U.S. Customs and Border Protection

# HB 2100-05B
# Records and Information Management Handbook

Version 1.0

June 3, 2019

# FOREWORD

## U.S. Customs and Border Protection
## Records and Information Management Handbook

I am pleased to bring you the U.S. Customs and Border Protection (CBP) Records and Information Management Handbook. This handbook along with the accompanying CBP Records and Information Management Directive provide the comprehensive policy documents for the CBP Records and Information Management (RIM) Program.

This Handbook builds on the previous Customs handbook and includes: Federal Records Act updates; alignment to DHS and CBP policy; enhanced instructions for electronic records; and expanded and clarified roles and responsibilities, off-boarding requirements, and annual/triennial RIM evaluations.

CBP and all other federal agencies are required by 44 U.S.C. 3101 and 36 C.F.R. 1220.30 to maintain and provide adequate and proper documentation of Government business – their organization, functions, policies, decisions, procedures, and essential transactions. In addition, federal agencies are required to ensure that all information necessary to protect the legal and financial rights of the Government, and of persons directly affected by the agency's activities, is properly created, maintained, and preserved.

Information is a key CBP strategic resource and records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records and information can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government. Records protect the rights and interests of people and hold officials accountable for their actions. Permanent records document our Nation's history.

Information is a perishable asset and must be managed. It is also expensive to create and maintain. We must plan for, organize, protect, share, and preserve our information more effectively. The information explosion and advances in technology have changed the way we do business. Effective records and information management is an essential component of cost-efficient management.

The *CBP Records and Information Management Handbook* (herein, "*Handbook*") provides the necessary guidance to manage and operate a RIM Program. The *Handbook* supersedes the *Interim Records Handbook* HB 2100-05A, issued April 19, 2001.

John Sanders

John P. Sanders
Chief Operating Officer and Senior Official
Performing the Functions and Duties of the Commissioner
U.S. Customs and Border Protection

## Contents

# Part 1: Introduction and Background

Information is a key CBP strategic resource. We are only as effective as the security, accuracy, timeliness, and availability of information we need to do our best work and make optimal, fact-based decisions.

Use of information technology continues to alter CBP work processes, change the nature of our workplace and activities, and significantly influence use of information as a strategic and valuable mission resource. At the same time, CBP continues to generate and manage paper materials.

These dynamics create complexities that require governance in order to achieve the optimal balance of control and agility.

All CBP employees and contractors have specific record keeping and information management responsibilities. This Handbook provides the following instructions:

- Processing, maintaining, preserving, and destroying records in accordance with the federal guidelines described below in Section B.
- Managing data and information not covered by the Federal Records Act, but subject to Freedom of Information Act (FOIA) disclosure and discovery in litigation.

Governance of all information is an integral part of CBP's mission environment and mission support infrastructure. Planning and resourcing decisions must be driven by clearly understood mission and business processes, consistent decision criteria, and well defined information uses and services. CBP will make improvements in mission performance and service delivery through its strategic use of information, application of technology, and governance of its information assets.

| RIM Directive Policy #: | Part 2-C: CBP Policy Statements | Reference |
|---|---|---|
| 2.10 | This Directive, the RIM Handbook, and the RIM Strategic Plan are reviewed and updated as appropriate every three (3) years. | 36 CFR §1220.34 |

## A. Scope and Applicability of Handbook

This Handbook covers records and information management objectives, instructions, and responsibilities. It includes guidance on:

- Lifecycle (creation, use, and disposition) of specific categories of federal records and information;
- Special issues with respect to electronic records, data, and information, including email and electronic messaging;
- Records and information requirements for departing employees and political appointees; and
- Records and information management training.

This handbook does not address the circumstances in which documents may need to be preserved for litigation; this guidance will be provided by Office of the Chief Counsel (OCC). All personnel are required to comply with OCC's guidance on litigation preservation.

This Handbook applies to all CBP employees and contractors doing business for CBP.

## B. Annotated Legislative and Regulatory References and Other Executive Branch Guidance

The following descriptions summarize the key legislative, regulatory, and directive references that apply to CBP RIM. Appendix 4 provides additional detailed references.

**The Federal Records Act** (as codified at **44 U.S.C. Chapters 29, 31, and 33**), updated on November 26, 2014, requires agencies to:

- Make and preserve records containing adequate and proper documentation of their organization, functions, policies, decisions, procedures, and essential transactions; and requires CBP to furnish the information necessary to protect the legal and financial rights of the government and of persons directly affected by CBP activities.
- Establish and maintain a program for the efficient management and governance of records. Records and information management programs provide schedules for the disposal of records with approval of the Archivist of the United States.
- Prevent officers and employees of the executive branch from using personal email accounts for government business, unless the employee copies all emails to either the originating officer or employee's government email, or to an official government record system to be recorded and archived.

**Title 36 C.F.R. Chapter XII, Subchapter B - Records Management** details regulations for federal agencies' records management programs relating to proper records creation and maintenance, adequate documentation, and records disposition.

**The Paperwork Reduction Act of 1995** (**44 U.S.C. 3506(f)**), with respect to records management, requires CBP to implement and enforce applicable policies, including requirements for archiving information maintained in electronic format, particularly in the planning, design, and operation of information systems.

**Title 18 U.S.C. 2071** establishes criminal penalties for the unlawful removal or destruction of federal records.

**Title 18 U.S.C. 793, 794, and 798** establishes criminal penalties for unlawful disclosure of certain information pertaining to national security.

**Office of Management and Budget (OMB) Circular A-130: Managing Information as a Strategic Resource** (updated 27 July 2016) implements the Paperwork Reduction Act and:

- Provides guidance for integration of records and information management with other information resources management disciplines.
- Reaffirms that records include information in any form and that CBP must ensure records management programs provide:
  - Adequate and proper documentation of CBP activities;
  - Access to records regardless of form or medium;
  - Approval for retention schedules for federal records from the Archivist; and

  - Training and guidance for CBP officials, employees, and contractors regarding their records and information management responsibilities.
- Requires agencies to incorporate records management and archival functions into the design, development, implementation, and decommissioning of information systems – especially internet resources such as storage solutions and cloud-based services (e.g., software as a service, platform as a service, and infrastructure as a service);
- Requires CBP to:
  - Manage electronic records in accordance with Government-wide requirements.  This includes:
    - Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by the National Archives and Records Administration (NARA) in an electronic format;
    - Managing all email records electronically and retaining them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed.
  - Ensure agency records are treated as information resources and follow the requirements in the Circular;
  - Ensure the proper and timely disposition of federal records in accordance with a retention schedule approved by the Archivist of the United States; and
  - Provide training and guidance, as appropriate, to all agency employees and contractors regarding their federal records management responsibilities.
- Emphasizes and clarifies the role of both privacy and security in the federal information lifecycle.
- Represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial components of a comprehensive, strategic, and continuous risk-based information management program.

**Executive Order (EO) 12958**, "Classified National Security Information", prescribes a uniform system for classifying, safeguarding, and declassifying national security information.  It promotes proper and effective classification and protection of official information in the interest of national security.  It also promotes the declassification of information no longer requiring such protection.

**The Freedom of Information Act (FOIA), 5 U.S.C. 552**, establishes procedures by which persons may access certain federal agency records, subject to certain exemptions from disclosure included in the law. The Electronic FOIA Amendments of 1996 (Pub. L. No. 104-231) emphasizes electronic access to records and requires agencies to provide copies of records in electronic form if they are readily reproducible in that form.

**The Privacy Act of 1974, 5 U.S.C. 552a**, mandates the agency requirements for the collection, use, maintenance, and dissemination of personal information under the control of the agency and retrievable by unique identifier.

**The Government Paperwork Elimination Act**, **44 U.S.C. Chapter 35**, as amended by Public Law 105-277, mandates that, when possible, federal agencies should use electronic forms, electronic filing, and electronic signatures to conduct official business with the public by 2003.

**Guidance on Managing Email OMB M-14-16** reminds federal agencies about their records management responsibilities regarding email and recommends agencies immediately begin to adopt automated or rules-based records management policies for email management.

## C. Responsibilities

All CBP employees are responsible for the processing and storage of records. CBP managers, supervisors, and records officers have the following specific responsibilities:

*CBP Commissioner:*[1]

- Implements the DHS Records and Information Management (RIM) Program within CBP (Delegated to CBP Chief Information Officer, Delegation Order 18-203);
- Designates a Chief Records Officer (CRO) for CBP with the responsibility for leading, overseeing, and implementing a CBP records program and ensures Records Custodians are identified for all records (Delegated to CBP Chief Information Officer, Delegation Order 18-203);
- Obtains CBP-specific records retention schedules (via the CRO) for all CBP records (Delegated to CBP Chief Information Officer, Delegation Order 18-203);
- Incorporates requirements for annual records training into contracts, as appropriate;
- Ensures all acquisitions and phases of the acquisition lifecycle incorporate records management requirements, to include coordination with the records program (Delegated to CBP Chief Information Officer, Delegation Order 18-203 and Directive 2130-019);
- Ensures CBP systems and programs are operating in compliance with the applicable privacy documentation and that privacy compliance documentation cites an accurate and appropriate NARA approved retention and disposal schedule (Delegated to CBP Chief Privacy Officer, Directive 2120-010);
- Reinforces the importance of records management at the leadership staff level through ongoing development training and ensures annual mandatory records management training is accomplished for all CBP employees (Delegated to CBP Chief Information Officer, Delegation Order 18-203);
- Ensures the identification, retention, and management of electronic and paper records (Delegated to CBP Chief Information Officer, Delegation Order 18-203); and
- Ensures records management is included in information technology systems acquired or developed within CBP (Delegated to CBP Chief Information Officer, Delegation Order 18-203 and Directive 2130-019).

*Assistant Commissioner, Office of Information and Technology (OIT), Chief Information Officer (CIO)*:

- Implements the DHS RIM program within CBP;
- Designates a CRO for CBP with the responsibility for leading, overseeing, and implementing a CBP records program and ensures Records Custodians are identified for all records;
- Obtains CBP-specific records retention schedules (via CRO) for all CBP records;
- Ensures all acquisitions and phases of the acquisition lifecycle incorporate records management requirements, to include coordination with the records program;
- Reinforces the importance of records management at the leadership staff level through ongoing

[1] These responsibilities are required by DHS Records and Information Management Directives and Instructions. The Commissioner may re-delegate these responsibilities as appropriate.

development training and ensures annual mandatory records management training is accomplished for all CBP employees;
- Ensures the identification, retention, and management of electronic and paper records;
- Ensures records management is included in information technology systems acquired or developed within CBP;
- Ensures preservation of material relevant to litigation holds;
- Establishes RIM policies, standards, and procedures to carry out program objectives; and
- Provides effective information technology and RIM practices, policies, and procedures to achieve the requirements of the Clinger-Cohen Act and other federal statutory and regulatory mandates.

*CBP Component Office Heads:*
- Appoint and oversee a senior-level Component Office RIM Accountable Executive;
- Oversee implementation of RIM policy, directives, and implementing guidance in respective Component Offices;
- Reinforce the importance of and advocate for RIM with Component Office staff; and
- Ensure protocols and procedures for safekeeping of and access to Component Office-specific essential/vital records, files, and databases.

*CBP Chief Records Officer (CRO):*
- Serves as the Agency Records Officer and leads the CBP RIM program;
- Proposes policy and directives and develops implementing guidance for management of CBP records, data, and information;
- Participates in the CBP Information Governance Board;
- Ensures periodic evaluations of Component Office records management programs to determine compliance with federal records regulations and reports their findings to CBP Commissioner, Component Offices, and CIO;
- Ensures annual reviews of CBP essential/vital records to confirm they are properly maintained and updated;
- Coordinates records management policy matters with NARA and the General Services Administration (GSA);
- Provides leadership and guidance to RIM Accountable Executives (RAEs), the RAE Council, Local Records and Information Managers (LRIMs), and the Records Management Working Group (RMWG) to ensure reasonable uniformity in RIM activities throughout CBP;
- Establishes recordkeeping requirements and ensures they are implemented in new or revised programs, processes, procedures, and automated systems;
- Establishes procedures to ensure officials, employees, and contractors do not remove records from CBP custody without written and appropriate authorization;
- Directs development and maintenance of Records Control Schedules (RCS) for all CBP records and reviews and updates those schedules as necessary;
- Ensures CBP personnel maintain a uniform file plan system;
- Ensures identification, retention, and management of electronic, paper, and essential/vital records;
- Ensures CBP records management procedures include guidance for identifying and managing essential/vital records;
- Ensures CBP records policy and guidance are aligned to the DHS records management policy

and requirements;

- Coordinates with RAEs to ensure all CBP personnel, including Program Managers, appropriately manage the records they create or receive in conducting DHS business;
- Ensures that relevant documents are preserved for purposes of discovery, including compliance with any obligations imposed by the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and any applicable judicial rules or DHS or CBP policies, as communicated by OCC;
- Ensures all CBP employees receive necessary records management training including annual records management training; and
- Notifies DHS RIM Program Office and NARA when aware of any actual, imminent, or threatened unlawful removal, defacing, alteration, or destruction of records (including electronic or machine-readable records) in CBP's custody.

