number and size of data fields in a logical record or the spacing and letter size used in a document. *See also FILE LAYOUT and RECORD LAYOUT.*

FROZEN RECORDS. In records disposition, those temporary records that cannot be destroyed on schedule because special circumstances, such as a court order, an investigation, or reappraisal of disposition, require a temporary extension of the approved retention period.

GENERAL CORRESPONDENCE FILES. Records arranged and filed according to their general informational, or subject, content. Mainly letters and memorandums but also forms, reports, and other material, all relating to program and administrative functions, not to specific items or transactions.

GENERAL RECORDS SCHEDULE (GRS). NARA-developed and issued records disposition schedules governing the disposition of specified administrative or housekeeping records common to several or all agencies.

GRAPHIC RECORDS. *See AUDIOVISUAL RECORDS.*

GSA. General Services Administration.

HARD COPY. (1) Recorded information on paper or some other durable surface. May be copied from a computer, microfilm or other medium where the information cannot be directly viewed.

HIERARCHICAL SYSTEM. Any classification system in which records are arranged under primary (first-level) categories and then, as necessary, under secondary (second-level) and further subdivisions.

HISTORY FILES. Electronic files copied from inactive master files for long-term or permanent retention. *See also MASTER FILES, PERMANENT RECORDS, TRANSFER.*

HOUSEKEEPING RECORDS. *See ADMINISTRATIVE RECORDS.*

INACTIVE RECORDS. *See NONCURRENT RECORDS, SEMICURRENT RECORDS.*

INDEX. An arrangement of subjects arranged differently from the related record series to make it easier to locate relevant documents. *See also FINDING AIDS.*

INFORMATION. (1) Facts or data communicated or received. *See also RECORDED INFORMATION* (2) In electronic records, processed data. *See also DATA, RECORDS.*

INFORMATION COPY. A nonrecord copy sent to individuals or offices interested in, but not acting on, a matter. *See also COPY (1).*

INPUT. Data to be entered into a computer for processing.

INPUT RECORDS. Documents designed and used to create, update, or modify records in an electronic medium. Sometimes called source records or source documents. *See also SOURCE DOCUMENTS.*

INSPECTION.

INTEGRATION. (1) Combining various pieces of hardware and software, often acquired from different sources, into a unified system. (2) Combining computer programs into a unified software package so that all programs can share common data.

INVENTORY. (1) A survey of agency records, and often nonrecord materials, that is conducted primarily to develop records schedules and to identify various records management problems.

LABEL. *See NAME.*

LEGAL CUSTODY. *See CUSTODY.*

LIFE CYCLE OF RECORDS. The management concept that records pass through three stages: creation, maintenance and use, and disposition. *See also DISPOSITION, FINAL DISPOSITION, RECORDS CREATION, RECORDS MAINTENANCE AND USE.*

LOGICAL RECORD. In electronic recordkeeping, a collection of related data elements, referring to one person, place, thing, or event, that are treated as a unit and have either a fixed or variable length. *See also RECORD LAYOUT, RECORDS.*

MACHINE-READABLE RECORDS. *See ELECTRONIC RECORDS.*

MACRODATA. Aggregated, or summarized, data. *See also DATA, MICRODATA.*

MAIN FILES. *See MASTER FILES.*

MAINTENANCE AND USE. *See RECORDS MAINTENANCE AND USE.*

MANAGEMENT INFORMATION SYSTEM (MIS). An organization's procedure for accumulating, processing, storing, and retrieving valuable information, usually in electronic media.

MASTER FILES. Relatively long-lived computer files containing an organized and consistent set of complete and accurate data. Usually updated periodically. Also called main files. *See also DOCUMENTATION (3), HISTORY FILES, PROCESSING FILES, TRANSACTION FILES.*

MEDIA. *See MEDIUM.*

MEDIUM. The physical form of recorded information. Includes hardcopy or paper, audiovisual media such as film and video tape, electronic media such as disk(ette)s and magnetic tape, micrographic media such as roll film and

fiche, and other materials on which information can be recorded. Also called record medium. *See also DOCUMENTARY MATERIALS, RECORDED INFORMATION, RECORDS.*

MEMORANDUM. A written communication much like a letter but having no salutation or complimentary ending. Usually used within or between offices of the same organization.

MICRODATA. Unaggregated or unsummarized data. *See also DATA, MACRODATA.*

MICROFICHE. Miniaturized images arranged in rows that form a grid pattern on card size transparent sheet film. Usually contains a title readable without a magnifying device. Sometimes abbreviated as fiche.

MICROFILM. High-resolution film containing micro images.

MICROFILMING. The process of recording microimages on film.

MICROFORM. Any form containing greatly reduced images, or microimages. Roll film microforms include microfilm on reels, cartridges, and cassettes. Flat, or generally unitized, microforms include microfiche, microfilm jackets, aperture cards, and (opaque) microcards. *See also MICRO IMAGE.*

MICROGRAPHICS. The practice of producing or reproducing information in miniature form.

MICROIMAGE. An image too small to be read without a magnifying device or other special equipment.

MICROIMAGING SYSTEMS. Systems constituting a bridge between traditional microforms and electronic records. Include standalone micrographics, computer-assisted retrieval (CAR), computer output microfilm (COM), electronic microimage transmission, and optical disk (OD) systems. Also called image processing or image management systems. *See also COMPUTER OUTPUT MICROFILM (COM), Optical DISK (OD).*

NAME. An alphanumeric term identifying a program, instruction, statement, record, item, or file. Also called a label..

NARA. The National Archives and Records Administration. The agency having overall responsibility for the records disposition program throughout the Federal government and the primary repository for federal permanent retention records. *See also ARCHIVES, DISPOSITION, FINAL DISPOSITION,*

NATIONAL ARCHIVES. *See ARCHIVES, NARA.*

NAMING CONVENTION. *See CONVENTION, NAME.*

NONCURRENT RECORDS. Records no longer required to conduct agency business and therefore ready for final disposition. *See also CURRENT RECORDS, PERMANENT RECORDS, SEMICURRENT RECORDS.*

NONRECORD MATERIALS. These are Government-owned documentary materials in any medium excluded from the definition of records. Includes those materials preserved only for convenience of reference, materials of transitory value such as routine requests for information and letters of transmittal, materials not needed for the conduct of future operations, stocks of publications, blank forms, processed documents, and library or museum materials intended solely for reference or exhibition. *See also COPY (1), DOCUMENTARY MATERIALS, INFORMATION COPY, PERSONAL PAPERS, TECHNICAL REFERENCE FILES, WORKING FILES.*

NONTEXTUAL RECORDS. A collective term applied to types of records usually maintained separately from textual/paper records because their physical form or characteristics require unusual care, in contrast to manuscript

and typescript paper records. They consist of audiovisual, electronic, film and other similar types of materials. *See also TEXTUAL RECORDS.*

OMB. Office of Management and Budget.

OFFICE OF MANAGEMENT SYSTEMS AND ORGANIZATION (OMSO). The OSHA office responsible for Records Management and Directives Management functions. Part of the Directorate of Administrative Programs.

OFFICE OF PRIMARY RESPONSIBILITY (OPR). The agency office delegated responsibility for a specific function. This office normally maintains the official agency record for that function, including the yellow copy of outgoing correspondence and related incoming correspondence, reports, completed forms, reports, and the like. The OPR might be one office or many offices. For example, the OPR for Official Personnel Folders (OPF's) is one office while the OPR for inspection case files is all area offices.

OFFICIAL FILE COPY. *See COPY (1), RECORD COPY, RECORDS.*

OFFICIAL FILE STATION. *See FILE STATION.*

OFFICIAL RECORD COPY. *See RECORD COPY.*

OFFICIAL RECORDS. *See RECORDS.*

OPTICAL CHARACTER RECOGNITION (OCR). A method of entering data into a computer by using an optical scanning device to read the contents of documents.

OPTICAL DISK (OD). A noncontact, random-access disk tracked by optical laser beams and used for mass storage and retrieval of digitized text and graphics or distribution of applications and other programs.

PAPER. *See MEDIUM.*

PERMANENT RECORDS. Any record that has sufficient historical or other value as to warrant its continued preservation is a permanent record of the Federal government. Sometimes called archival records. *See also ARCHIVES.*

PERSONAL PAPERS. Nonofficial, or private, papers relating solely to an individual's own affairs. Personal papers must be clearly designated as such and kept separate from the agency's records. Also called personal files or personal records. *See also NONRECORD MATERIALS, RECORDS.*

PHOTOGRAPHIC RECORDS. Records taking the form of pictures, or photographs, sometimes with related textual records. *See also AUDIOVISUAL RECORDS.*

PRIMARY SUBJECT. *See SUBJECT-NUMERIC FILING SYSTEM.*

PRINTOUT. Output produced by a computer printer, generally on continuous paper sheets.

PRIVILEGED INFORMATION. *See ADMINISTRATIVELY CONTROLLED INFORMATION.*

PROCESSED DOCUMENTS. Supplies such as bond paper, blank forms, empty databases and spreadsheets, unused film, and the like which has been worked on, filled in, data input, pictures produced, etc., thereby producing documentary materials.

PROCESSING FILES. Those data files used to produce a computer master file. Include work files, test files, input/source files, intermediate input/output files, transaction files, and audit trail files. *See also DOCUMENTATION (3) MASTER FILES, TRANSACTION FILES, WORK FILES.*

PROGRAM RECORDS. Records, regardless of medium, documenting the unique, substantive functions, for which an agency is responsible, such as occupational safety and health compliance activities and occupational safety and health standards development, in contrast to administrative records, such as budget and personnel.

PROGRAM RECORDS OFFICER (PRO). The person responsible for overseeing a records management program in a headquarters directorate or independent office in cooperation with the agency records management officer.

PROJECT FILES. A type of case file. Projects are specific undertakings which are not part of normal day-to-day ongoing operations but are special studies or investigations usually to solve problems or determine the best policy, procedure or action.

PUBLIC RECORDS. (1) In general usage, records accumulated by Government agencies. (2) Records open to public inspection by law or custom.

PUBLIC USE FILE. *See DISCLOSURE-FREE EXTRACT.*

PUBLICATIONS. Documents printed or otherwise produced for wide distribution inside or outside an agency.

READING FILES. Extra information copies (usually paper) of outgoing correspondence records arranged chronologically for reference. Sometimes called chronological (chron) or day files. They are used mainly as cross-references to the record copy. Sometimes reading files are considered record copies when they can document policies, decisions, and overall activities of an agency or major subdivision; for example, the chronological files in the Office of the Assistant Secretary document the overall activities of the agency. *See also GENERAL CORRESPONDENCE FILES.*

RECALL. To withdraw or temporarily call back records which have been retired to a records center.

RECORD COPY. The copy of a record, regardless of media, and usually maintained by the office that created it. Also included are incoming correspondence, reports, completed or processed forms, database information, spreadsheets, and the like. *See also COPY (1), READING FILES, RECORDS.*

RECORD CUSTODIAN. *See FILES CUSTODIAN.*

RECORD GROUP. A body of records belonging to an agency.

RECORD GROUP NUMBER. The identifying number assigned by NARA to an agency's functions and records. The Records Group Number assigned to OSHA is 100.

RECORD LAYOUT. A diagram or list of the contents of a logical record describing each data field's informational content, length, and position. *See also, DATA FIELD, DOCUMENTATION (3), FILE LAYOUT, LOGICAL RECORD.*

RECORD MEDIA. *SEE MEDIUM.*

RECORD SERIES. *See SERIES.*

RECORD UNIT. All the materials which provide sufficient documentation for an event, decision, policy, transaction, procedure, operation, project, and the like. Also called a file unit.

RECORDED INFORMATION. Information placed on a medium, such as paper, computer disk, or microform, to be available for later retrieval and use. *See also DOCUMENTARY MATERIALS, FILES, INFORMATION, MEDIUM, NONRECORD MATERIALS, RECORDS.*

RECORDKEEPING. The act or process of records creation and accumulation, maintenance, and disposition. *See also RECORDKEEPING REQUIREMENTS, RECORDS MANAGEMENT.*

RECORDKEEPING REQUIREMENTS. (1) All statements in statutes, regulations, agency directives or authoritative issuances, or other pronouncements providing general and specific guidance for Federal agency personnel on particular records to be created and maintained by the agency. *See also ADEQUACY OF DOCUMENTATION, RECORDS MAINTENANCE AND USE.* (2) Statements in statutes and regulations imposed by an agency on individuals, companies, other Federal agencies, State and local governments, and others, on particular records to be created and maintained or retained but not necessarily provided to that agency.

RECORDKEEPING SYSTEM. *See FILING SYSTEM.*

RECORDS. Documentary materials, regardless of physical form or media, made or received and maintained by an agency to comply with its legal obligations and to provide evidence of the agency's organization, functions, policies, decisions, procedures, operations or other transactions of public business or for their informational value. Includes correspondence, reports, completed forms, case files, photographs, maps, motion pictures, tape recordings, data sets, computer tapes, disk(ette)s, microforms, and other materials. The essential qualifying characteristics of records relate to evidence and information, not physical form or format. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. *See also DOCUMENTARY MATERIALS, FILES, LOGICAL RECORD, MEDIUM, NONRECORD MATERIALS, PERSONAL PAPERS, RECORDED INFORMATION.*

RECORDS (LEGAL DEFINITION). As defined in 44 USC 3301, the term "includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference, and stocks of publications and of processed documents are not included."

RECORDS CENTER. A facility for the low cost storage and servicing of records pending their disposal or transfer to the National Archives.

RECORDS CREATION. The first stage of the records life cycle in which records are made (or received) by an organization.

RECORDS CUSTODIAN. *See FILES CUSTODIAN.*

RECORDS LIAISON OFFICER (RLO). The person responsible for overseeing a records management program in a headquarters or field office under the direction of the appropriate program or regional records management officer. Oversees file custodians in the organization.

RECORDS MAINTENANCE AND USE. Any action involving the storage, retrieval, and handling of records kept in offices by, or for, a Federal agency. This is the second stage of the records life cycle. *See also LIFE CYCLE OF RECORDS, RECORDKEEPING REQUIREMENTS, RECORDS.*

RECORDS MANAGEMENT. The planning, directing, promoting, training, and other managerial activities related to the creation, maintenance and use, and disposition of records to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of agency operations.

RECORDS MANAGEMENT PROGRAM. The planned, coordinated set of policies, procedures, and activities needed to manage an agency's recorded information. Encompasses the creation, maintenance and use, and disposition of records, regardless of media.

RECORDS OFFICER (RO). The person responsible for overseeing an agency wide records management program. Also called records manager.

RECORDS RETIREMENT. *See RETIREMENT*

RECORDS SCHEDULE. A document providing authority for the final disposition of recurring or nonrecurring records. A schedule lists series of records and shows interim disposition measures such as retirement to Federal records centers and the mandatory final disposition of those records and the actions to be taken when the end of that disposition period is reached. Also called records disposition schedule, records control schedule, records retention schedule, or schedule. *See also DISPOSITION AUTHORITY, FINAL DISPOSITION, GENERAL RECORDS SCHEDULE, SCHEDULED RECORDS, SCHEDULING, UNSCHEDULED RECORDS.*

RECORDS SERIES. *See SERIES.*

RECORDS STORAGE FACILITY. *See ARCHIVES, FEDERAL RECORDS CENTER, RECORDS CENTER.*

REFERENCE COPY. *See INFORMATION COPY, READING FILES.*

REGIONAL RECORDS OFFICER (RRO). The person responsible for overseeing a records management program throughout a region in cooperation with the agency records management officer.

RETENTION. *See DISPOSITION.*

RETENTION SCHEDULE. *See RECORDS SCHEDULE.*

RETIREMENT. The transfer of records to agency storage facilities or a Federal records center. *See also ACCESSION (2) AND (3), DISPOSITION, TRANSFER.*

RIGHTS-AND-INTEREST RECORDS. That type of vital records essential to protecting the rights and interests of an organization and of the individuals directly affected by its activities. *See also VITAL RECORDS.*

SCHEDULED RECORDS. Records whose final disposition has been approved by NARA, through the General Records Schedules or submission of a records schedule. *See also DISPOSITION, FINAL DISPOSITION, RECORDS SCHEDULE.*

SCHEDULING. The process of developing schedules for the disposition of records, along with disposition instructions for nonrecord materials. *See also DISPOSITION, RECORDS SCHEDULE.*

SECONDARY SUBJECT. *See SUBJECT-NUMERIC FILING SYSTEM.*

SEMICURRENT RECORDS. Records required so seldom to conduct agency business that they should be moved to a holding area or directly to a records center. *See also CURRENT RECORDS, NONCURRENT RECORDS.*

SERIES. Also called a record series. A group of documents concerning the same or related functions which are disposable under one item of a records schedule. Nonelectronic records are generally scheduled by series whereas electronic records are generally scheduled by information system. *See also RECORDS SCHEDULE.*

SOURCE DOCUMENTS. Documents containing data entered into a microform or electronic records system. Also called source records. *See also INPUT RECORDS.*

SPECIAL RECORDS. *See NONTEXTUAL RECORDS.*

STOCK COPY. An extra copy of printed records or of other published materials. *See also COPY (1), PUBLICATIONS, TECHNICAL REFERENCE FILES.*

SUBJECT CLASSIFICATION SYSTEM. A plan used for identifying and coding documents by topic to provide an orderly and accurate way of filing and finding.

SUBJECT-EXPANSION FILES. Authorized subdivisions of the prescribed subject files made in a particular office to provide for expansion of a particular subject so that information may be further broken down for the convenience of filing and retrieval. Subject-expansion files are regarded as an integral part of the subject files, and are designed for needs which are unique to a given office. Subject-expansion files are identified by use of alphabetic coding. Example: PER 12 A (PERSONNEL 12 is Retirement while "A" could be early outs.).