CBP Privacy Officer, Privacy and Diversity Office (PDO):

- Ensures CBP systems and programs are operating in compliance with the applicable privacy documentation and that privacy compliance documentation cites an accurate and appropriate NARA approved retention and disposal schedule;
- Is responsible for ensuring that all uses of personally identifiable information (PII) are consistent with law and Departmental policy;
- Sets the policies and procedures for PII collection, use, maintenance, and dissemination within CBP;
- Ensures that proposed record schedules are consistent with published System of Records Notices (SORN) pursuant to the Privacy Act, and updates SORNs as appropriate;
- Ensures that the Agency maintains the minimum amount of PII necessary to accomplish authorized Agency purposes;
- Reviews all information sharing access arrangement for PII to mitigate risk and ensure safe handling requirements;
- Reviews all Information Collections pursuant to the Paperwork Reduction Act for PII implications and compliance requirements;
- Conducts Privacy Threshold Analyses (PTAs) on all information technology systems as part of the security authorization package;
- Manages all privacy incidents and remediates unauthorized disclosures of PII; and
- Participates in the CBP Information Governance Board.

*Chief Counsel, Office of the Chief Counsel (OCC):*

- Issues specific guidance to address CBP litigation matters including but not limited to preservation of material relevant to litigation holds;
- Provides legal advice as requested on issues related to document preservation.

*Records Management Working Group (RMWG)*:

- Provides CRO recommendations on records management requirements, standards, and practices based on Component Office business needs;
- Is the formal dissemination vehicle for updated records management statute, regulation, and policy;
- Is managed and led by the CBP CRO;
- Members include LRIMs and other authorized representatives from all Component Offices.

*Managers, and supervisors at all levels,* for their respective offices and sub-offices, must:

- Know their records and information management responsibilities;
- Implement an approved records, data, and information disposition program;
- Develop internal implementing processes and procedures;
- Encourage adherence to, and periodically remind employees of RIM responsibilities and hold them accountable to discharge those responsibilities;
- Review and properly dispose of non-records, data, and information when no longer needed for CBP business purposes;
- Review RIM processes and their office's records periodically.  Provide timely compliance feedback to employees;
- Remind all employees annually of CBP RIM policies and sanctions provided for unlawful removal or destruction of federal records;
- Ensure any non-record, data, and information material being removed by a separating or transferring employee is reviewed and authorized by a CBP reviewing official (or a designee).
- Ensure RIM training is included in the on-boarding process and that all new employees and contractors understand and commit to following RIM policies and practices including those in this handbook.

*The Records and Information Management (RIM) Accountable Executive (RAE*) is the Component Office RIM Compliance Accountable Official and decision-making POC for RIM issues.  The RAE:

- Leads and oversees Component Office Records and Information Management and serves as the authorizing RIM official ensuring CBP and NARA records management policies and guidelines are applied and incorporated into day-to-day activities and business processes;
- Provides or ensures provision of funding and personnel necessary to support compliant Component Office RIM processes and practices;
- Ensures compliance with federal records statute and regulation and approves the annual internal RIM evaluation report;
- Reports compliance and progress regularly to Component Office Leadership and RIM Office;
- Ensures Local Records and Information Managers (LRIM) and RIM Custodians are appointed, trained, and allocated sufficient time to perform their required RIM duties;
- Leads Component LRIMs and RIM Custodians and holds them accountable, ensuring all records management tasks are completed accurately and timely;
- Learns about RIM and stays current on changes and trends;
- Contributes to RAE Council and attends monthly meetings;
- Advocates for Records and Information Management.

*Local Records and Information Managers (LRIM) under RAE direction*:

- Serve as implementing records points of contact for their Component Office and as extensions of the CRO;
- Coordinate Component Office RIM activities on behalf of CBP RIM, whether at headquarters or in the field;
- Promote and advocate CBP RIM in Component Office and CBP RIM community;
- Participate in the RMWG;

- Build and strengthen Component Office Records Custodians;
- Ensure and report to CRO that Component Office is appropriately staffed with Records Custodians and that they are trained and effectively functioning;
- Ensure Component Office recordkeeping requirements are established, implemented, and regularly updated including systematically updating all program directives and handbooks, for all subcomponent offices at all levels and for all record media, including electronic and other special records;
- Ensure each Component Office subcomponent creates and maintains records documenting its programs, electronic information systems, business processes, and administrative activities;
- Work with Records Custodians to ensure all records of each subcomponent/office are listed in office file plan and are described accurately in CBP's records schedules and all essential/vital records are identified;
- Coordinate changes to Component Office records schedule and file plans with CBP RIM at: [redacted] (b) (7)(E)
- Coordinate matters relating to RIM with system administrators and program managers, and with program managers responsible for special media such as audiovisual, cartographic, architectural, and printed records;
- Work with Records Custodians to ensure transfer of eligible records to a Federal Records Center (FRC), prompt disposal of temporary records when retention period expires, and timely transfer of permanent records to NARA;
- Conduct annual Component Office RIM internal evaluation including essential/vital records; and
- Brief senior managers and leadership regularly on RIM status and progress.

*Records Custodians:*

- Work with managers and supervisors to ensure RIM is established within the unit and all staff is applying policies and practices to safeguard all records in all media (paper and electronic);
- Work with LRIMs to identify, schedule, preserve, and properly dispose of records including informing LRIMs of unauthorized disposals;
- Work with LRIMs to ensure all records of each subcomponent/office are listed in office file plan and are described accurately in CBP's records schedules and all essential/vital records are identified;
- Follow CBP and Component Office file plan to ensure proper disposition of records including:
  - Systematic file cutoffs (breaks);
  - Retirement of eligible records to an approved records storage center;
  - Litigation holds upon Chief Counsel notification; and
  - Timely transfer of permanent records to NARA;
- Assist program managers to regularly remind staff not to mix personal papers and non-record materials with federal records, and not to remove records from CBP without proper authorization;
- Assist program managers to implement procedures preventing separating executives and employees from destroying ineligible records or removing records from CBP's custody;
- Cooperate with LRIM and CBP CRO in periodic evaluations of Component Office records; and
- Work with managers and supervisors to ensure RIM training is included in the on-boarding process and that all new employees and contractors understand and commit to following RIM policies and practices.

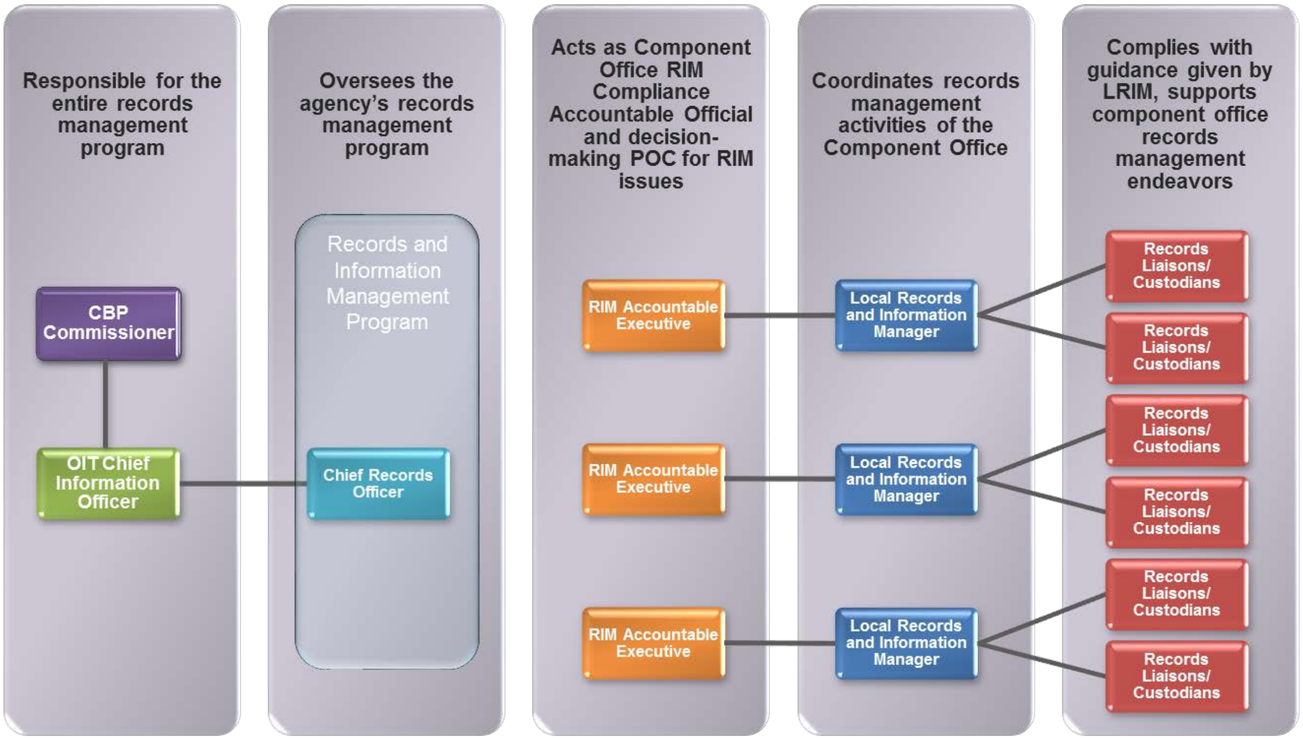
*Program Managers and Process Owners:*

- Serve as records management program officials who have primary responsibility for creating, maintaining, using, protecting, and disposing of records in their programs or processes;
- Create systems of records needed to ensure adequate and proper documentation of business process transactions in their area of responsibility;
- Ensure program or process records are listed in their Component Office file plan and accurately described;
- Implement procedures to ensure records are protected from loss, theft, and unauthorized access;
- Establish filing systems and work with LRIM and Custodians to implement procedures to ensure records are maintained in such a manner that information and documents are readily retrievable;
- Conduct an annual review of their specific program or process records to ensure timely transfer of eligible records to an FRC, prompt disposal of temporary records when retention expires and timely transfer of permanent records to NARA, coordinating with and reporting findings and recommendations to Component Office LRIM or Custodian;
- Ensures identification, retention, management, and currency of program and process essential/vital records;
- Notify LRIM or Custodian of organization, program, or process changes that result in creation of new record types, transfer or termination of records no longer required, or a business need to change a record retention period; and
- Incorporate mandatory records management training for all DHS contractors when contractors handle, review, or process DHS records.

*CBP Employees and Contractors*:

- Understand they are responsible for creating, organizing, maintaining, using, protecting, and properly disposing of records, data, and information within their program areas as described in this Handbook;
- **Understand these tasks are not optional, but are an integral part of their job requirements;**
- Adequately and properly document transactions of government business;
- Properly identify, manage, and maintain essential/vital records consistent with Component Office CoOP Implementation Plan;
- Learn and follow all records and information policies and practices;
- Complete records management training annually;
- Coordinate records management activities with their LRIMs and Custodians to ensure compliance with applicable policies and procedures;
- When teleworking, identify, safeguard, and manage all records in accordance with records management policies;
- Do not remove federal records from CBP custody without prior approval, nor destroy records unless there is an approved records schedule that authorizes destruction and that destruction has been authorized by the cognizant supervisor;
- Transfer, upon their separation, all government records and information, to either their supervisor, an appropriate agency recordkeeping system, or another employee assuming their duties; and
- Ensure and certify all relevant records and information are accounted for and available for reference and use after their departure. Note: Electronic materials may be stored on a desktop, laptop, thumb drive, or share drive locally or in the cloud.

*Figure 1: RIM Program Structure*


Responsible for the entire records management program
Oversees the agency's records management program
Acts as Component Office RIM Compliance Accountable Official and decision-making POC for RIM issues
Coordinates records management activities of the Component Office
Complies with guidance given by LRIM, supports component office records management endeavors
CBP Commissioner
OIT Chief Information Officer
Records and Information Management Program
Chief Records Officer
RIM Accountable Executive
RIM Accountable Executive
RIM Accountable Executive
Local Records and Information Manager
Local Records and Information Manager
Local Records and Information Manager
Records Liaisons/ Custodians
Records Liaisons/ Custodians
Records Liaisons/ Custodians
Records Liaisons/ Custodians
Records Liaisons/ Custodians
Records Liaisons/ Custodians

# Part 2: Records and Information Management Program

## A. Records and Information Management Concepts

The Federal Records Act (as codified at 44 U.S.C. Chapters 29, 31, and 33) requires CBP and CBP employees and contractors to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions. 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, the Federal Records Act requires agencies to establish and maintain a program for the efficient management of records and information. Records and information programs must, among other provisions, provide for schedules proposing disposal of records for approval by the Archivist of the United States.

Records are the memory of CBP and, as such, must be properly managed to ensure that valuable information is available to support current operations, litigation, fact-based decisions, historical research, and analytics. This goal is attainable only through continuous, systematic, and effective controls over creation or receipt, maintenance, use, repurposing, and disposition of records consistent with an established RIM Program. The following are essential RIM program objectives:

- Efficient management of capture and creation of records;
- Promotion of effective files maintenance practices;
- Preservation of records of continuing value and transfer of them to NARA at the appropriate time as indicated in the RCSs;
- Removal of noncurrent records from office space, filing equipment, and data storage areas to less expensive storage facilities; and
- Destruction of records of temporary value as soon as they have served the purpose for which they were created; and
- All CBP records are scheduled, regardless of form or media.