SUBJECT FILES. *See GENERAL CORRESPONDENCE FILES.*

SUBJECT-NUMERIC FILING SYSTEM. An organizational subject classification system in which the main topics consist of a selected number of primary subject titles arranged alphabetically and the secondary (second), and tertiary (third) subdivisions of the primary subjects are arranged numerically. These subdivisions of the filing system are called: (1) *PRIMARY SUBJECTS* are the prime or major subject designations that identify and describe groups of related records. (2) *SECONDARY SUBJECTS* are one or more related subjects that have been created or established by the division of a primary subject. (3) *TERTIARY SUBJECTS* are one or more related subjects that have been created or established by the division of a secondary subject. This system is modified by adding an abbreviation creating a file code so that, for example, "Personnel 8" becomes "PER 8."

SUBJECT OUTLINE. A list of topics arranged hierarchically (i.e., by primary, secondary, and tertiary topics) and serving as the source for selecting file designations for arranging, or classifying, the documents of a subject file. Normally uses file codes.

SUMMARIZED DATA. *See MACRODATA.*

SUSPENSE FILES. Files arranged chronologically to remind officials of actions to be completed by a specific date or other indicator. Also called FOLLOW UP files or tickler files. *See also COPY (1).*

TECHNICAL REFERENCE FILES. Nonrecord copies of correspondence, forms, articles, periodicals, reports, studies, vendor catalogs, and similar materials that are needed for reference and information but are not properly part of the office's records. *See also CONVENIENCE FILES, NONRECORD MATERIALS, WORKING FILES.*

TEMPORARY RECORDS. Records approved by NARA for disposal, either immediately or after a specified retention period, when their administrative, legal, fiscal, and evidentiary value ends. *See also DISPOSAL, FINAL DISPOSITION, PERMANENT RECORDS.*

TERTIARY SUBJECTS. *See SUBJECT-NUMERIC FILING SYSTEM.*

TEXTUAL RECORDS. Narrative, manuscript, typescript, or tabular paper documents, such as letters, memorandums, and reports, organized in a loosely prescribed form and format as distinct from electronic, audiovisual, cartographic, remote-sensing imagery, architectural, and engineering records. *See also NONTEXTUAL RECORDS.*

TICKLER FILES. *See SUSPENSE FILES.*

TRANSACTION FILES. (1) *See CASE FILES.* (2) In electronic recordkeeping, files containing new data to be processed together with master files to create updated master files. *See also MASTER FILES, PROCESSING FILES.*

TRANSFER. The act or process of moving records from agency storage facilities or Federal records centers to the National Archives for permanent preservation.

UNAGGREGATED DATA. *See MICRODATA.*

UNSUMMARIZED DATA. *See MICRODATA.*

UNSCHEDULED RECORDS. Records whose final disposition has not been approved by NARA and, therefore, may not be destroyed. *See also DISPOSITION, FINAL DISPOSITION, RECORDS SCHEDULE.*

VITAL RECORDS. Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities. Includes both emergency-operating and rights-and-interests records. *See also EMERGENCY OPERATING RECORDS, RIGHTS-AND-INTEREST RECORDS.*

WITHDRAWAL. *See RECALL.*

WORK FILES. In electronic recordkeeping, temporary files in auxiliary storage. *See also PROCESSING FILES.*

WORKING FILES. A collection of drafts, rough notes, extra copies of correspondence, tapes, graphs and charts, calculations, and other preliminary materials related to a particular project or activity. Although working file materials record certain activities and are included in the definition of records, their documentary value ceases after their purpose is served unless there is a continuing need to document the official file. *See also CASE WORKING FILES, CONVENIENCE FILES, NONRECORD MATERIALS, RECORDS, TECHNICAL REFERENCE FILES.*

II. Abbreviations and Acronyms

ADP	Automatic data processing or automated data processing.
CD	Compact disk.
COM	Computer output microfilm.
CPU	Central processing unit.
DAT	Digital audio tape.
DBMS	Database management system.
EDP	Electronic data processing.
ER	Electronic records.
ERK	Electronic recordkeeping.
FOIA	Freedom of Information Act.

FRC	Federal records center.
GRS	General Records Schedule.
LAN	Local area network.
MIS	Management information system.
NARA	National Archives and Records Administration.
OCR	Optical character recognition.
OD	Optical disk.
PC	Personal computer.
PRO	Program Records Officer
RAM	Random access memory.
RLO	Records Liaison Officer.
RO	Records Officer.
ROM	Read only memory.
RRO	Regional Records Officer
SF	Standard Form.
WORM	Write once read many.

Appendix C

CARE OF ELECTRONIC RECORDS

I. General.

This appendix is a guideline for agency personnel concerning care of electronic records and record systems. The increased use of personal computers and other electronic office equipment results in more employees, ranging from senior program officials to clerks, making decisions concerning the maintenance, accessibility, and preservation of information.

II. Record Storage Medium.

Records may be stored on a variety of media including paper, microform, magnetic tape or disk, and optical digital data disks. Each medium has characteristics that may make it suitable or unsuitable depending upon the requirements. The characteristics of various media are shown in Appendix D. If a magnetic medium is chosen to store records, the records should meet the following minimum requirements:

- Need to quickly retrieve the information.
- Need to manipulate the information.
- Need to retain the information on electronic media until the authorized disposition date.

III. Records Labeling.

To retrieve information created and stored electronically, the user is dependent upon labels, both external and internal (directories). Accurate and complete labels are essential to ensure that agency personnel can identify the contents of individual disks and diskettes and that they can retrieve information stored on them.

IV. External Labels.

Accurate and complete external labels are necessary regardless of how an office chooses to store the information it creates and/or accumulates.

Insufficient external labels result in the inability to identify the contents of disks and diskettes. A label such as "Smith 3" or "Jane 5" generally is of use only to the creators

and sometimes not to them.

External labels should include the title of the file, file code, inclusive dates, software used, and the identification of the equipment on which the records were created. For example; a label might contain the following information:

ADM 9 OSHA Goals 4/97 - 5/31/97 WordPerfect 6.1 Pentium PC

V. Internal Labels.

Agency personnel need to use readily understandable and standard internal document labels so that they, their colleagues, and their successors can retrieve information which is stored electronically.

The agency's file code headings and subheadings should be used in labeling electronically created records wherever possible. Every document should be named, dated, and described. The labels should be accurate and sufficiently detailed to permit the user to retrieve documents previously created. Enter the descriptions on the diskette directory (internal label) as part of the file title.

The user should make every effort to obtain software which requires the entry of whether the item is a record, its file code, subject terms, the date the document is created and its disposition date. This information should reflect the OSHA filing system and records disposition schedules. For example:

CPL 2 Inspection Correspondence 5/1/97 - 5/30/96 Destroy 10/99.
--

VI. Indexing Electronic Records.

Electronic records need to be indexed to permit their retrieval. System software should provide the means of accomplishing this.

The complexity of the electronic indexing system must strike a balance between the volume of records, how long the records must be retained, and the familiarity of the persons retrieving the records. Do not assume that since the current users are very familiar with the records that either no index or only a very limited index is needed. Remember that employee turnover and reorganizations are a fact of life. Consider what

indexes will be required by personnel unfamiliar with the records or the function. Also consider what indexes will be required by persons or organizations to whom the records may be transferred.

In a small system, the diskettes may be largely self-indexing if they are properly labeled.

The electronic indexing system should be capable of locating the records based upon the characteristics of the particular record. The characteristics could include such things as date, subject, sender, receiver, and number as in an inspection, contract, purchase order, or travel voucher. Operating instructions, including system architecture, for the index should be in an easily accessible part of the system documentation.

If there are more than a few diskettes, the electronic directories may need to be logically subdivided to be easily retrievable. Diskette directories should be printed out to ensure easy access to them.

VII. Security.

Special precautions may need to be taken to ensure the security of data stored electronically. Before developing solutions, however, determine the degree of risk. This can be done by following established risk management techniques, keeping a reasonable ratio between the cost of the risk management study and the likely risk to be identified. The following items need to be considered:

- Poor quality electrical power may cause equipment to malfunction and affect the electronic records. Check with your administrative office or the Office of Administrative Services to find out what steps need to be taken to prevent problems of this type. Some problems can be solved with inexpensive devices. More serious problems may require additional electrical circuits.
- Cleanliness of equipment and magnetic media can affect the records. See paragraph G for suggestions.
- Procedures for using the equipment and the records may need to be examined to ensure that only authorized persons have access. The provisions of the Privacy Act and the protection of sensitive information should particularly be considered. Problems identified may be solved by limiting physical access or by encrypting the data.
- Make copies of vital or master flexible disks and store in an alternate location. This will protect your electronic records in the event of fire, water damage, or other physical problem. Also, electronic media may deteriorate or a machine malfunction may cause erasure of the data. Make copies of electronic records

before problems arise.