**Records Management Control:** CBP is required to establish and maintain an active, continuing program for the economical and efficient management of the records of the Agency (44 U.S.C. 3102). The program, at a minimum, will provide for:

- Effective controls over records in the conduct of current business; and
- Cooperation with the GSA and the Archivist of the United States in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value.

| RIM Directive Policy #: | Part 2-A: CBP Policy Statements | Reference |
|---|---|---|
| 2 | It is CBP policy to create, preserve, maintain, use, ensure access to, and dispose of federal records, data, and information, including electronic messaging, wherever that material resides, in compliance with requirements of the Federal Records Act, OMB Circulars and Directives, applicable NARA regulations, | 36 C.F.R. §1220.32 |

| | | |
|---|---|---|
| | and DHS policy, and the Rules of Civil and Criminal Procedure. | |
| 2.1.1 | Each Component Office shall "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and 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." (44 U.S.C. 3101) | 44 U.S.C. §3101 |
| 2.1.3 | Each Component Office may also have separate and additional obligations to preserve information relevant to litigation. Each Component Office shall comply with all litigation holds, court rules, and other rules and policies as well as any guidance provided by Office of the Chief Counsel (OCC) related to preservation of information. | |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(A) | Create, receive, and maintain official records providing adequate and proper documentation in support of DHS activities (Title 44 U.S.C. Section 3301). | 44, U.S.C. § 3301 |
| Directive 141-01(V)(B) | Ensure all records are properly maintained in all programs, projects, and administration efforts. | |
| Instruction 141-01-001(VI)(A) | Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business and preserved or are appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in the records | 44, U.S.C. § 3301 |
| Instruction 141-01-001 (VI)(B) | Records, regardless of media or phase of creation stage (records lifecycle) are properly identified, captured, retained, filed, and disposed of or transferred in accordance with Title 44 U.S.C. Chapter 31; NARA regulations, 36 CFR, Chapter XII, Subpart B; and DHS records policy. | |

## B. Definitions

Acronyms are defined in Appendix 8. The following definitions include records management terms extracted from 36 C.F.R. Part 1220.

**Administrative records**: Records that reflect routine, transitory, and internal housekeeping activities relating to subjects and functions common to all offices. Examples include training, personnel, and travel reimbursement files. Administrative records, in conjunction with program records, comprise the universe of agency records.

**Annual internal evaluation**: Formal evaluation that measures the effectiveness of records management programs and practices, and ensures compliance with NARA regulations on an annual basis.

**Business transaction**: As used in this handbook, a CBP business process transaction. CBP records document transactions of CBP business processes. Business process examples include: financial, human capital and payroll, arrest, arrival, detention, decisions, policy development, acquisition, intelligence gathering, asset forfeiture, inventory control, etc.

**Component Office**: Any CBP Office headed by an Executive Assistant Commissioner (EAC), Assistant Commissioner (AC), or equivalent. A subcomponent is any office or organizational unit subordinate to a Component Office. For example, Human Resource Management (HRM) is a Component Office, and Labor and Employee Relations is a subcomponent of HRM. U.S. Border Patrol (USBP) is a Component Office, and the El Paso Sector is a subcomponent.

**Continuity of Operations (CoOP)**: Contingency action plan that provides the capability for a Department and/or Agency to continue operations during a crisis that renders the organization's headquarters unusable.

**Continuity of Operations (CoOP) Records**: See Essential/Vital Records.

**Contractor records**: Records and information created or stored by a CBP contractor that are subject to the same records and information management requirements as all other CBP material. Process Owners and Contracting Officers Representatives (CORs) must oversee contractor records and processes.

**Controlled Unclassified Information (CUI)**: Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

**Disaster**: An unexpected occurrence inflicting widespread destruction and distress resulting in long-term adverse effects on agency operations.

**Disposition schedules**: Mandatory disposition instructions that provide continuous authority to dispose of recurring series or systems of records, or to transfer them to the National Archives and its national network of FRCs.

**Documentary material**: Collective term for records and non-record materials that refers to recorded information, regardless of the nature of the medium or the method or circumstances of recording (36 C.F.R. 1220.18).

**Electronically Stored Information (ESI)**: Any data, records, or information created, manipulated, communicated, stored, and best utilized in digital form, requiring use of computer hardware and software.

**Emergency**: A situation or occurrence that warrants immediate action to save lives and protect property, public health, and safety. An emergency would, to some degree, disrupt normal CBP operations. Examples of an emergency are:

- Natural disasters
- Man-made and technological hazards
- Civil disturbances
- Terrorism
- Material and emergency shortages
- Infrastructure failures

**Emergency operating records**: Records vital to the continued functioning or reconstitution of an organization during and after an emergency. These records are deemed vital under the CBP Comprehensive Emergency Management/Continuity of Operations (CoOP) Program plan. Emergency operating records may include: emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, and related policy or procedural records that assist agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency. Appendix 10B identifies examples of emergency operating records.

**Essential/vital records**: Records and information CBP would use in an emergency. CBP is required to plan for the storage and maintenance of essential records and information necessary to minimize disruption of its operations in consequence of a catastrophic event. These records are divided into two categories:

- Records and information that ensure the survivability of essential operations under a national emergency
- Records and information essential to the legal and financial rights of individual citizens, CBP and the Federal Government. These materials include such groups as retirement records, finance and accounting records, and valuable personnel research records and information.

**Federal Enterprise Architecture (FEA)**: DHS File Codes are records, information, and data categories based on the structure of the Federal Enterprise Architecture. All CBP records series have an associated Federal Enterprise Architecture – DHS File Code, and file plans always cross-reference these codes.

**File plan**: A comprehensive outline that includes the records series, file organization, active file locations, Federal Enterprise Architecture - DHS File Code, file transfer instructions, file retention and disposition instructions, and other specific instructions that provide guidance for effective management of records, including essential/vital records.

**General Records Schedule (GRS)**: Mandatory disposition instructions issued by NARA for temporary administrative records that are common to most federal agencies.

**Legal and financial rights records**: Records that are essential for the preservation of legal rights and interests of individual citizens and the Federal Government. Examples include: official personnel files, accounts receivable records, payroll records, and valuable research records. Appendix 10C identifies examples of legal and financial rights records.

**Litigation and oversight holds**: This requirement stipulates that all records that may relate to a legal or Congressional oversight action involving CBP must be retained. It ensures that the applicable records are available for the discovery process prior to litigation. CBP must preserve records when it learns of pending or imminent litigation or when litigation is reasonably anticipated. Litigation holds prevent the spoliation (e.g. destruction, alteration, or mutilation) of evidence, which can have a negative impact in litigation. Each litigation hold will provide specific records production and preservation guidance.

**National Archives and Records Administration (NARA)**: Agency that establishes policies and procedures for managing U.S. Government records. NARA assists federal agencies in documenting their activities, administering records management programs, scheduling records, and retiring noncurrent records to FRCs, and conducts periodic evaluations of agency compliance.

**Non-record material**: U.S. Government-owned documentary materials excluded from the legal definition of records (44 U.S.C. 3301), either by failing to meet the general conditions of record status already described or by falling under one of three specific categories: Extra copies of documents preserved only for convenience of reference; stocks of publications and of processed documents; or library and museum material made or acquired and preserved solely for reference or exhibition purposes.. These materials should be managed and destroyed promptly when no longer needed for business purposes. NARA's approval is not required to destroy non-record material. (36 C.F.R. 1222.16 – "How are non-record materials managed?")

**Off-site storage:** A facility other than CBP's normal place of business where essential/vital records are stored for protection. Off-site storage ensures essential/vital records are not subject to damage or destruction from an emergency or disaster affecting CBP's normal place of business.

**Permanent records**: Records sufficiently valuable for historical or other purposes that warrants continued preservation by the Federal Government. Relatively few federal records are permanent. CBP needs to maintain record sets of processed documents and of publications, including annual and special reports, directives, forms, special studies, brochures, pamphlets, books, handbooks, posters, and maps. The National Archives stores permanent records of primarily national interest at its facilities in the Washington, DC, area and those of primarily regional and local interest at its regional archives located in major metropolitan areas throughout the country.

**Personal and private papers:** Personal materials refer to documentary items not relating to or having an effect upon agency business. Personal materials belong to an individual, not the agency (See 36 C.F.R. § 1220.18). Personal materials include the following categories:

- Business or professional files created before entering Government service
- Reference files, for example professional association journals or library materials
- Copies of official personnel files that were created when the staff member entered federal service
- Personal correspondence, emails, and other materials documenting outside business or political pursuits not relating to agency business.

CBP employees may remove documentary materials of a purely personal nature when they leave the agency. Employees must not intermingle their personal and official files. In situations where personal papers are found to be intermingled with official records, the agency may need to review and approve the removal of personal materials to ensure all federal records are properly preserved and agency policies are followed. CBP employees should consult CBP RIM staff, legal counsel, or other designated officials to determine whether files are personal or federal records.

**Personally Identifiable Information (PII):** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

**Program records**: Records created, received, and maintained by CBP in the conduct of its mission functions for which it is accountable. The term is used in contrast to administrative records. Program records, in conjunction with administrative records, comprise the universe of CBP records.

**Recordkeeping requirements**: Statements in statutes, regulations, or directives that provide general and specific information on particular records to be created and maintained by CBP.

**Records:** All recorded information, regardless of form or characteristics, made or received by a federal agency 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 United States Government or because of the informational value of data in them.

Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (44 U.S.C. § 3301 Amended 26 Nov. 2014).

Records do not include:

- Library and museum material made or acquired and preserved solely for reference or exhibition purposes; or
- Duplicate copies of records preserved only for convenience.

**Records Control Schedules (RCS)**: NARA-approved disposition schedules developed specifically for an agency’s unique program records.

**Records management program**: The planned and coordinated set of policies, procedures, and activities needed to manage an agency or department's recorded information. The records management program encompasses the creation, maintenance and use, and disposition of records, regardless of media. Essential elements include issuing up-to-date program directives, properly training those responsible for implementation, and carefully evaluating the results to ensure adequacy, effectiveness, and efficiency.

**Records series/series of records**: The basic unit for organizing and controlling files. It is a group of files or documents kept together (either physically or intellectually) because they relate to a particular subject or function, result from the same activity, document a specific type of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, maintenance, or use (36 C.F.R. § 1220.18).

**Retention period**: The period of time that records are to be kept in accordance with NARA-approved records disposition schedules.

**Temporary records**: Records determined by NARA to be disposable or nonpermanent. Most federal records are temporary. NARA approves such records for destruction or, occasionally, for donation to an eligible person or organization. Many temporary records are eligible for destruction when no longer needed in an office to conduct current business. Others are eligible only later, after storage. Temporary records should be destroyed promptly in accordance with NARA-approved record schedules.

**Transitory records:** Some records are transitory in nature, which means they are of short-term (180 days or less) interest, including in electronic form, and have minimal or no documentary or evidential value.

**Unidentified** or **unscheduled records**: Records that do not have a NARA-approved disposition schedule. RIM Office works with LRIMs, Records Custodians and Process Owners to obtain NARA approval of RCSs. Any ***unscheduled records are permanent records and may not be destroyed until their disposition has been determined by NARA. Only the Archivist of the United States has authority to determine disposition of federal records.***

**Vital records**: See Essential/Vital Records.

## C. Importance of Records and Information Management

Records are among the basic tools the government uses to do its work. Whenever the government makes a transaction or a decision, takes an action, or creates a policy, the resulting documentation is a record. Without a good RIM program, records clutter CBP offices and electronic storage, requiring costly space and equipment. This congestion interferes with the efficient administration of programs.

An effective RIM program helps guard against unauthorized disposal of automated files that contain evidence of financial and legal commitments, which must be preserved to protect the government; or information needed to protect the civic, legal, and property rights of private citizens; or provide continuity of policies, actions, and organizational and procedural patterns for sound administration.

Records are the memory of every federal agency and contain a wealth of data for scholarly and technical research and analytics in almost every field. The problems caused by premature disposal include the need for costly re-creation of automated files; the lack of audit trails to support management policy, decisions and, accounting operations or financial statements; and the ability to detect fraud or other potential irregularities.

| RIM Directive Policy #: | Part 2-C: CBP Policy Statements | Reference |
|---|---|---|
| 2.1.6 | Each Component Office shall adopt safeguards for records under its custody and control commensurate with the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to, or modification of those records as stipulated in CBP Handbook HB1400-05D. Component Offices shall safeguard all Personally Identifiable Information (PII) as detailed in CBP Directive 2120-010. | OMB Circular A-130 Part E |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(H) | Implement a Vital Records Program. | |

## D. The Records and Information Management Process

The records process can best be followed by taking the steps noted below.