VIII. Disk Maintenance and Care.

Maintain a clean working environment.

- Contamination of the flexible disk surface is a serious cause of data losses.
- Do not touch the exposed media surface through the elongated, oval slot where the head-to-disk access or contact is made.
- Avoid touching the exposed media surface area near the hub.
- Finger oil, smoke, food and drinks, abrasive materials such as dust or filings, pencil eraser debris, and the like, are typical contaminants.

Read/write heads last longer when used with clean media.

Clean the flexible disk drive regularly, particularly at its insertion slot position. Dirt and dust can be picked up by the disk during operation.

Clean the read/write heads on a regular basis. (Contact individual manufacturers for head cleaning information since some flexible disk head and drive manufacturers will invalidate their warranties if some types of head cleaner are used.)

- Dilute isopropyl alcohol on a lint-free swab will clean contaminants from the head. Exert minimum force on the delicate tension springs.
- Cleaning kits are available which employ flexible disks made of a special material as the rotating media rather than the magnetic media of the regular disks. The cleaning material is either run dry or wetted with a cleaning fluid. The head is then lowered onto the surface and cleaned under rotation.
- Consult the equipment manufacturer's cleaning instructions when using cleaning kits. Kit manufacturer's suggestions for cleaning vary from a daily cleaning to as infrequently as when data errors appear.

Handle, use and store the diskette with care so the magnetic media will not be damaged.

Always return the flexible disk to its protective envelope after it is used. This prevents contamination and physical damage to the media. Don't lose the envelope. Don't scatter the disks around on table tops and desks in a random fashion.

Don't flex or fold the flexible disks. Avoid bending the disk loading into or extracting it from the drive. Although the envelope may recover, the internal media may be damaged permanently. A warped disk does not rotate properly.

Don't put a rubber band or a paperclip onto the flexible disk envelope. The rubber band may cause the disk to remain bent permanently after long-term storage. The paperclip may emboss the media and cause permanent data losses due to head-to-media separation.

Always write on the label before it is applied to the disk. However, if the original label is used, do not write on it with a ball point pen. A ball point pen can emboss the surface of the disk and cause permanent surface defects and data losses. Do not use a pencil. Use a soft, fiber tipped pen.

Never erase the label on a flexible disk cartridge. Cross out previous information and replace the label when full. Erasure can be a source of contamination. Don't paste a new label over the old label and do not cover any flexible disk holes with the new label.

Don't use a flexible disk as a place mat.

Discontinue the use and acquisition of flexible disks which appear to shed excess debris and cause rapid head wear. They may have abrasive surfaces which create considerable friction and heat and usually have short operating lives. A rapid decrease in the disk signal level may indicate a rapidly wearing disk surface. Inspect and replace worn head pads if necessary.

Never place a magnet of any kind onto the envelope surface of a flexible disk cartridge. These include typical bar magnets found in offices, coat and picture hanger magnets, flashlight magnets, magnetized screwdrivers, etc. Keep magnets at least 76 mm (3 inches) away from recorded disks. This applies to both rigid and flexible disks.

Flexible disks should be stored in a vertical position in a storage container. Do not use a cardboard container. Use a more rigid type of container such as a hard plastic unit.

Do not use reinforced flexible disk hub rings. Use flexible disks having a rigid hub material.

Maintain a schedule for checking, cleaning, or replacing associated air filters. Dirt causes data losses and media damage.

Use the tabs which are supplied with the disks to cover the write protect notch on the disk envelope. Do not use any tab which leaves a sticky residue.

Electrical discharges produced by static electricity cannot damage or alter the data which

has been correctly recorded and stored on flexible disks.

IX. Environmental Considerations.

Acceptable temperatures and humidities are normally maintained in an operating area such as an office. Be careful about the storage location and especially about transportation. The temperatures in a closed, hot, stationary automobile in the sunlight may exceed the upper limits. Excessively cold temperatures may make disks rigid. Acclimatize the affected disks in a normal temperature and humidity environment for several hours before using.

Offices must apply the following environmental standards to assure the viability of the magnetic media during operation, storage and transportation of flexible disk cartridges. Failure to observe the temperature and humidity guidelines can result in media damage. The following general environmental standards are applicable to all flexible disk cartridges with the exception of the special conditions so marked below

Operation and Storage.

Temperature: 50°F to 125°F (10°C to 51.6°C). Relative Humidity: 8% to 80%.

Wet Bulb Reading: Not to exceed 85°F (29.4°C).

Transportation.

Temperature: -40°F to 125°F (-40°C to 51.6°C). Relative Humidity: 8% to 90%.

Special Conditions affecting flexible disk cartridges.

130 mm (5-1/4 inch) flexible disk cartridge (single sided, 48 tpi). During operation and storage, condition at least one hour before operating. For further information, refer to ANSI X3.82-1980.

130 mm (5-1/4 inch) flexible disk cartridge (double sided, double density, 48 tpi). During operation and storage, condition at least 24 hours before operation. Rate of temperature change must not exceed 36°F (20°C) per hour. For further information, refer to ANSI X3.125-1984.

130 mm (5-1/4 inch) flexible disk cartridge (double sided, 96 tpi). During operation and storage, temperature in the 50°F to 115°F (10°C to 46.1°C) range. Relative Humidity between 20% to 80%. Wet Bulb Reading not to exceed 80°F (26.6°C) conditions at least 24 hours before operating. Rate of temperature change shall not exceed 36°F (20°C) per hour. For further Information, refer to ANSI X3.126-1985.

X. Additional Information.

Care and Handling of Computer Magnetic Storage Media. NBS Special Publication 500-101, June 1983, National Bureau of Standards, Department of Commerce. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402, order number: S.N. 003-003-02486-4.

Refer to 36 CFR Chapter XII (NARA) which furnish guidelines on the care and handling of magnetic computer tape.

Appendix D

COMPARISON OF VARIOUS MEDIA
FOR INFORMATION STORAGE AND RETRIEVAL

Paper	Microfilm	Magnetic	Optical (CD)
Strengths			
Versatile and flexible	Saves storage space	Very fast access	Saves Space
Easy for people to use	Low bulk	Good standards	Short turnaround time
Least equipment investment	Records retain integrity - no losses, misfiles or missing pages	Can use with other media to manage work flow	Excellent control over documents and workflow
Very long life, with care	Inexpensive copies	Excellent availability to information	Records retain integrity
Most legally acceptable	Long life expectancy, with care	Easily updated	Can add and replace records
	Most systems adhere to established standards		Can link computer database with record information
	May speed retrieval, if indexed		Very fast retrieval
	Equipment tends to be interchangeable		Can store both images and machine-readable records
	Thoroughly tested legal acceptability		Excellent availability to information
Weaknesses			
Hard to control	Special equipment needed	Special equipment needed	Special equipment needed

Paper	Microfilm	Magnetic	Optical (CD)
Easily lost	Difficult to add or update a record	Very vulnerable to inadvertent change or loss	Easier to use than microfilm but not as easy as paper
Easily damaged	Not as easy to use as paper	Not a permanent record	Not a permanent record
Single person access	Must convert most documents	Must be substantiated by documentation	Costly per user and to add users
Labor intensive	Conversion time can interrupt workflow	Periodic migration of records to new hardware and software	Periodic migration of records to new hardware and software
	Limited use during processing		
Application Suitability			
Small collections of records	Records of medium to high volume with low to medium retrieval rates	Records in draft or that have relational aspects	Records of high volume with low to medium value
Very long multi-page records	Vital record collections	Transitory information	Records requiring fast access
Records with low number of references	Records where the entire collection must be available	Records that need to be examined or searched in different ways for reporting	Records subject to errors or long processing times that require controls on original form or location
Records with limited uses or not needing massaging	Records requiring long inactive storage	Information intended to manage or locate other records	Records having high reference rates for short periods of time
Historically significant records	Records having very long retention periods	Records requiring very fast access	Records needing to be recorded before processing

Paper	Microfilm	Magnetic	Optical (CD)
Long-retention records	Records with few additions or deletions over time	Records that need to be easily shared	Information suitable for publication
Short-term records	Records requiring high file integrity		Records valuable to organization
	Records are transactions, reference or inactive and unitized		Transactional records
	Records are publications		Reference materials and publications
			Storage of machine-readable records

Appendix E

RECORDS TRANSFER FORMS

Examples of the SF-135, Records Transmittal and Receipt, records transfer forms for the National Office and the field are on the following pages together with the instructions on the reverse of the forms as Figures E-1, E-2 and E-3. For additional information on transferring records to Federal Records Centers, see Chapter VIII.

Figure E-1

SF-135 NATIONAL OFFICE EXAMPLE

RECORDS TRANSMITTAL AND RECEIPT		Complete and send original and two copies of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.		PAGE	OF
1. TO		2. FROM (Enter the name and complete mailing address of the office retaining the records. The signed receipt of this form will be sent to this address.)		1	1
As shown in FPMR 201-11.400-1 Federal Archives and Records Center General Services Administration Washington, D.C. 20409		DOL, Occupational Safety and Health Administration Office of Management Systems and Organization N3618 Frances Perkins Building 200 Constitution Ave., NW Washington, D.C. 20210			
2. AGENCY NUMBER AUTHORITY ORGANIZATION (Leave blank)		TRANSFERRING AGENCY OFFICIAL (Name, office and telephone No.) DATE			
3. AGENCY CONTACT (Leave blank)		TRANSFERRING AGENCY LAIBSON OFFICIAL (Name, office and telephone No.) DATE			
4. RECORDS CENTER RECEIPT (Leave blank)		(Transferring Office Contact) DATE			
RECORDS DATA					
ADMISSION NUMBER		AGENCY NUMBERS		SERIES DESCRIPTION (With inclusive dates of records)	
RG	FY	VOLUME (ex. Jc.)	AGENCY NUMBERS	DISPOSAL AUTHORITY (Schedule and item number)	DISPOSAL DATE
(a)	(b)	(c)	(d)	(e)	(f)
100	98	0007	2	1-2	2
				DOL, OSHA, Federal/State Operations, Office of State Programs N3700 Frances Perkins Building Consists of State Plan Files. Closed Fiscal Year 1994	
				Obsolete State Plan Elements for Alaska, Arizona, Nevada, New Mexico, Oregon, Washington, and Wyoming. Obsolete in FY 1993. Folder listing attached.	
				NI-100-93-1 Item 1A	Permanent
				COMPLETED BY RECORDS CENTER	
				LOCATION	
				DATE	
				BY	
				INITIALS	
				SIGNATURE	

Standard Form 135 (Rev. 6-76)
 Prescribed by GSA
 FPMR (41 CFR) 101-11.4

Figure E-2

SF-135 FIELD OFFICE EXAMPLE

RECORDS TRANSMITTAL AND RECEIPT		Complete and send original and two copies of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.		PAGE	OF	PAGES	
<p>1. TO (Complete the address for the appropriate records center serving your area)</p> <p style="text-align: center;">Federal Archives and Records Center General Services Administration</p> <p>Washington National Records Center Washington, D.C. 20409</p>		<p>5. FROM (Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address)</p> <p style="text-align: center;">DOL, OSHA Minneapolis Area Office Federal Courts Building, Room 116 110 South 4th St. Minneapolis, MN 55401</p>		1	1		
<p>2. AGENCY TRANSFER AUTHORITY (Leave blank)</p> <p>TRANSFERRING AGENCY OFFICIAL (Signature and title)</p> <p>(Leave blank)</p>		<p>DATE</p>					
<p>3. AGENCY CONTACT</p> <p>TRANSFERRING AGENCY LIAISON OFFICIAL (Name, office and telephone No.)</p> <p>(Transferring Office Contact)</p>		<p>DATE</p>					
<p>4. RECORDS CENTER RECEIPT</p> <p>RECORDS RECEIVED BY (Signature and title)</p> <p>(Leave blank)</p>		<p>DATE</p>					
RECORDS DATA							
ACCESSION NUMBER		VOLUME (ex. 7/L)	AGENCY BOX NUMBERS	SERIES DESCRIPTION (With inclusive dates of records)	DISPOSAL AUTHORITY (Schedule and item number)	DISPOSAL DATE	COMPLETED BY RECORDS CENTER
RG (a)	FY (b)	NUMBER (c)	(d)	(f)	(h)	(i)	LOCATION (j)
100	97	0001	5	Consists of Safety Inspection Case Files, Fiscal Year 1995. General Safety Inspections	NCI-100-82-1 Item 7a	10/2001	
100	97	0002	1	5 a 1 Safety Inspections	NCI-100-82-1	10/2005	

Standard Form 135 (Rev. 6-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.4

INSTRUCTIONS FOR COMPLETION OF STANDARD FORM 135

FOR COMPLETION BY THE TRANSFERRING AGENCY

Items 1, 2, 3 and 5 are self-explanatory. Specific instructions for item 6 are as follows:

Col.

Accession Number. A separate accession number is required for each series of records listed on the form. A series consists of records having the same disposal authority and disposal date that are transferred together to the records center. The accession number is entered in three parts, consisting of:

- (a) The NARS record group number assigned to the records of the agency making the transfer;
- (b) The last two digits of the current fiscal year; and
- (c) A four digit sequential number obtained in advance from the records center. (Arrangements may be made with the center to have these numbers assigned by the agency records officer or other official.)

(d) *Volume.* Enter the volume in cubic feet of each series of records being transferred.

(e) *Agency Box Numbers.* Show the inclusive box numbers for each series of records being transferred. The agency shall number each carton sequentially as follows: 1 of 25, 2 of 25, 3 of 25, etc. (Each new series of records should begin with carton number 1.) To facilitate control of the records and future reference service, the agency also shall mark each container with the assigned accession number prior to shipment.

(f) *Series Description.* Describe the records in sufficient detail to allow the records center to check for proper application of the disposal schedule. Inclusive dates of the records should be indicated. Show the organizational component that created the records when it is other than that shown in item 5.

(g) *Restriction.* Enter one of the following codes to show a restriction on use of the records. Restrictions other than (or in addition to) security classifications, such as limiting access to certain agency officials, are to be specified by a statement in the Series Description column (f).

Code	Restrictions
Q	Q security classification
T	Top Secret security classification
S	Secret security classification
C	Confidential security classification
R	Restricted use—witnessed disposal <i>not required</i> (specify in column (f))
W	Restricted use—witnessed disposal <i>required</i> (specify in column (f))
N	No restrictions

(h) *Disposal Authority.* For each series of records, cite the agency schedule and specific item number authorizing disposal. Cite the NARS disposal job and item number if it has not been incorporated into an updated agency schedule.

(i) *Disposal Date.* Applying the disposal authority previously cited in column (h), enter the month and year in which the records may be destroyed.

FOR COMPLETION BY THE RECORDS CENTER

Item 4 is self-explanatory. Specific instructions for item 6 are as follows:

Col.

(j) *Location.* The records center annotates the shelf location of the first carton for each series of records.

(k) *Shelving Plan.* The records center enters the appropriate code from Chap. 7-10c, IIB, Records Center Operations (NAR P 1864.1A), to reflect the shelving system.

(l) *Container Type.* The records center enters the appropriate code from Chap. 7-10b, NAR P 1864.1A, to reflect the type of container in which the records are retired.

(m) *Automatic Disposal.* The records center enters either Y (yes) to indicate automatic disposal applies or N (no) indicating that the agency wishes to receive disposal concurrence notice prior to destruction of the records. Automatic disposal is applied only when previously agreed upon by the agency.

Use Standard Form 135-A, Records Transmittal and Receipt Continuation, when additional space is required for listing records data.

Standard Form 135 Book (Rev. 6-76)

GPO 1976 - 238-011

Appendix F

RECORDKEEPING PRACTICES CHECKLIST

I. HOW TO USE THIS CHECKLIST

- A. Offices need to review their recordkeeping practices at least once each year; when functions are added, changed or deleted; or whenever a new record keeper comes on board. This checklist is designed to assist you in this evaluation.
- B. Check either the "yes" or "no" box after reading each question. If your answer to any question is "no," see if you need to take corrective action. The general rules following the questions can give you a start in resolving any problems.
- C. You do not have to complete the checklist all at once. The questions are grouped so that you can answer them when you have time. We suggest, however, that you do an entire section together, since the questions in each are interrelated. At the end of each group of questions are references to publications that contain information relevant to that section.
- D. If you find that you need more help or information, contact your supervisor or your records liaison. They will then confer with the OSHA Records Officer if necessary.
- E. This checklist is designed for use primarily by the custodian(s) of the files in an office. However, it can also be useful for the records liaison or responsible program official in evaluating the files management activities of an office. For more comprehensive reviews of the records management program of an office, contact the OSHA Records Officer.

Appendix F

RECORDKEEPING PRACTICES CHECKLIST

I. HOW TO USE THIS CHECKLIST

- A. Offices need to review their recordkeeping practices at least once each year; when functions are added, changed or deleted; or whenever a new record keeper comes on board. This checklist is designed to assist you in this evaluation.
- B. Check either the "yes" or "no" box after reading each question. If your answer to any question is "no," see if you need to take corrective action. The general rules following the questions can give you a start in resolving any problems.
- C. You do not have to complete the checklist all at once. The questions are grouped so that you can answer them when you have time. We suggest, however, that you do an entire section together, since the questions in each are interrelated. At the end of each group of questions are references to publications that contain information relevant to that section.
- D. If you find that you need more help or information, contact your supervisor or your records liaison. They will then confer with the OSHA Records Officer if necessary.
- E. This checklist is designed for use primarily by the custodian(s) of the files in an office. However, it can also be useful for the records liaison or responsible program official in evaluating the files management activities of an office. For more comprehensive reviews of the records management program of an office, contact the OSHA Records Officer.