A. Each Component Office designates a Local Records and Information Manager (LRIM). When an LRIM leaves, a replacement is designated and the name of the LRIM is forwarded to CBP RIM at (b) (7)(E)
B. Each Component Office provides consistent, visible support for RIM through established communication channels.
C. LRIM and all other employees with RIM responsibilities (see Part 1, section C) are trained in records and information management. Training is available from NARA and in DHS Performance and Learning Management System (PALMS).
D. The RIM Handbook is made available to all employees and contractors. This Handbook can be found on the RIM SharePoint site and in the Policy Online Document Search (PODS).
E. LRIM conducts records inventory annually and updates file plans as necessary. For more information on the File Plan, see Part 6.
F. All records are identified regardless of form (including electronic, photographic, audiovisual, original posters, and engineering or architectural drawings) and need to be physically segregated or readily identified and segregated from all other materials. If a clear determination cannot be made, the materials should be treated as records. Consult with CBP RIM for guidance.
G. Eligible temporary records are destroyed in accordance with approved records schedule retention instructions. Temporary records are disposed of promptly when their retention periods expire, except when the records are the subject of a pending request, appeal, or lawsuit under the Privacy Act, pursuant to General Records Schedule (GRS) 4.2.
H. Non-record materials and information should be managed and purged when no longer needed for business purposes. NARA's approval is not required to destroy such materials.
I. Eligible permanent records are transferred to NARA.
J. If storage is unavailable locally, records are appropriately transferred to and stored in an FRC or other CBP RIM-approved storage facility.
K. Records or their containers are labeled with their contents and dispositions ensuring they can be filed, located, and retrieved as needed.
L. Permanent records are identified and preserved, and should be transferred to NARA in a timely manner. Permanent records must be stored separate from temporary records and non-records.
M. All record materials must be organized by Federal Enterprise Architecture – DHS File Codes.
N. LRIM must respond to FRC Notices of Destruction in a timely manner but not more than two weeks after receipt.
O. GRS lists the disposition schedules for all administrative records.

| RIM Directive Policy #: | Part 2-D: CBP Policy Statements | Reference |
|---|---|---|
| 2.1 | CBP and its Component Offices shall establish and maintain effective and efficient processes and practices for governance and management of federal records, data, and information.  Program and administrative managers have ultimate functional responsibility for implementing CBP records, data, and information management policies and procedures set forth in this Directive in their operational areas. | 36 C.F.R. §1220.34 |
| 2.1.2 | Each Component Office shall work with CBP RIM to ensure all its records have a NARA-approved retention schedule. Records, regardless of media type, that do not have NARA-approved schedules intended for CBP use must be treated as permanent until a retention schedule is approved.  Component Offices must establish internal retention periods for non-record materials, data, and information that ensure prompt and proper destruction when no longer needed for business purposes. | 36 C.F.R. §1224.10 |
| 2.1.4 | Each Component Office shall conduct an annual inventory and file plan review of all Office records to identify new records and review business needs for existing record series.  File plans must include record series title and description, location, and retention schedules that are aligned and cross-referenced with Federal Enterprise Architecture - DHS File Codes. | 36 C.F.R. §1222.26; §1222.28 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(G) | Create and/or Implement Record Schedules:<br>1. Where acceptable, apply the General Records Schedules (GRS), as approved by the National Archives and Records Administration.<br>2. For mission related records, follow the instructions for disposition of records as specified by the approved DHS, Component, or Enterprise Records Schedule and dispose of as authorized by that schedule.<br>3. In the absence of a Record Schedule, create DHS, Component, or Enterprise Record Schedules which specify disposition instructions for unscheduled records and submit to the National Archives and Records Administration for approval by the Archivist of the United States. | |

## E. Safekeeping Records

CBP offices should file their records in accordance with the approved CBP File Plans. Records maintenance and safekeeping procedures should be reviewed annually.

Managers proposing to keep records beyond their retention periods for the purposes of audit, court order, litigation, study, or any other administrative purpose must submit an explanation and justification for such action to the CBP Chief Records Officer.

LRIMs should perform an annual review of their records management programs to ensure adherence to proper records management standards. It is particularly important that permanent records are properly maintained and promptly retired to FRCs according to the CBP File Plan. A copy of the annual review should be forwarded to the CBP Chief Records Officer.

LRIMs should also ensure that records stored off-site are maintained in accordance with approved disposition schedules and separated from personal and private papers.

| RIM Directive Policy #: | Part 2-C: CBP Policy Statements | Reference |
|---|---|---|
| 2.1.3 | Each Component Office may also have separate and additional obligations to preserve information relevant to litigation. Each Component Office shall comply with all litigation holds, court rules, and other rules and policies as well as any guidance provided by Office of the Chief Counsel (OCC) related to preservation of information. | 36 C.F.R. §1220.34 |

## F. Essential/Vital Records

CBP Directive 2110-040 requires each Component Office annually identify the essential/vital records necessary to ensure Continuity of Operations (CoOP) and provide up-to-date, accessible copies when and where needed.

NARA has issued an Essential Records Guide that addresses identification and protection of records. It highlights accessing information needed to conduct agency business under emergency operating conditions or to protect the legal and financial rights of the Federal government and the people it serves. This Guide also provides information to assist agencies assessing damage and implementing recovery of records affected by an emergency or disaster.

Please see Appendix 10 for NARA's Essential Records Guide issued August 2018.

For more information on the CBP CoOP process, please see the CBP-wide Continuity Plan and Component Office CoOP Implementation Plans.

| RIM Directive Policy #: | Part 2-C: CBP Policy Statements | Reference |
|---|---|---|
| 2.1.5 | Each Component Office shall annually identify the essential/vital records necessary to ensure Continuity of Operations (CoOP) and provide up-to-date, accessible copies when and where needed. | 36 C.F.R. §1223.14; §1223.22 |

## G. Evaluation and Certification

Beginning January 2020, each Component Office will conduct an annual internal evaluation of its RIM program to certify its compliance with NARA regulations and CBP policies and procedures. LRIMs will need to submit their annual certification to the CBP CRO by September 30 of each year.

Beginning January 2020, the CBP CRO, in conjunction with each Component Office, will conduct an in-depth evaluation of its records management program every three (3) years. This in-depth review will consist of, but is not be limited to, records sampling, record inventories, updates to program record schedules, and data, information, and non-record materials. Each Component Office will submit an annual Corrective Action Plan to the CBP CRO, addressing any deficiencies identified in the annual internal evaluation and/or the triennial review.

The process and forms for completing evaluations and certifications are found in Appendix 9.

| RIM Directive Policy #: | Part 2-F: CBP Policy Statements | Reference |
|---|---|---|
| 2.4 | Beginning January 2020, each Component Office shall conduct an annual internal evaluation of its RIM program to certify compliance with NARA regulations and CBP policies and procedures. LRIMs designated by each Component Office shall submit the annual certification to CBP's CRO by September 30 of each year. | 36 C.F.R. §1220.34 |
| 2.5 | Beginning January 2020, CBP's CRO, in conjunction with each Component Office, shall conduct an in-depth evaluation of its records management program every three (3) years. Reviews and evaluations will be conducted consistent with the CBP RIM Evaluation and Certification Process, located in Appendix 9 of the RIM Handbook. | 36 C.F.R. §1220.34 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(I) | Evaluate annually the RIM Program, including records disposition, responsibilities, training, and records maintenance. | |

## H. Basic File Types for Records

CBP creates and maintains several types of federal records. These include:

- **General or subject files** - Consists of materials arranged by subject. Files may include correspondence, memoranda, reports, studies, and other miscellaneous materials.
- **Case files** (includes project and transaction files) - Contains material on a specific action, event, organization, product, or thing (e.g., entries, Return on Investments, manifests, or audits). The documents may cover one subject or many subjects about a case or project.
- **Case working papers** - Consists of working papers and related short-lived correspondence gathered for a specific case or project. They may include background and support materials, such as worksheets, questionnaires, rough notes, and calculations. They may even include drafts used to prepare or analyze case file official documents. Working papers should not be separated from the case files until the project or case is completed. Once the case is closed, working papers that are incorporated in the case file should be kept separately, as retention periods will differ.
- **Drafts and working files -** Support documents for reports, special studies, memorandums, and correspondence that may not be otherwise incorporated into office files. Support documents may be needed to fully understand the alternatives and options considered for high-level program initiatives and serve as draft courses of action. Some drafts contain unique information in substantive annotations or comments added during circulation for comment or approval. Agencies should maintain such drafts, with the file copy of the final document when the drafts relate to formulation and execution of policies, decisions, actions, or responsibilities. In the development of policies and decisions, drafts and working files that propose and evaluate options or alternatives and their implications or that document findings or support recommendations should be preserved.

CBP employees may also maintain reference materials or technical reference papers, and personal materials—none of which are considered federal records and are, therefore, not subject to disposition schedules. The following items must be kept separate from federal records:

- **Reference materials or technical reference files -** Usually consists of publications that have a direct program relationship to the official mission of the office. Required for technical reference, they may include handbooks, brochures, pamphlets, periodicals, special reports or studies, and similar publications. Technical reference files often serve to supplement available library resource materials.
- **Personal materials** - Refers to documentary items not relating to or having an effect upon agency business. Personal materials belong to an individual, not to CBP (See 36 C.F.R. § 1220.18). Traditionally, personal materials have included the following categories:
    - Business or professional files created before entering Government service;
    - Reference files, for example professional association journals or library materials;
    - Copies of your official personnel file that were created when you entered federal service;
    - Personal correspondence, emails, and other materials documenting outside business or political pursuits not relating to agency business.

Employees may remove documentary materials of a purely personal nature when they leave CBP. Employees should consult CBP RIM staff, legal counsel, or other designated officials to help determine whether files are personal or federal records.

## I. File Arrangements

CBP files should be organized according to the Federal Enterprise Architecture (FEA) – DHS File Codes. See Appendix 1B for more details. Other file arrangements are authorized if needed for business use. Underneath the file code, more granular file arrangements can be used to more easily locate and access records. Examples of these more granular file arrangements include:

- **Alphabetic/Subject files** – Records arranged by main subject as well as subdivisions in alphabetical order. Numbers are not used. This filing method has the advantage of being easily understood, and works well for a small number of files and users. The difficulty in maintaining alphabetical files is selecting the same subject each time.
- **Numeric files** - Records arranged and referred to by number such as contracts, grants, projects, purchase orders, and similar files.
- **Alphanumeric files** – Records filed according to a letter code and number. Subjects are broken down into primary, secondary, and tertiary subjects. Examples of file codes include ADS, ADS 1, ADS 1-1, and ADS 2. The alpha element can, in this manner, indicate the function or part of the organization served by the file. The alphanumeric method permits adding or deleting the primary heading in an alphabetical sequence.
- **Chronologically arranged files** - Records maintained in a chronological (time) order with the date serving as the primary means of reference. Reading files and suspense files are commonly arranged by date.

| RIM Directive Policy #: | Part 2-H: CBP Policy Statements | Reference |
|---|---|---|
| 2.1.4 | Each Component Office shall conduct an annual inventory and file plan review of all Office records to identify new records and review business needs for existing record series. File plans must include record series title and description, location, and retention schedules that are aligned and cross-referenced with Federal Enterprise Architecture - DHS File Codes. | 36 C.F.R. §1222.28 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(A)(1-2) | 1. Non-records are not retained beyond the usefulness of the records or when no longer needed for reference and should be kept separate from official DHS records.<br>2. Keep personal records to a minimum and separate from official DHS records. Personal files are excluded from the definition of federal records and are not owned by the Government. | 44 U.S.C. § 3301 |
| Instruction 141-01-001 (VI)(B)(2) | Non-records are managed separately from records, inventoried, and deleted or destroyed in accordance with DHS Records Policy. | |

| | | |
|---|---|---|
| Instruction 141-01-001 (VI)(B)(3) | Personal records are non-records and maintained separately from DHS records and kept to a minimum. | |

## J. Removal of Records from CBP Custody

Records, information, data, and non-record materials are the property of the Federal Government, not the property of individual employees, and may not be removed from CBP without proper authority. All officers and employees shall maintain records and non-record materials separately from one another.

No manager or employee shall allow CBP records, information, data, or non-record materials to leave CBP custody, even temporarily, other than as authorized by this Handbook. This restriction does not apply to authorized release of records, information, data, and non-record materials or other documents in the conduct of official business.

The responsibility to determine what documentary materials in CBP constitute records, as defined in 44 U.S.C. § 3301, rests with the CBP Commissioner. CBP will work directly with NARA on an initial determination, consulting with the Office of Chief Counsel (OCC) as necessary.

No departing officer or employee shall remove any materials, whether records or not, that contain national security information or information of a confidential nature. Questions about national security materials should be addressed to the Office of Professional Responsibility. Questions about other kinds of confidential or protected information should be addressed to OCC. Non-record materials may be removed by departing officers if their removal is not prohibited.