II. CHECKLIST

YES	NO	Description
A. RECORDKEEPING PRACTICES		
<input type="checkbox"/>	<input type="checkbox"/>	<p>1. Are you aware of the types of materials that your office has decided it must maintain in order to document its activities?</p> <p><i>General rule: Your agency has determined which records made or received by your office must be kept to document its activities. They are defined in your agency*@ records schedule. You should be aware of the schedule items that apply to your office's recordkeeping requirements.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>2. Do people in your office clearly understand which papers they deal with are Federal records, which are nonrecord material, and the differences in how they are handled?</p> <p><i>General rule: There are different policies and procedures for the management of record and nonrecord materials. Records may only be maintained and disposed of as prescribed by your agency *@ records schedule. The records schedule may also contain instructions for nonrecord materials.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>3. Are personal papers maintained separately from official records?</p> <p><i>General rule: Records documenting the official business of Federal agencies are the property of the Government, not of individuals. Documentary materials that relate only to an individual*@ personal affairs and do not relate to or affect the conduct of agency business are considered personal papers (and private property). Keep personal papers separate from official records.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. Does your office have a single official files location or several stations? Does it forbid maintenance of records in other places?</p> <p><i>General rule: You should have designated files in which to keep your official records. Staff should not keep records in other places.</i></p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>5. Do you maintain electronic, microform, and audiovisual records as carefully as you maintain paper files?</p> <p><i>General rule: These non-paper materials are records and should be maintained in a manner appropriate to their use and format. You should know which copy is the record copy and what constitutes a complete record.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>6. Do you follow the standards in your agency's regulations for storage of security-classified documents?</p> <p><i>General rule: Classified information must be stored in locations and equipment that ensure access is limited exclusively to authorized persons.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>7. Are Privacy Act materials and other restricted records stored in locked file cabinets?</p> <p><i>General rule: Records accessible by personal names, Social Security numbers, or other personal identifiers, and records containing sensitive or restricted information must be stored in locked file cabinets to prevent access by unauthorized persons.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>8. Are permanent series of records clearly identified and maintained separately from temporary series?</p> <p><i>General rule: Permanent records eventually are kept in the National Archives. They need special care by agencies to prevent damage or accidental destruction.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>9. Have "vital records" been identified and provisions made for their duplication and preservation?</p> <p><i>General rule: Vital records are records that are necessary to ensure an agency's continued operation during and after an emergency or records that protect the rights and interests of the Government and individuals. Duplicate copies of vital records must be separately maintained</i></p>

YES NO	Description	
<input type="checkbox"/> <input type="checkbox"/>	10.	<p>Do you have procedures established for staff to follow when they wish to use records?</p> <p><i>General rule: You should have reference and charge out procedures that facilitate the finding, borrowing, and refiling of records.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	11	<p>Are office supplies, personal belongings, and stocks of blank forms and publications kept out of file cabinets?</p> <p><i>General rule: Filing cabinet space is valuable and should not be wasted on such items. These materials should be stored in supply cabinets, shelving, or other suitable locations.</i></p>
<p>B. FILE LESS</p>		
<input type="checkbox"/> <input type="checkbox"/>	1.	<p>Does someone in your office determine whether each document being created or received must be filed?</p> <p><i>General rule: In every office where files are maintained, someone should make this determination; otherwise many papers may be filed that need not be.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	2.	<p>Does your office have a policy that the following materials are not to be filed?</p> <ul style="list-style-type: none"> • envelopes • routing slips lacking significant notations • duplicates of correspondence and reports not needed for cross-reference <p><i>General rule: Every office should have a firm rule that such obviously unneeded papers will not be filed. Keeping this material out of the files prevents wasted effort, saves filing space and equipment, and makes it easier to find papers when they are needed.</i></p>

YES NO		Description
<input type="checkbox"/> <input type="checkbox"/>	3.	<p>Are information copies from other offices that are not needed for future reference or that do not concern your office discarded without filing?</p> <p><i>General rule: Information copies intended to keep officials posted and not needed for future reference usually should not be filed.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	4.	<p>In responding to purely routine correspondence (such as requests for publications or routine inquiries) does your office use one or both of these methods:</p> <p>(a) reply on the incoming letter, which is returned to the sender, or</p> <p>(b) reply by form letter, printed slip, or other ready-made answer, a file copy of which is not made?</p> <p><i>General rule: Unless agency policy dictates otherwise, one or both of these practices should be followed. They eliminate preparation of file copies of replies and unnecessary filing.</i></p>
C. BREAK FILES DOWN		
<input type="checkbox"/> <input type="checkbox"/>	1.	<p>Have the files in the office been broken down into the major file types (case, subject, transitory, and technical reference)?</p> <p><i>General rule: Files should be broken down into file types to simplify filing and facilitate finding and disposal</i></p>
<input type="checkbox"/> <input type="checkbox"/>	2.	<p>Are the documents within each file type or series arranged according to the way they are requested by office staff?</p> <p><i>General rule: Arrange documents within each file type according to the filing feature most often referred to by the users.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	3.	<p>Are indexes to the files worth the time, effort, and cost required to prepare and maintain them?</p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. If required, is the index for a file arranged by the second most often known filing feature?</p> <p><i>General rule: Create an index only when the work required for maintaining the index is less than that involved in making an occasional extended search of the main file or when requests are so urgent that users cannot wait for an extended search. An index should be arranged by the filing feature second most frequently requested by staff. Indexes to permanent records need to be retained with the permanent records.</i></p>
D. CASE FILING		
<input type="checkbox"/>	<input type="checkbox"/>	<p>1. Do you know what records must be included in your offices case files?</p> <p><i>General rule: Your agency should have established and communicated to you rules for what materials are necessary to include in case files your office may have.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>2. Do all case filed papers contain standard case identifiers such as number, name, or code?</p> <p><i>General rule: Case identifiers should be shown on all papers belonging in a case file and appear in a consistent location.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>3. Are case working papers kept separate from regular case records?</p> <p><i>General rule: A separate working papers file should be established to manage the case's bulky background and supporting papers. They may be filed near the case files themselves. A separate disposal date is usually established for working papers.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. When documents that close a case are filed, is the case file clearly marked "CLOSED <u> (date) </u> " and filed separately from the active cases?</p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>5. Is timely disposition made of closed case files in accordance with the agency records schedule?</p> <p><i>General rule: As cases are closed, they should be marked "closed" Inactive closed case files should not remain in office filing cabinets. As prescribed in the agency records schedule, they should be removed to an inactive files area or to a records center or should be destroyed.</i></p>
E. SUBJECT FILING		
<input type="checkbox"/>	<input type="checkbox"/>	<p>1. Do subject files contain only official record copies filed by the subject they concern?</p> <p><i>General rule: Documents that are filed by their general subject content should be kept separate from records that can be case filed by a number, name, place, organization, or thing. Only substantive official records should be allowed in subject files.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>2. Are program subject files kept separate from administrative subject files?</p> <p><i>General rule: Subject files that contain substantive information about the program operation of your office should be kept separate from administrative (housekeeping) subject files. The latter usually have shorter retention periods.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>3. Is transitory correspondence kept apart from subject files?</p> <p><i>General rule: Reading files, information copies, acknowledgments, routine inquiries, and announcements should be kept separate from subject files. They are nonrecord or have shorter retention periods than subject files.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. Have subject topics been clearly defined to assure consistency in filing?</p> <p><i>General rule: Definitions should be written for all primary topics and any second- or third-level subjects that require clarification.</i></p>

YES NO		Description
<input type="checkbox"/> <input type="checkbox"/>	5.	<p>Are subject files cut off periodically and retired or disposed of when eligible?</p> <p><i>General rule: Subject files should not hold papers that are more than 1 year old. At the end of each year, close the file and start a new one. Closed, inactive files should be removed from file cabinets and retired or destroyed in accordance with the agency's records schedules.</i></p>
F. ELECTRONIC RECORDS		
<input type="checkbox"/> <input type="checkbox"/>	1.	<p>Are equipment users aware of the record status of electronic records?</p> <p><i>General rule: Electronic documents that relate to the transaction of public business are Federal records.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	2.	<p>Are the records created on your office's computer equipment disposed of or preserved in accordance with the agency records schedule or the General Records Schedules?</p> <p><i>General rule: Electronic records may not be erased, deleted, scratched or otherwise disposed of without the authority of a NARA-approved schedule.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	3.	<p>Are equipment users required to list or index the records that they create?</p> <p><i>General rule: Electronic indexes should assist in locating particular records by date, subject, case identifier, sender, or receiver as appropriate to the file type.</i></p>
<input type="checkbox"/> <input type="checkbox"/>	4.	<p>Do equipment users create adequate external labels for storage media?</p> <p><i>General rule: Disks, tapes, and other storage media require external labels with identifying information, including national security classification level if appropriate.</i></p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>5. Is the work area kept free of substances that will damage the equipment or stored information?</p> <p><i>General rule: Dust, food, beverages, and magnetic or electrostatic sources should be removed or barred from equipment and the computer work area.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>6. Are file backups regularly made?</p> <p><i>General rule: To ensure retention of electronic data in the event of electricity failures or power surges, backups should be made on a regular schedule (generally daily) and when thunderstorms are anticipated</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>7. Can you identify and do you keep the documentation necessary to understand and use your electronic records?</p> <p><i>General rule: To utilize records stored in electronic formats, the documentation that explains the electronic system is needed.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>8. Are permanent or unscheduled electronic records kept under proper storage conditions?</p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>9. Are permanent records transferred to the National Archives at the earliest feasible time?</p> <p><i>General rule: Permanent or unscheduled electronic records should be kept on magnetic tape, stored under proper temperature/humidity conditions, rewound at specified times, and scheduled or placed in archival custody as soon as possible to prevent information loss.</i></p>
G. TECHNICAL REFERENCE		
<input type="checkbox"/>	<input type="checkbox"/>	<p>1. Are technical reference materials (which are nonrecord) identified and kept separately from record material?</p> <p><i>General rule: These publications are not government records and should not be confused with official files.</i></p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>2. Is shelf storage used for these materials whenever possible and filing cabinet storage kept to a minimum?</p> <p><i>General rule: Shelf storage is less expensive and allows staff easy access.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>3. Are publishers requested to stop sending materials that are no longer needed?</p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. Are reference materials periodically (at least annually) reviewed and purged of all superseded/obsolete items?</p> <p><i>General rule: Valuable office furniture should not be used for unneeded material whose retention prevents quick access to needed information.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>5. Has an arrangement pattern been developed that best meets user needs?</p> <p><i>General rule: The pattern should reflect the workflow of the organization</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>6. Has the need for an index been evaluated?</p> <p><i>General rule: An index should be developed only if reference materials are extensive and used often and cannot be physically arranged to satisfy user needs. The time required to maintain the index should be less than that needed to search for material without it.</i></p>
H. DAILY FILING		
<input type="checkbox"/>	<input type="checkbox"/>	<p>1. Are files kept up to date?</p> <p><i>General rule: The most recently received papers are those most frequently requested and should be filed on a daily basis for easy finding.</i></p>

YES	NO	Description
<input type="checkbox"/>	<input type="checkbox"/>	<p>2. Is a "profile check" performed to assure that each item belongs in the files, papers are complete, and file authority is present?</p> <p><i>General rule: ff the file authority is absent, it is possible that necessary staff action has not been taken. The check for completeness prevents loss of essential record material.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>3. Are documents properly assembled, sorted, and classified before filing begins?</p> <p><i>General rule: Taking a stack of unorganized papers to the file cabinets wastes effort and time. Related records, such as incoming and outgoing correspondence, should be stapled together</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>4. When needed, are cross-references made to extra or photo duplicated copies?</p> <p><i>General rule: Cross-references should be limited to subjects proven by experience to need them. Copies are easier and cheaper to make than completed cross-reference forms.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>5. Are file drawers and folders adequately labeled to allow for quick reference?</p> <p><i>General rule: Drawer, guide card, and folder labels should be standardized and easy to read.</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	<p>6. Are file labels aligned and colored labels used in a consistent manner to aid finding?</p> <p><i>General rule: Simple arrangements and color coding by period of time, value, and type of record speeds the filing and finding of records.</i></p>

YES	NO	Description	
<input type="checkbox"/>	<input type="checkbox"/>	7.	<p>Are files kept upright in the drawers and new folders made when they become 3/4 inch thick?</p> <p><i>General rule: Individual folders hold no more than 75 to 100 sheets. Labels should be kept visible to make finding files easier</i></p>
<input type="checkbox"/>	<input type="checkbox"/>	8.	<p>Is access to files limited to authorized personnel, and is a charge-out procedure enforced for all office files?</p> <p>General rule: Minimum access to the files and strict charge-out rules protect the office from expensive misfiles and loss of important records.</p>
<input type="checkbox"/>	<input type="checkbox"/>	9.	<p>Are periodic checks made for misfiles?</p> <p><i>General rule: Misfiles are expensive in terms of staff time and lost records. Files should be checked once or twice a year for misfiles. Be alert for misfiles during daily filing, and refile them in their proper locations.</i></p>

Appendix G

CLASSIFICATION OUTLINE

This appendix provides an outline of the subjects contained in OSHA Instruction ADM 12-0.1 covering the subject classification scheme used to provide structure to the OSHA directives system and provide a framework for the filing of OSHA records.

<p>ADM ADMINISTRATIVE MANAGEMENT</p> <ul style="list-style-type: none"> 1 Automation and Mechanization <ul style="list-style-type: none"> 1-1 Management Information Systems (MIS) 1-2 Word Processing 2 Awards and Incentives <ul style="list-style-type: none"> 2-1 Awards Committee 2-2 Cash Awards and Commendations 2-3 Honor Awards 2-4 Suggestion Program 3 Communications Management <ul style="list-style-type: none"> 3-1 Communications Control 3-2 Handbooks 3-3 Letters and Memoranda 3-4 Mail Service 3-5 Messenger Service 3-6 Security 3-7 Telecommunications 3-8 Translation Service 4 Delegation of Authority <ul style="list-style-type: none"> 4-1 Signature 5 Emergency Planning <ul style="list-style-type: none"> 5-1 Civil Defense 5-2 Continuity of Government 5-3 Operation Alerts 5-4 Relocation Sites 6 Employee Services and Activities 7 Forms Management 8 Issuance Management <ul style="list-style-type: none"> *8-1 Directives System *8-2 Subscription Service 9 Management Improvement Program 10 Manpower Utilization 11 Organization and Functions <ul style="list-style-type: none"> 11-1 Department 11-2 Field Facilities 11-3 Other Government Agencies 12 Records Management <ul style="list-style-type: none"> 12-1 Filing Equipment and Supplies 12-2 Maintenance 	<ul style="list-style-type: none"> 12-3 Manuals 12-4 Microfilm 12-5 Preservation of Essential Records 12-6 Records Control Schedules 12-7 Records Disposition 12-8 Records Inventories 12-9 Safeguarding Information 13 Surveys and Inspections 14 Work Measurement and Simplification <p>ADC ADVISORY COMMITTEES</p> <ul style="list-style-type: none"> 1 National Advisory Committee on Occupational Safety and Health 2 Advisory Committee on Construction Safety and Health <p>BUD BUDGET</p> <ul style="list-style-type: none"> 1 Annual; Budget Submission <ul style="list-style-type: none"> 1-1 Review and Revision 2 Office of Management and Budget (OMB) <ul style="list-style-type: none"> 2-1 OMB Bulletins 2-2 OMB Circulars 2-3 OMB Hearings 3 Congressional Hearings 4 Funding Plan <ul style="list-style-type: none"> 4-1 Allotments 4-2 Apportionment 4-3 Personnel Ceilings 4-4 Utilization of Funds <p>COM COMMITTEES, ORGANIZATIONS, AND MEETINGS</p> <ul style="list-style-type: none"> 1 Department 2 Interagency 3 International 4 Others <p>CPL COMPLIANCE</p> <ul style="list-style-type: none"> 1 Accreditation of Testing Laboratories
--	---

2	Inspection	8-5	Fees
	2-1 Safety	8-6	Field
	2-2 Health	8-7	Inter-Office Transfers
3	Hearings	8-8	Performance Bonds
	3-1 Administrative	8-9	Rents
	3-2 Investigational	8-10	Reports
4	Litigation	8-11	Schedules
5	Voluntary Compliance Programs	8-12	Summaries
		9	Discounts
DIS	DISCRIMINATION	10	Disbursements
	*1 Complaints	10-1	Accounts Payable
	*2 11 [©] Case Files	10-2	Adjustments
		10-3	Advices
FAP	FEDERAL AGENCY PROGRAMS	10-4	Disbursing Office Cash
	1 Compliance	10-5	Expenditures
	1-1 Complaints	10-6	Petty Purchases
	1-2 Fatalities and Catastrophes	10-7	Refunds
		10-8	Reports
	2 Evaluations	10-9	Schedules
		10-10	Summaries
	3 Consultation	11	Entertainment Fund
FIN	FINANCIAL MANAGEMENT	12	Interest
	1 Accounts Current	13	Irregularities
		14	Ledgers
	2 Allowances-Expense Accounts	14-1	Allotment
		14-2	Cash
	3 Audits	15	Liquidation of Accounts
	3-1 Claims and Inquiries	16	Obligations and Encumbrances
	3-2 GAO Exceptions	17	Payrolls-Salaries
	3-3 Internal	17-1	Bond Deductions or Distribution
	3-4 Suspensions and Disallowances	17-2	Checks (Salary)
		17-3	Government Life Insurance
	4 Authorizations	17-4	Government Medical and Hospital Insurance
	4-1 Agents to Receive Checks	17-5	Powers of Attorney
	4-2 Collection Officers or Agent Cashiers	17-6	Retirement Deductions
	4-3 Delegations of Authority	17-7	Social Security
		17-8	Time and Attendance Reports
	5 Contracts	17-9	Vouchers
		17-10	Withholding Taxes, Federal
	6 Obligations and Liquidations	17-11	Withholding Taxes, State
		18	Reconciliations
	7 Bonding of Employees	18-1	Cash
		18-2	Closing Schedules, FY
	8 Collections-Receipts		
	8-1 Accounts Receivable		
	8-2 Adjustments		
	8-3 Checks		
	8-4 Deposits		