CBP records management officers shall establish informational programs to ensure that all officers and employees are aware of their record management responsibilities. Periodic memoranda to all employees, briefings, posters, and brochures are suitable techniques for disseminating this information. The following information, at a minimum, should be disseminated:

> *The willful and unlawful concealment, mutilation, obliteration, falsification, or unauthorized removal or destruction of federal records is against the law. The individual shall be fined or imprisoned not more than three years, or both, and risk forfeiture of his or her position and disqualification from holding any other federal office (18 U.S.C. 2071(b)).*

Employees are required to report any apparent instances of unauthorized disposition to their supervisor and CBP CRO. Managers or supervisors will report to the CBP CRO, NARA, and where appropriate, the Joint Intake Center, any unlawful or accidental removal, defacing, alteration, or destruction of CBP records (44 U.S.C. 3106).

| RIM Directive Policy #: | Part 2-I: CBP Policy Statements | Reference |
|---|---|---|
| 2.6 | All records created, contributed to, or received by a CBP official, employee, or contractor in the course of | 36 C.F.R. §1222.24 |

| | | |
|---|---|---|
| | conducting Government business are CBP property, wherever the records reside. No person attains proprietary rights or interest in any record that he/she may create, provide input into, or acquire custody or possession of, by virtue of his/her position as an official, employee, or contractor. | |
| 2.7 | Materials that are entirely personal are not "records" for purposes of CBP records and information management requirements. Personal materials must be maintained separately from CBP records at all times. | 36 C.F.R. §1222.24 |
| 2.8 | Removal of documentary materials (see Section 5.7) by a separating Presidential appointee or employee must be approved by the CBP CRO in accordance with the provisions of this directive to ensure that CBP's abilities to claim privileges during litigation, to apply FOIA exemptions, and to protect confidential information are not diminished or waived. | 36 C.F.R. §1222.24 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(F) | Establish appropriate out-processing for departing employees and ensure that the program or process is established to review and adjudicate requests for the removal of records. | |
| Instruction 141-01-001 (VI)(B)(4) | Employees (including Career Senior Executive Service and Political Appointees) may not remove or duplicate DHS records upon separation without prior approval by the Component Head. | |

## K. Donation of Temporary Records

When the public interest will be served, managers desiring to donate records may propose transfer of records eligible for disposal to an appropriate person, organization, institution, corporation, or government (including a foreign government) that has requested them. Records will not be transferred without prior written approval of NARA.

CBP shall request approval of such transfer by sending a letter to NARA at 8601 Adelphi Road, College Park, Maryland, 20740-6001, following the instructions in Section 1228.60 of Title 36 of the C.F.R., "Donation of Temporary Records."

## L. Retirement or Storage of Records to a Federal Records Center (FRC)

Acceptance for storage at FRCs is referred to as "retirement". FRCs will accept retirement records, subject to the following conditions:

- The records are properly scheduled.
- Records are not authorized for immediate disposal and transportation costs are not in excess of resulting savings.

- Facilities are available for storing and providing reference on the records.
- See Appendix 3 for detailed instructions.

Upon receipt of the records at FRC, the cartons will be matched against the copy of the SF-135 submitted with the shipment. A copy of the SF-135 is signed by the officials at FRC and returned to CBP.

## M. Transfer of Records to the National Archives

Records scheduled as permanent shall be transferred to the National Archives after the period specified on the disposition schedule. Transfers of records constituting systems of records subject to the Privacy Act of 1974 (5 U.S.C. § 552a) shall be accompanied by the most recent CBP privacy notice covering the records. Records officially transferred to the legal custody of the National Archives will be available to CBP employees, if needed, in the course of official business. Officials requiring access to such records shall make their request known to their LRIM.

## N. Destruction of Temporary Records

Offices are required to follow the regulations issued by the Archivist of the United States governing the method of destroying records. CBP employees are expected to follow OCC guidance and take all reasonable steps to preserve information that is relevant to litigation, regardless of the approved retention period.

- Paper records to be disposed of normally shall be sold as wastepaper.
- If the records are national security classified their disposal is governed by E.O. 12958.
- If the records are restricted; that is, if laws, including the Privacy Act or regulations that forbid their use by the public, the wastepaper contractor shall be required to pulp, macerate, shred, or otherwise definitively destroy the information contained in the records, and their destruction must be witnessed by a federal employee or a contractor employee, if authorized by the CBP program official responsible for the records.
- The contract for sale shall prohibit the resale of all other records for use as records or documents. Records other than paper may be salvaged and sold in the same manner and under the same conditions as paper records.
- When records cannot be sold advantageously or otherwise salvaged, they may be destroyed by burning, pulping, shredding, macerating, or other suitable means.

| RIM Directive Policy #: | Part 2-M: CBP Policy Statements | Reference |
|---|---|---|
| 2.9 | Destruction of records is authorized only in compliance with NARA-approved retention schedules intended for CBP use. Criminal penalties are assessed for willful and unlawful destruction, damage, or removal of federal records, as described in 18 U.S.C. § 2071. | 44 U.S.C.§3105;<br>36 C.F.R. §1230.10 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Instruction 141-01-001 (VI)(B)(5) | DHS records, regardless of format, cannot be destroyed without an approved schedule. | |

## O. Photographs and Audiovisual Records

Audiovisual records are federal records, in picture or sound form, that include still and motion pictures, graphic materials, sound and video recordings, and combinations of media, such as slide-tape productions. These materials are considered records in the same way as any letter, memorandum, or case file related to official business, and the basic principles and practices of managing paper records also apply to audiovisual records.

Audiovisual records must also be managed to ensure adequate and proper documentation and appropriate disposition. CBP RIM establishes standards for physical security of audiovisual records and reviews audiovisual recordkeeping practices to improve procedures.

### 1. Responsibilities

The offices and individuals listed below are assigned responsibility for audiovisual records and prescribe the types of records to be created and maintained so that audiovisual operations and their products are properly documented.

**The Assistant Commissioner, Office of Information and Technology** has overall responsibility for management and coordination of the CBP Audiovisual Program.

**The Chief Records Officer (CRO)** reviews the audiovisual plans and policies of public affairs activities at CBP. CBP's CRO provides program guidelines, coordination, technical assistance and serves as a point of contact for audiovisual records with the Office of Management and Budget and the National Technical Information Service.

**CBP managers** provide an appropriate program for management of audiovisual records. The following guidelines apply to CBP managers:

- Establish contract specifications that will protect the Government's legal title and control over contract produced audiovisual records, such as audiovisual media and related documentation; and
- Keep inventories indicating the location of all generations of audiovisual records, whether in CBP storage, at a FRC, or in a commercial facility, such as a laboratory or library distribution center.

All CBP employees are responsible for creating, maintaining, using, protecting, and disposing of audiovisual records in their program areas consistent with approved records schedules.

### 2. Disposition Audiovisual Records Including Photographs

The inventorying and scheduling of audiovisual records including photographs are especially important because of the fragility of the media. As with other types of records, most audiovisual records are not permanent. Audiovisual records should not be evaluated in isolation from other records. The following rules should be used:

- Inventory and schedule photographs, films, and magnetic media at the same time as other CBP records.
- Schedule audiovisual records as early as possible in their lifecycle. This is important because appraisal decisions made as part of the scheduling process will affect the way in which these records are created and maintained. For example, if a photographic series has been identified as permanent, all negatives in that series should be jacketed individually rather than collectively.
- The disposition of audiovisual records will be carried out in the manner as prescribed for other types of records. Erasable media, such as audiotape, should be reused whenever practical.

## 3. Potentially Permanent Photographs and Audiovisual Records

The following examples of audiovisual records are normally of permanent value and shall be transferred to the National Archives as soon as they become inactive or CBP cannot provide proper care and handling:

- Official portraits of CBP Officials; photographs produced or collected for use in CBP publications, exhibitions, or other media productions; documentary photographs shot for fact-finding purposes, research and development, or other studies; photographs that depict the program or mission of CBP; and slides of filmstrip programs that depict CBP's program or mission.
- Original poster artwork distributed CBP-wide or to the public and original artwork of unusual or outstanding merit.
- CBP-sponsored informational, educational, and recruiting films, videos, or sound recordings intended for public distribution; television news releases or information reports; training programs that explain CBP functions or activities intended for internal or external distribution; films acquired from outside sources that document or are used to carry out CBP programs; administrative training programs; and recordings of public meetings or speeches, conferences, guest speakers, and testimony of CBP officials before Congress and at other hearings.

## 4. Management of Analog Audiovisual Records

Audiovisual records have complex and diverse physical attributes that require special handling, storage, and preservation processes. Appendix 7 provides NARA guidance on storage and handling practices. More detailed and current information can be found at NARA's website: https://www.archives.gov/records-mgmt/publications/managing-audiovisual-records.html.

## 5. Analog Cartographic, Architectural, and Engineering Records

**Analog Cartographic** records are graphic representations drawn to scale of selected cultural and physical features of the earth, of other planetary bodies, and the atmosphere. Architectural and engineering drawings, also known as design and construction drawings, are graphic records that depict the proposed and the actual construction of stationary structures, such as buildings, canals, and movable objects. Closely-related records such as indexes and written specifications frequently accompany the drawings. Maps and charts fall into four types and are considered PERMANENT records:

- **Manuscript maps** - Printed and processed maps on which manuscript changes, additions, or annotations have been made for record purposes or that bear manuscript signatures to indicate official approval; and single printed or processed maps that have been attached to or inter-filed with other documents of a record character.
- **Master sets of printed or processed maps issued by CBP** - A master set should include one copy of each edition.
- **Computer related and plotted maps** - Cannot be reproduced by NARA without the appropriate computer equipment.
- **Index maps, cards, index lists, or other finding aids** - Helpful in using the transferred maps.

For specific guidance on management and preservation of cartographic materials, contact the CRO.

**Analog Architectural and Related Engineering**: There are multiple types of engineering drawings. These include:

- **Design drawings, preliminary and presentation drawings, and models** - Document the evolution of the design of a building or structure.
- **Master sets of drawings** - Document the condition of a building or structure in terms of its initial construction and subsequent alterations. This category includes final working drawings, "as-built" drawings, shop drawings, and repair and alteration drawings.
- **Drawings of repetitive or standard details of one or more buildings or structures** - "Measured" drawings of existing buildings and original or photocopies of drawings are reviewed for approval.
- **Related finding aids and specifications** - Necessary for engineering drawings to be followed.

For specific guidance on management and preservation of architectural and engineering materials, contact the CRO.

## P. Micrographic Records

Use of micrographic systems to maintain a system of records requires direct NARA approval. For specific guidance on management and preservation of micrographic records, contact the CRO.

# Part 3: Electronically Stored Information, Including Email and Messaging

This section contains instructions, standards, and guidelines for managing records and information in electronic form to comply with regulations and guidance issued by NARA (36 C.F.R. Chapter XII, Subchapter B, Part 1236). It also includes information on scheduling copies of program and administrative records created in electronic mail (email), messaging systems, office productivity applications, and other computer applications.

## A. Objectives

Unless otherwise noted, these requirements apply to all CBP systems that create records, information, and data, which are more commonly known as Electronically Stored Information (or "ESI"[2]). ESI must be managed, regardless of technology platform or storage media, in networked, stand-alone, or Cloud configurations. To ensure that information will be available when needed, and that unneeded information will be properly disposed of, CBP RIM will ensure that managers, employees, and contractors are advised as technology and recordkeeping requirements evolve and electronic recordkeeping responsibilities change.

Electronic records must be:

- Secured and managed throughout their life from creation and receipt to final disposition.
- Preserved for fiscal, legal, administrative, or historical purposes and accessible and useable throughout their life.
- Destroyed in a timely fashion, in accordance with the correct disposition schedules.
- Managed to make cost-effective use of computing, storage, and other resources.

Electronic information not considered a record must be:

- Secured and managed throughout its life.
- Managed to make cost-effective use of computing, storage, and other resources.
- Destroyed when no longer needed.

[2] This Handbook uses the industry standard term "Electronically Stored Information (ESI)" to refer to records, information, and data.

## B. Responsibilities

**Assistant Commissioner, Office of Information and Technology (OIT) CIO**:

- Establishes procedures for addressing records management requirements, including recordkeeping and disposition requirements, before approving new electronic information systems or enhancements to existing systems. (36 C.F.R. § 1236.10)
- Ensures recordkeeping requirement procedures are implemented and followed for each new or modernized electronic information system.
- Ensures revisions and updates are made to ESI Retention Schedules, as appropriate, to reflect changes in operational policy that impact retention periods established in the schedules, and/or other essential procedural and technical changes (including data retention guidelines required for new systems) relative to the overall management of data retention.
- Complies with NARA regulations, guidance, and standards for management, disposition, or transfer and retirement of ESI to a FRC.
- Collaborates with OCC to determine legal implications of electronically stored information including litigation and preservation requirements.
- Collaborates with CBP Privacy Officer to ensure that all records are stored, disseminated, and managed consistent with DHS policies for safeguarding PII.

**All CBP organizations developing automated systems must**:

- Ensure automated business transactions are adequately and properly documented by creating appropriate records. See Agile Governance Framework[3] for detailed guidance.
- Ensure ESI for all systems is properly managed and maintained and that it adheres to retention periods established in Records and Data Retention Schedules.
- Ensure operational responsiveness to user needs for access to ESI.
- Acquire or develop and implement archive and digital preservation services or applications to support approved records and data retention schedules, and scheduling execution of these archive applications by the Enterprise Networks and Technology Support Directorate, Enterprise Data Management and Engineering Directorate, or their successors.
- Conduct a Privacy Threshold Analysis (PTA) to determine any privacy compliance requirements and ensure that all records are stored, disseminated, and managed consistent with DHS policies for safeguarding PII.

**Director of Enterprise Networks and Technology Support Directorate and Director of Enterprise Data Management and Engineering Directorate** or their successor organizations are responsible along with the product owner for managing hardware and software required for storage and preservation of historical ESI and ensuring systemic responsiveness to user needs for access to it.

**Executive Director, Office of Policy** collaborates with CBP RIM to establish and implement policies and procedures to guard against unauthorized destruction, loss, removal, or theft of ESI.

**Chief Information Security Officer** is responsible to ensure physical and logical security controls are in place and functioning in all CBP systems that create, store or provide access to ESI.

[3] https://uconnect.cbpnet.cbp.dhs.gov/sites/oit/ais/Pages/Default.aspx

**Executive Director, Privacy and Diversity Office** is responsible for ensuring the CBP RIM is consistent with FOIA, Privacy Act, and all applicable laws and Departmental policies to ensure the safe handling of PII.
**Executive Assistant Commissioners, Assistant Commissioners, and equivalent** ensure the instructions outlined in this section are executed for their respective operational areas.

**Process Owners**:

- Work with CBP RIM to propose proper retention periods for ESI used by computer applications supporting their business processes.
- Mutually agree on proposed retention periods where ESI is used by multiple Process Owners. Each process owner is responsible for conducting ESI retention and disposition evaluations annually.

**CBP Program Managers (system owners)**:

- Oversee creation and use of ESI in an information system;
- Work with RIM team to ensure new Systems of Record are specified, funded, designed, and developed to federal recordkeeping requirements detailed in NARA regulation and guidance before they are authorized to operate (36 C.F.R. § 1236.10).
- Ensure the requirements of this section are implemented for their systems. They are responsible for managing those systems under their functional control and for maintaining those systems in accordance with electronic recordkeeping guidelines; and
- Ensure that all CBP systems that create, handle, and store records are scheduled and that proper records controls are applied.

**Information creators and/or content providers**, including all CBP employees and contractors:

- Ensure all electronic records are properly maintained and disposed of in accordance with the provisions of this section and NARA's GRS;
- Notify CBP RIM when planning a new system or applications;
- Determine who is responsible for creating and maintaining records;
- Become familiar with the requirements of this section;
- Identify and describe the applications supported by automated systems by means of defining their purposes, their information contents, and the main stages through which the data flow;
- Determine the length of time the information is needed to support organization operations and protect rights and interests; and
- Describe the indexing arrangement and, to the extent possible, the internal information structure and search possibilities; and implement disposition instructions on an approved schedule.

## C. Electronic Recordkeeping Concepts

OMB Circular A-130: Managing Information as a Strategic Resource requires agencies to:

- Manage all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format;
- Manage all email records electronically and retain them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed.

Management of electronic records is similar to that of paper records in some key respects. Electronic records:

- Must, in any form or on any media that meet criteria established for federal records, be managed consistent with federal regulation. (36 C.F.R. Chapter XII, Subchapter B, Part 1236)
- Must be maintained and disposed of consistent with an approved RCS.
- Are destroyed or transferred to NARA for permanent retention after the retention period.

CBP requires the digital version of a record be treated as the record copy. All other copies are subject to treatment specified in CBP RCS or GRS. Although paper copies may be printed for distribution, **the official record copy is retained and managed as ESI**.

## D. Creation and Receipt of Electronic Records

Information in any form, media created or received by CBP in carrying out its mission, and business transactions constitute a federal record. How long a record needs to be kept to facilitate CBP business and the degree to which it needs to be controlled are functions of its value to the CBP's mission and its legal requirements.

### Lifecycle of records and information

ESI has a lifecycle and exists in different formats during the different stages of its lifecycle. When establishing a system of electronic records, the full life of the records must be considered and planned.

- System designers should contact CBP RIM as part of the initial planning phase of the development process. This will enable the designers to correctly determine and incorporate necessary recordkeeping requirements into the system design, development, testing, and implementation, thereby avoiding potentially costly changes after the system is deployed.
- Early involvement of CBP RIM is especially critical in the case of major systems that may contain permanent records.

ESI is created or used in most facets of CBP work. Increasingly, ESI is created by or inputs are made using mobile devices. It is then stored and managed in cloud-based infrastructures where it is accessible anytime or any place it is needed.

Regardless of how or where ESI is created or where it is stored, it must be protected and managed according to federal statutes, regulations, and approved RCSs throughout its life.

Any electronic record suspected or determined to be permanent must be created and maintained in an acceptable format. See Appendix 1F, Electronic Records Transfer Formats, for more details.

## E. Security of Electronic Records

Care must be taken to ensure the security of ESI. Before developing solutions, each system owner must: (1) determine the degree of acceptable risk associated with the proposed application and the records, data, and information it will process, store, and present; (2) follow established CBP risk management processes; and (3) work with the Cyber Security Directorate/Chief Security Officer to plan for and build information security controls into the application from the outset.

| RIM Directive Policy #: | Part 3-E: CBP Policy Statements | Reference |
|---|---|---|
| 2.1.6 | Each Component Office shall adopt safeguards for records under its custody and control commensurate with the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to, or modification of those records as stipulated in CBP Handbook HB1400-05D. Component Offices shall safeguard all Personally Identifiable Information (PII) as detailed in CBP Directive 2120-010. | 36 C.F.R. §1222.34 |

## F. Organization and Maintenance of Electronic Records and other ESI

**ESI must be:**

- Stored in a format and in a way that will ensure its protection and that allows efficient discovery, access, and use.
- Identified sufficiently to enable authorized personnel to retrieve, protect, and carry out its disposition.

**ESI Storage:**

- **Network drives:** CBP encourages the use of network drives such as SharePoint or shared drives for storage of records and other relevant business data and information.
- **Local drives:** CBP expressly discourages the use of local drives and removable media such as the C: drive, flash drives, removable hard drives, or compact discs for storage of records and other business relevant data and information.

**Folder structure:** Folder structures for ESI, in any form or storage system, are best patterned after approved office file plans. This includes email, SharePoint, MySites, shared drives, home drives, local drives, and removable media. See Appendix 2, Approaches for Organizing a Shared Drive, and Appendix 1B, Use of FEA – DHS File Codes, for more information.

- More granular folders for each approved record series or file category may be established as needed. If desired, the retention period for each folder may be included in the file name or a persistent identifier to assist disposition. See Part 2, Section H for further information about file arrangements.

**Folder and file naming conventions**: To facilitate access, preservation, and disposition, a standardized approach to folder and file naming is highly recommended. See Appendix 1C, File Naming Conventions, for more details.

**Removable media maintenance**: ESI stored on some removable media has a relatively short life expectancy. Such ESI should be transferred to another, more reliable medium to ensure its continued use and readability. CBP encourages the transfer of business relevant records, data, and information to CBP network storage in an appropriate office file plan folder structure.

**Media conversion**: Long-term, business relevant records, data, and information stored on disks/diskettes or other maturing or obsolete media should be transferred to CBP network storage.

**Storage of inactive records:** Generally, electronic records are not transferred to an FRC for retention or disposal. Contact CBP RIM for information on off-site ESI storage requirements and alternatives.

## G. Access to Electronic Records

Authorized CBP staff should be able to easily discover and retrieve ESI until its final disposition. This requirement is particularly important when an existing automated system is upgraded or replaced. Where appropriate, legacy ESI should be converted, or the new system should be designed such that these records continue to be usable until their authorized disposition date. ***Reminder: federal record retention periods are authorized by NARA. Retention of other CBP ESI is established and documented by the responsible Records Custodian in consultation with the cognizant LRIM.***

## H. Inventory of Electronic Records, Data, and Information

- Inventorying and scheduling records, data, and information in a system are the most effective ways to ensure important electronics materials are saved and disposable materials deleted when no longer needed.
- The disposition process for electronic records begins with an inventory of existing information systems, what they do, what data and information they contain, and who is responsible for them. Each office must ensure its systems inventory is kept current.
- Work with CBP RIM to use the systems inventory to gather information necessary to develop a proposed records schedule for the information in each information system.

| RIM Directive Policy #: | Part 3-H: CBP Policy Statements | Reference |
|---|---|---|
| 2.2 | CBP RIM shall ensure an inventory of all electronic systems consistent with requirements of 36 CFR 1236.26 is updated annually. | 36 C.F.R. §1236.26 |

## I. Identifying Permanent Electronic Records

Given the variety of ESI, it is impossible to compile a comprehensive list of potentially permanent electronic records. The NARA examples provided below are illustrative.

- **Permanent electronic records** that replace records scheduled as permanent in another form, such as reports or indexes.
- **Administrative data** that have unusually broad coverage or significance, such as the budgets of entire Offices.
- **Emergency operations data** that document military or civilian operations during the times of war, civil emergency, or natural disaster.
- **Political, survey, or judicial data** related to such topics as elections, special investigations, or court proceedings.
- **National security and international relations data** that document such activities as strategic or foreign policy assessments, intelligence collection, foreign public opinion, or international negotiations.

Additional examples of permanent records can be found in NARA's Disposition of Federal Records Handbook. A copy of this document may be found on the CBP RIM website.

## J. Retention of Electronic Records

- The fact that information is created or stored electronically has no bearing upon whether that information is a record or non-record.
- Record status is determined by the same criteria for all information, regardless of the medium on which it is created or stored. This is referred to as "media neutral".
- Ensuring retention of records stored electronically is not as simple as ensuring the retention of records stored on microform or paper.
- ESI can be erased or altered. This increases the risk of unauthorized destruction of federal records. Since electronic records are official federal records, they may not be destroyed without proper authorization from NARA in an approved RCS.

## K. Disposition of Electronic Records

- NARA-approved disposition schedules are required to destroy federal electronic records.
- System owners should work with RIM staff to develop proposed RCSs for all CBP electronic records or systems not covered by an approved NARA disposition schedule.
- Once approved, disposition of electronic records should follow the instructions provided in the CBP file plans.

## L. Scheduling Electronic Records

After identifying existing electronic information systems, the value of the information in each system must be determined.

**General considerations**:

- The first step in this appraisal process is to decide how long CBP needs to keep the information (and in what form) for operational, legal, administrative, or fiscal purposes. This decision requires consultation with the system owner, system users, Component LRIM(s), and CBP RIM.
- The office of primary responsibility, system managers, and users can best judge the usefulness of electronic records for current or future operations.
- NARA appraisers review retention recommendation and determine whether any of the records have enough potential value to warrant permanent preservation in the National Archives.

**The General Records Schedule (GRS)**:

- The first step in drafting a proposed RCS for the disposition of temporary electronic records is to determine whether they are already covered by the GRS. The GRS lists administrative temporary records common to most federal agencies.
- The GRS gives federal agencies the authority to dispose of such records.

## M. Electronic Mail and Messaging Systems

All CBP email and messaging accounts contain federal records. This includes email accounts with multiple users (such as public correspondence email addresses) or email accounts for an individual on multiple systems (such as classified and unclassified email accounts), text, and instant messaging, including third party applications (such as Twitter, Instagram, and Snapchat). All email and messaging created in the course of conducting CBP business is a record, and is treated like any other record. (To determine its retention period, refer to the file plans under the record category to which it pertains.)

- Users of CBP electronic mail systems will not alter or improperly dispose of any electronic mail message, record of transmission and receipt date, or attachment (such as a document) that meets the definition of a federal record received or created on these systems.
- The government email system is provided for the conduct of official DHS business. Limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services; no expectation of privacy or confidentiality applies.
- Emails, like other CBP materials, are subject to disclosure under FOIA and litigation discovery.
- In 2014, the Federal Records Act was amended to require that officers and employees may not create or send a record using a non-official electronic messaging account unless they:
    - Copy an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or
    - Forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.
- NARA guidance further requires that if an officer or employee of an executive agency receives electronic messages on a personal account, they must forward a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 calendar days after the original creation or transmission of the record.
    - All CBP employees are responsible for managing the creation and retention of documents created or transmitted on email systems.
    - Email creators and recipients must decide whether a particular message is appropriate for preservation. In making these decisions, all personnel should exercise the same judgment they use when determining whether to retain and file records in any format.
        - This does not require preservation of every email message.
        - Its purpose is to ensure preservation of those messages that contain information necessary for adequate and proper documentation of CBP policies, programs, business process transactions, and activities.

**Organizing Email**

CBP RIM recommends email be:

- Organized to separate federal records from other materials.
- Filed in a way that allows efficient discovery, access, and use.
- Identified sufficiently to enable authorized personnel to retrieve, access, protect, and execute its disposition.
- Organized in folder structures patterned after approved office file plans. See Appendix 1B, Use of Federal Enterprise Architecture – DHS File Codes, and Appendix 2, Approaches for Organizing a Shared Drive, for more information.

- More granular folders for each approved record series or file category may be established as needed, but the retention period for each folder should be included in the file name, accessible meta-data, or a persistent identifier.

See Appendix 1G, DHS Policy 142-03: Electronic Mail Usage and Maintenance, for more specific details on email roles and responsibilities.

# Part 4: Records and Information Management Training and Program Publicity

To ensure CBP RIM remains viable and is effectively executed, it is important that all CBP employees are aware of the program and have adequate training to perform the records and information management duties required. This can be accomplished by having an active and comprehensive training and a publicity program. The guidance listed below will aid you in carrying out essential training requirements.

## A. Classroom Training

- Records management training courses are available in the Washington, DC, area from the NARA, Office of Records Services.
- NARA's Office of Regional Services also offers training opportunities, both in the Washington, DC area and in the field.
- NARA publishes schedules of records management classes each fiscal year. Copies of these schedules are available by contacting your Local Records and Information Manager or at NARA's Learning Management System.