19	Reports and Statistics	6-3	Reports (GSA)
20	Systems of Accounting	7	Stenographic Services
21	Vouchers-Invoices	PER	PERSONNEL
22	Working Capital Fund	1	Attendance and Leave
		1-1	Hours of Work
		1-2	Leave Records
LEG	LEGISLATIVE AND LEGAL		
1	Claims and Litigations	2	Compensation
2	Congressional Relations	3	Conduct and Discipline
	2-1 Congressional Committees	3-1	Disciplinary Action
3	Executive Orders and Proclamations	4	Employee-Management Relations (LMR)
4	Legislation	5	Employment
5	Opinions and decisions	5-1	Accessions
		5-2	Applications
		5-3	Consultants and Experts
		5-4	Examinations
		5-5	Fair Employment Practices
		5-6	Merit Staffing Plan
		5-7	Placement
		5-8	Recruitment
		5-9	Reduction in Force
6	Patents, Copyrights, and Trademarks		
7	Seals		
OFF	OFFICE SERVICES		
1	Building Service		
	1-1 Construction	6	Evaluation
	1-2 Directories		
	1-3 Lost or Stolen Property	7	Excepted Positions
	1-4 Maintenance and Repair		
	1-5 Parking	8	Health
	1-6 Passes	8-1	Accidents
	1-7 Protection	8-2	Medical Examinations and Care
	1-8 Safety		
	1-9 Telephone	9	Insurance
	1-10 Utilities	9-1	Federal Employees Health Benefits Plans
		9-2	Government Life Insurance
2	Cafeteria		
3	Library Services	10	Orientation and Training
	3-1 Cataloging	10-1	Employee Development
	3-2 Circulation	10-2	Intern Program
	3-3 Interlibrary Loans	10-3	Orientation
	3-4 Research		
4	Motor Pool	11	Position Classification
	4-1 Accidents	11-1	Position Descriptions
	4-2 Dispatching and Scheduling	11-2	Job Series and Standards
	4-3 Maintenance		
	4-4 Use of government-owned Vehicles	12	Retirement
5	Reproduction and Distribution	13	Security
	5-1 Distribution Lists	14	Separation
	5-2 Field Printing	15	Veterans
	5-3 Graphic and Visual		
	5-4 Processes and Methods	PRO	PROCUREMENT
	5-5 Requisitions	1	Bids and Contracts
6	Space	2	Catalogs
	6-1 Leases		
	6-2 Office		

3	Equipment and Supplies	11	Visitors
4	Property Accountability	REP	REPORTS AND STATISTICS
4-1	Equipment Inventory	1	Recurring Reports
4-2	Supply Inventory	1-1	Annual
5	Storage and Warehousing	1-2	Monthly
6	Surplus Property	1-3	Quarterly
6-1	Acquisition	1-4	Weekly
6-2	Boards of Surveys	2	Reports Management and Control
6-3	Disposal	2-1	Clearance
PBM	PROGRAM BUDGET MANAGEMENT	2-2	Discontinuances and Revision
1	Plans and Policy	2-3	Instructions
2	Execution Schedules	3	Statistics and Statistical Reporting
3	Program Objectives	3-1	Charts, Graphs, and Tables
4	Review and Analysis	3-2	Instructions and Procedures
PAE	PROGRAM OPERATIONS, ANALYSIS, AND EVALUATION	RSH	RESEARCH AND RELATED ACTIVITIES
1	Field Operations Plan	1	Administration
2	Audit Programs	2	Certification
2-1	National Audit Programs	3	Evaluations
2-2	Regional Audit Programs	4	Grants
2-3	Area Self Audit Programs	RVC	REVIEW COMMISSION
3	Field Performance analysis Evaluation Items	RUL	RULEMAKING
4	Special Reviews and Analyses	STD	STANDARDS
5	Program and Policy Evaluation	1	General Industry
PUB	PUBLIC INFORMATION	1-1	Walking-Working Surfaces
1	Anonymous and Crank Letters	1-2	Means of Egress
2	Biographies	1-3	Powered Platforms, Manlifts, and Vehicle-mounted Work Platforms
3	Commendations	1-4	Occupational Health and Environmental Controls
4	Criticisms	1-5	Hazardous Materials
5	Exhibits	1-6	Personal Protective Equipment
6	Motion Pictures	1-7	General Environmental Controls
7	Press, Radio, and Television	1-8	Medical and First Aid
8	Publications	1-9	Fire Protection
8-1	Technical Information	1-10	Compressed Gas and Compressed Air Equipment
9	Requests	1-11	Materials Handling and Storage
10	Speeches	1-12	Machinery and Machine Guarding
		1-13	Hand and Portable Powered Tools and Other Hand-Held Equipment
		1-14	Welding, Cutting, and Brazing
		1-15	Special Industries
		1-16	Electrical
		1-17	Commercial Diving Operation
			(1-18 through 1-22 Reserved)
		1-23	Toxic and Hazardous Substances

2	Maritime	2	Plans
2-1	Longshoring	2-1	Procedures
2-2	Shipbreaking	2-2	Provisions
2-3	Shipbuilding	2-3	Grants
2-4	Ship Repairing	2-4	Evaluation and Monitoring
2-5	Gear Certification		
		TNR	TECHNICAL AND REGULATORY ANALYSIS
3	Construction	*1	Impact Statements
3-1	General Safety and Health Provisions	*2	Studies
3-2	Occupational Health and Environmental Controls	*3	Regulatory Calendar for Standards Development
3-3	Personal Protective and Life Saving Equipment		
3-4	Fire Protection and Prevention	TED	TRAINING AND EDUCATION
3-5	Signs, Signals, and Barricades	1	OSHA Personnel
3-6	Materials Handling, Storage, Use, and Disposal	2	State Personnel
3-7	Tools-Hand and Power	3	Consultation
3-8	Welding and Cutting	4	Small Business
3-9	Electrical	5	Labor Liaison
3-10	Ladders and Scaffolding	6	Grant Monitoring
3-11	Floors and Wall Openings, and Stairways	7	Federal Personnel
3-12	Cranes, Derricks, Hoists, Elevators, and Conveyors		
3-13	Motor Vehicles, Mechanized Equipment, and Marine Operations	TRA	TRAVEL AND TRANSPORTATION
3-14	Excavations, Trenching, and Shoring	1	Allowances
3-15	Concrete, Concrete Forms, and Shoring	1-1	Advances
3-16	Steel Erection	2	Authorization
3-17	Tunnels and Shafts, Caissons, Cofferdams, and Compressed Air	3	Carriers
3-18	Demolition	3-1	Air
3-19	Blasting and Use of Explosives	3-2	Local Transportation
3-20	Power Transmission and Distribution	3-3	Surface
3-21	Rollover Protective Structures; Overhead Protection	3-4	Tokens, Tickets, and Passes
4	Agriculture	4	Passports
5	Other Facilities	4-1	Visas
6	Variances and Other Relief	5	Transportation
*6-1	Policy and Procedures	5-1	Bills of Lading
*6-2	Status Reports	5-2	Claims
*6-3	Inspection and Enforcement	5-3	Personal and Household Effects
7	Coverage	5-4	Rates and Tariffs
8	Standard Interpretation	5-5	Routings
STP	STATE PROGRAMS		
1	Agreements		

INDEX

Certification	G-4, G-5
Classified Material	1-1, 2-1, 2-2, 7-2, 9-1
Conversion	5-5, 5-11, 7-1, 7-2, D-2
Cross-reference	4-1, 5-2, 7-6
Directory	5-3-5-7, C-2
Diskettes	5-1, 5-11, 5-12, C-1, C-3
Electronic Directories	C-3
Electronic File	2-3
File Category	B-2
File Coding	4-2
File Equipment	9-2
Filing Arrangement	8-2
Filing Equipment	10-2, 10-3, G-1
Justification	8-1
Mailing Lists	7-5
Marking	9-1
Privacy Act Material	1-8
Projects	3-3, 3-4, B-11
Reading File	4-1, 4-2, 7-6
Responsibilities	1-1, 1-5, 3-4, 10-2
Safeguard	1-8, 9-2
Security of Electronic Records	5-11
Stenographic Notes	7-7
Subdivision	B-11
Subject File	2-2, 4-2, A-4, B-14
Subject-expansion	B-14
Supplemental Records Listing	8-4, 8-5
System Revisions	1-4
Temporary Files	B-15
Tickler File	2-3
Transfer of Records	7-2, 7-3, 10-2, B-13
Transmittal Sheets	7-7
Work Papers	7-7