## B. Orientation Training

**All employees and contractors** receive a records management orientation briefing by records management personnel or DHS's Performance and Learning Management Systems (PALMS) records management training module.

Additionally, employees should follow the guidance in this handbook including these practices:

- Implement records management instructions issued by the RIM staff, including guidelines on records creation and procedures for capturing federal records.
- Document the substance of meetings and conversations where decisions are made, issues are resolved, or policy is established.
- Keep personal materials separate from official accounts or systems. This avoids the laborious and difficult task of reviewing voluminous materials when leaving the Agency.

**New employees and contractors** will be trained as part of an overall "new employee" orientation program or individually if the number of new staff does not warrant such a program. All CBP employees and contractors will eventually be involved with some aspect of the CBP RIM program. All individuals' instruction will include:

- The need to have and use a file plan for all materials.
- Contact information for LRIMs and Records Custodians.
- Use of GRS and CBP RCSs.
- General outline of the methods used to properly dispose of records (e.g., packaging, authorization, destruction, or transfer to a local staging area, FRC, or transfer to the National Archives and the necessary documentation).
- Differentiating between permanent and temporary records, other information, and personal materials.

- Need to inform LRIM of any necessary changes to records schedules and instructions on how to maintain and cut off files.
- Caution that if records are not identified on an approved RCS, they **may not** be destroyed and are considered permanent records until properly scheduled.

**New supervisors** will be trained as part of supervisor training or orientation. All CBP supervisors have the responsibility to:

- Manage their own records consistent with Part 4, Section B above.
- Train employees and contractors in the records management practices outlined in this Handbook and hold them accountable to adhere to those practices.

**When employees or contractors separate or are transferred:**
When leaving federal service or transferring to another assignment, CBP employees need to ensure all federal records are properly managed and preserved until their authorized disposition. Employees should contact their supervisors to determine how materials should be transferred for proper handling. In the event that an employee leaves without notice, the responsible supervisor must ensure the proper transfer and handling of the employee's records. Possible responsibilities may include ensuring records are appropriately identified and captured from:

- Email, social media, or electronic messaging accounts;
- All internal and external advisory boards, committees, or councils in which the employee participated; and
- Reports to Congress and/or the President, speeches, testimonies, or major correspondence.

Federal records must be maintained under the control of the Government. Employees generally may take extra copies of federal records that are already publicly available, or subject to review and approval. Any removal of information is subject to review by CBP officials. Approval should be granted only if all of the following conditions are met:

- Removal would not adversely affect official CBP records;
- Removal would be at no cost to CBP;
- The materials do not contain classified national security information;
- The information removed is not subject to the Privacy Act of 1974 (5 U.S.C. § 552a); and
- Disclosure of the information removed is not otherwise prohibited by law.

However, when determining whether to permit departing employees to remove copies of federal records, CBP will also consider the extent to which such removal could affect its ability to invoke specific legal privileges, and will consider use of nondisclosure agreements in appropriate cases. In those instances, CBP will also review and approve removal of personal materials to ensure that all CBP policies are followed properly.

| RIM Directive Policy #: | Part 4-B: CBP Policy Statements | Reference |
|---|---|---|
| 2.3 | CBP RIM shall ensure new and current employees have access to appropriate annual records and information training. | 36 C.F.R. §1220.34; §1222.24 |

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(E) | Provide appropriate training to new employees and annual training to current employees to ensure awareness of their responsibilities to maintain and safeguard DHS records. | |

## C. Communicating Records and Information Management

In addition to training courses and orientation sessions, other means of publicizing the program and reminding employees of their records management responsibilities should be employed including:

- **Posters and flyers**. Appropriate posters are available for display on wall or in hallways. You may request materials from CBP RIM.
- **Memoranda.** At least annually, the heads of offices should issue a memorandum reminding all employees of their records management responsibilities.
- **NARA Bulletins.** Make NARA Bulletins available to CBP employees as necessary.

## D. NARA Instructional Guide Series: Pamphlets and Guides

NARA publishes pamphlets and other publications that offer guidance pertaining to specific records management activities that can be of great value in conducting records management programs. NARA's publications can be found on their Records Management Information Page: https://www.archives.gov/records-mgmt.

# Part 5: Summary Records and Information Management Responsibilities Checklist

The following is a summary checklist of key RIM responsibilities. These steps are described in detail in Part 2, Section D of this Handbook.

- ☑ Component Office management appoints a LRIM and supports appointment of Records Custodians. See Section Part 1C, Responsibilities for more information.

Component LRIM ensures:

- ☑ Records Custodians are appointed and trained.
- ☑ Component Office business processes transactions are adequately and properly documented with appropriate records.
- ☑ Component Office data and information not subject to NARA regulations have established retention periods and are properly dispositioned.
- ☑ Employees with record responsibilities are trained in records management.
- ☑ Annual records inventory is conducted.
- ☑ Employees have access to CBP RIM Handbook.
- ☑ Records or their containers are appropriately labeled.
- ☑ Records in all media are organized by FEA – DHS File Codes.
- ☑ Standard operating procedures are followed when disposing materials.
- ☑ Timely response to FRC Notice of Eligibility for Disposal (two weeks)

# Part 6: CBP File Plans

Information contained in records is useful only if it can be accessed and retrieved. CBP File Plans have been designed to facilitate access to records and guide their authorized disposition. File plans are based on the FEA – DHS File Codes and include record retention periods and authority for disposition. CBP File Plans are available on the CBP RIM website. For the most recent version of the CBP File Plan Template, visit the OIT Process Asset Library (PAL)

(b) (7)(E)

# Part 7: Contacting CBP Records and Information Management

Contact CBP RIM at: (b) (7)(E)

# Appendix 1: Managing Electronic Records – Guides

This section will include specific future instructions for:

A. Use of Automated Tools
B. Use of FEA - DHS File Codes
C. File Naming Conventions
D. Electronic Record, Data, and Information Management requirements
E. Email Success Criteria
F. Electronic Records Transfer Formats
G. DHS Directive 142-03: Electronic Mail Usage and Maintenance

# Appendix 1A: Use of Automated Tools

RESERVED FOR FUTURE USE. Contact CBP RIM at: (b) (7)(E) for guidance.

# Appendix 1B: Use of Federal Enterprise Architecture – DHS File Codes

DHS directs that File Codes be used when describing and organizing records. The information below was taken directly from DHS guidance:

## Records File Plan - The Federal Enterprise Architecture (FEA)

### A. Background/Overview

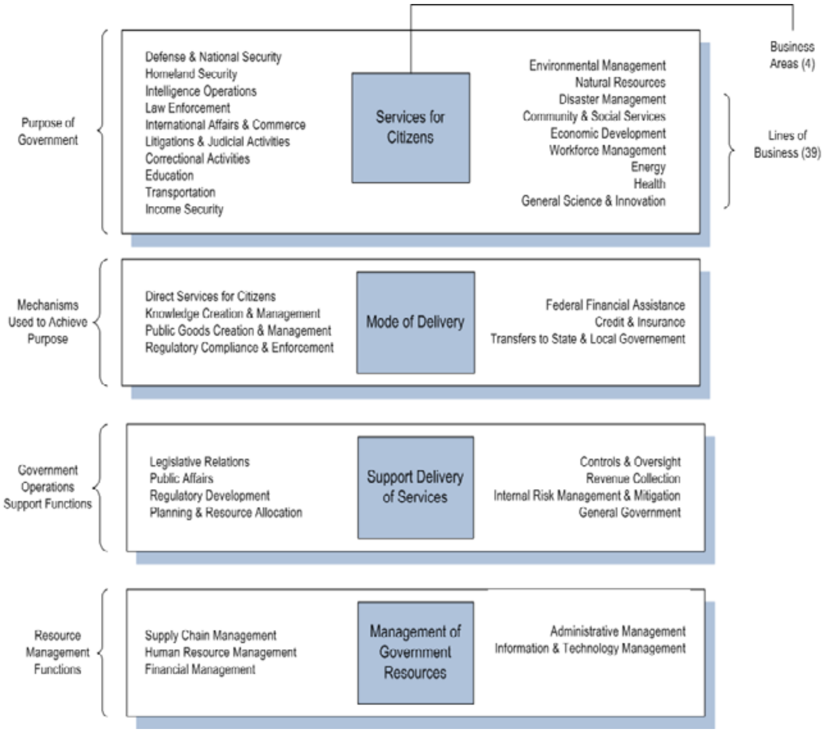
Developed collaboratively by federal agencies, the Federal Chief Information Officers (CIO) Council, and the Office of Management and Budget (OMB), FEA is a business and performance-based framework for Government-wide improvement. By describing the Federal Government around common business areas instead of by an agency-by-agency view, the Business Reference Model (BRM) promotes agency collaboration and serves as the underlying foundation for FEA and E-Government strategies.

BRM provides an organized, hierarchical construct for describing the day-to-day business operations of the Federal Government using a functionally driven (not an organizational) approach.

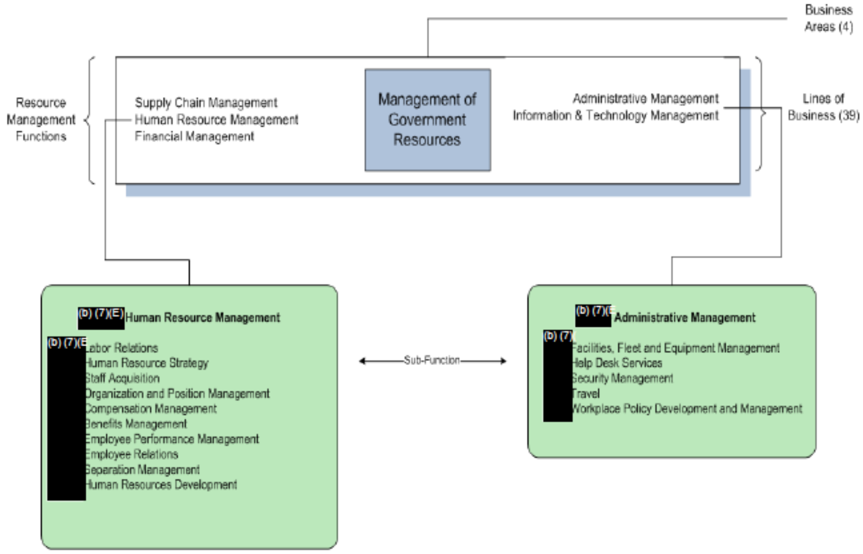
BRM is broken down into four areas:

1. Services For Citizens
2. Mode of Delivery
3. Support Delivery of Services
4. Management of Government Resources

The above four business areas are further broken into 39 Lines of Business as shown below:


Business Areas (4)
Lines of Business (39)
Purpose of Government
Defense & National Security
Homeland Security
Intelligence Operations
Law Enforcement
International Affairs & Commerce
Litigations & Judicial Activities
Correctional Activities
Education
Transportation
Income Security
Services for Citizens
Environmental Management
Natural Resources
Disaster Management
Community & Social Services
Economic Development
Workforce Management
Energy
Health
General Science & Innovation
Mechanisms Used to Achieve Purpose
Direct Services for Citizens
Knowledge Creation & Management
Public Goods Creation & Management
Regulatory Compliance & Enforcement
Mode of Delivery
Federal Financial Assistance
Credit & Insurance
Transfers to State & Local Governement
Government Operations Support Functions
Legislative Relations
Public Affairs
Regulatory Development
Planning & Resource Allocation
Support Delivery of Services
Controls & Oversight
Revenue Collection
Internal Risk Management & Mitigation
General Government
Resource Management Functions
Supply Chain Management
Human Resource Management
Financial Management
Management of Government Resources
Administrative Management
Information & Technology Management

Each Line of Business is then composed of a series of sub-functions:


Business Areas (4)
Resource Management Functions
Supply Chain Management
Human Resource Management
Financial Management
Management of Government Resources
Administrative Management
Information & Technology Management
Lines of Business (39)
(b) (7)(E) [redacted]
Human Resource Management
(b) (7)(E [redacted]
abor Relations
uman Resource Strategy
taff Acquisition
rganization and Position Management
ompensation Management
enefits Management
mployee Performance Management
mployee Relations
eparation Management
uman Resources Development
Sub-Function
(b) (7)( [redacted]
Administrative Management
(b) (7) [redacted]
acilities, Fleet and Equipment Management
elp Desk Services
ecurity Management
ravel
orkplace Policy Development and Management

The DHS File Plan number is composed of the Line of Business and Sub-Function.

## B. Identifying and Using the File Plan

To determine which file plan is assigned; determine the function of the record(s).

- ***The disposition of the record is not a factor in determining the file plan.***
- ***If you are unsure of a record's function, contact the program personnel in the program that initiated the record.***

Whether the record is electronic or hard copy; permanent or temporary; the function of the record determines the file plan.

1. The file plan will be identified in two (2) phases:
    1. First – identify the line of business; and

    2. Second – identify the appropriate sub-function within that line of business.

Example:

- Annual Reports to Congress
- Annual Statistical Reports on Immigration
- National Infrastructure Protection Plan

These reports are prepared by different DHS Components and cover various topics. The commonality between these reports is the function; the reports are created by statutory requirements to submit specified information to Congress or its committees for the purpose of legislative oversight.

.

The file plan assigned to these records is 303-100:

- **Line of Business 303 - Legislative Relations**
  Legislative Relations involves activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the federal Government.
- **Sub-Function 100 - Congressional Liaison Operations**
  Involves all activities associated with supporting the formal relationship between a federal agency and the U.S. Congress.

2. The final element of the File Plan is the Task number; this is the only part of the File Plan number that is generated by the records programs.

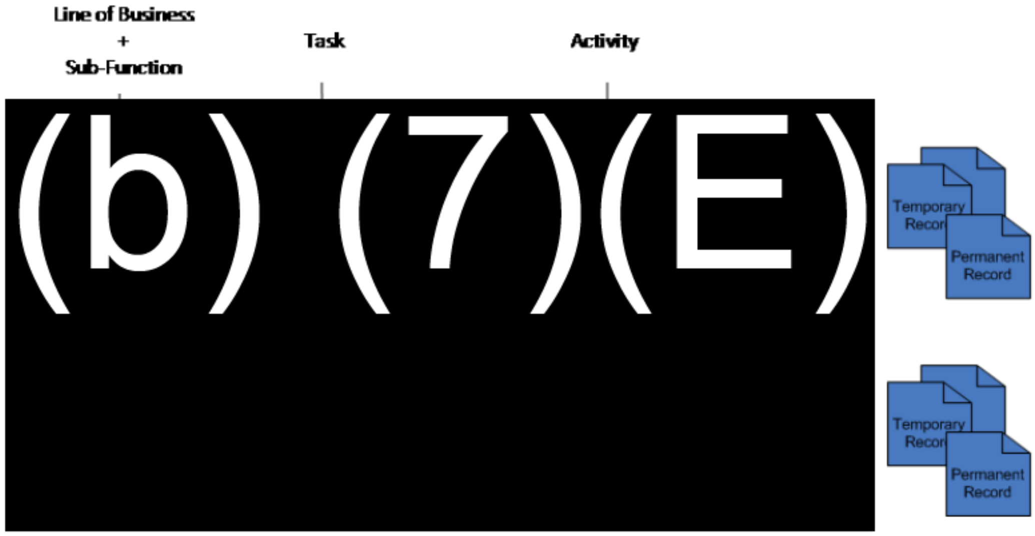
For DHS and the Support Components, the records were numbered in order by the way the records appeared alphabetically within each File Plan.

These are Support Component record and system schedules organized by File Plan. The record titles in *italics* are the DHS Record Series titles.

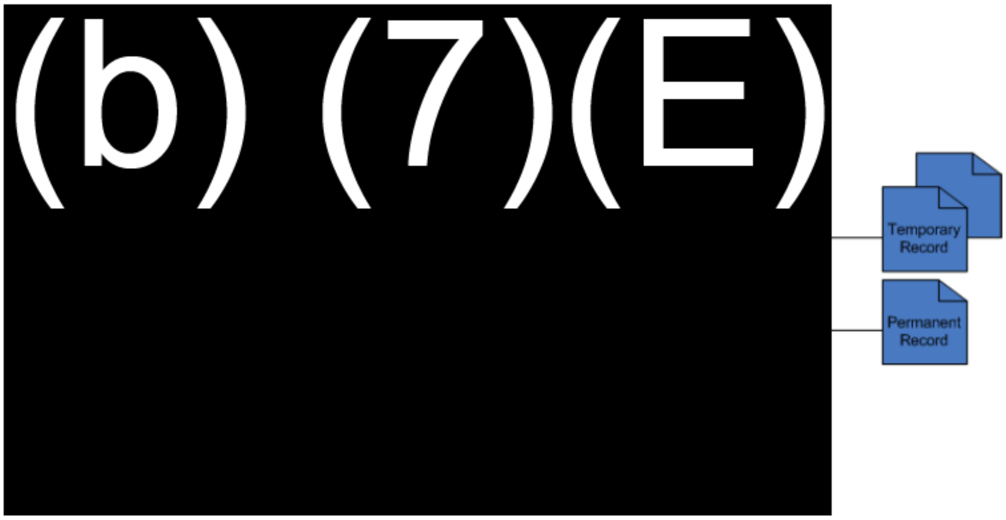
(b) (7)(E)

The final DHS file plan number contains four elements: the Line of Business, Sub-Function, Task and Activity.

Documents/Records are filed at the Activity Level or below.

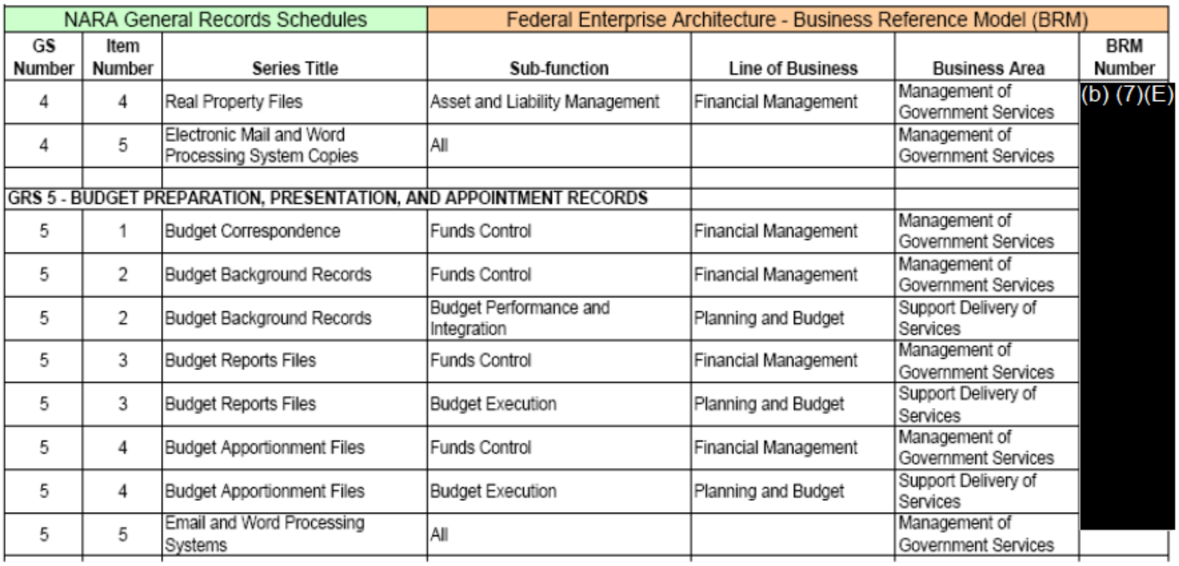


The folder under that filing level could be further broken down to cover each of the disposition statements. This step is optional, but breaking down the sub-folders will aid the user in identifying the specific documents and applying the appropriate dispositions.



On the DHS Intranet Records Management/Schedules page under the topic "DHS Records Schedules", Schedules Listed by File Plan is a complete listing of all Support Component record and system schedules organized by file plan as well as guidance and links to FEA information.

NARA has endorsed FEA; the table below shows an example of how FEA aligns to GRS[4]:



| NARA General Records Schedules | | | Federal Enterprise Architecture - Business Reference Model (BRM) | | | |
|---|---|---|---|---|---|---|
| GS Number | Item Number | Series Title | Sub-function | Line of Business | Business Area | BRM Number |
| 4 | 4 | Real Property Files | Asset and Liability Management | Financial Management | Management of Government Services | (b) (7)(E) [redacted] |
| 4 | 5 | Electronic Mail and Word Processing System Copies | All | | Management of Government Services | [redacted] |
| | | | | | | [redacted] |
| GRS 5 - BUDGET PREPARATION, PRESENTATION, AND APPOINTMENT RECORDS | | | | | | [redacted] |
| 5 | 1 | Budget Correspondence | Funds Control | Financial Management | Management of Government Services | [redacted] |
| 5 | 2 | Budget Background Records | Funds Control | Financial Management | Management of Government Services | [redacted] |
| 5 | 2 | Budget Background Records | Budget Performance and Integration | Planning and Budget | Support Delivery of Services | [redacted] |
| 5 | 3 | Budget Reports Files | Funds Control | Financial Management | Management of Government Services | [redacted] |
| 5 | 3 | Budget Reports Files | Budget Execution | Planning and Budget | Support Delivery of Services | [redacted] |
| 5 | 4 | Budget Apportionment Files | Funds Control | Financial Management | Management of Government Services | [redacted] |
| 5 | 4 | Budget Apportionment Files | Budget Execution | Planning and Budget | Support Delivery of Services | [redacted] |
| 5 | 5 | Email and Word Processing Systems | All | | Management of Government Services | |

## C. Applying the File Plan/Organizing Records

### (1) Using the File Plan on the Shared Drive:

Use your record schedule, set up the File Plan hierarchy on your shared drive.

File Plan Hierarchy

(b) (7)(E) [redacted]

Expand the top level folders to add/view the file plan sub-function(s).

[4] See Forms

(b) (7)(E)

Expand the top level folders to add/view the file plan sub-function(s).

Expand the Sub-Function folders in step 2 to create the Sub-folders created and assigned to the record types on the current DHS Records Schedule.

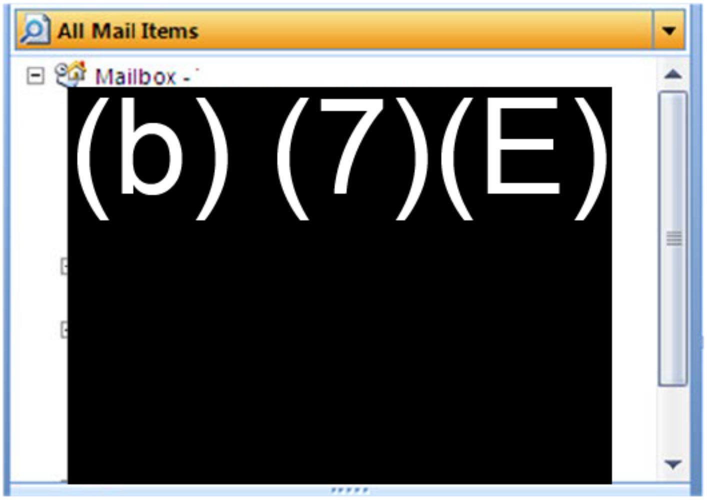
This is the level for filing electronic documents.

**D. Using the File Plan in Outlook**

Create the applicable folders in your mailbox; ***only create the folders that apply to your records***. Unlike the structure on the shared drive, it is not necessary to create a folder for every document type your Component may create. This is your mailbox for your records.

As with the shared drive, file the emails within the appropriate file plan sub-folder.

Emails and documents are filed at the Activity level or below.



(b) (7)(E)

In preparation for ERMS, use the DHS File Plan on the Outlook folder. (See the instruction in section 10 D) of this appendix for detail on how to set up Outlook folders by File Plan.)

Most users will only need to use, at most, five different file structures to identify their work process.

Drag the email and drop it into the appropriate subject folder.

### E. "My Documents" or "Shared Drive" Folder

The same process used to organize Outlook folders can be applied to "My Documents" or "shared drive" folders.

To save an individual email to a shared drive folder, open the email, select "file/save as" and select an option to save the file as html, text, outlook message format or PDF.

1. To save an individual email as a document, file the message in the appropriate subject folder on the shared drive as with any other corresponding document or report.

2. To archive an email subject folder containing multiple messages, select file/archive; in the "archive" window, highlight the folder to archive, select the date range and the location (share drive/my documents) to place the folder; this process creates the archived folder (.pst)[5] in the specified location.

[5] **Storage and Use of PST files:** Please note that CBP will no longer support the use of Outlook PST files within users OneDrive folders based on Microsoft guidance and best practices. Users may still store and utilize PST files that are local to their PC. Information on how to manage your PST files can be found in the PST Guidance for ODFB Users document. Any additional questions regarding management of PST files can be submitted to the CBP Technology Service Desk.

| DHS Policy #: | DHS Policy Statements | Reference |
|---|---|---|
| Directive 141-01(V)(D) | Maintain records according to a designated DHS file plan, which allows for retrieval across the varied DHS missions. | |
| Instruction<br>(b) (7)(E) [redacted] | Records are organized and identified across the Department through a standard filing system, the DHS-wide FEA BRM file plan. | |

# Appendix 1C: File Naming Conventions

RESERVED FOR FUTURE USE. Contact CBP RIM at: (b) (7)(E) for guidance.

# Appendix 1D: Electronic Record, Data, and Information Management Requirements

RESERVED FOR FUTURE USE. Contact CBP RIM at: (b) (7)(E) for guidance.

# Appendix 1E: Email Success Criteria

NARA established the “2016 Email Management Success Criteria” to guide CBP email management:

**2016 Email Management Success Criteria**

## 1. Purpose

OMB Circular A-130 includes a requirement that by December 31, 2016 Federal agencies must manage all email records in an electronic format and can no longer use print and file policies to manage email records. Accordingly, email records must be retained in an appropriate electronic system that supports records management and other agency business needs. In order to successfully meet the Directive’s 2016 requirement of managing email electronically, each agency must have in place applicable records schedules, agency policies, and IT systems to ensure that emails that are Federal records can be accessed, managed, and preserved until the appropriate disposition is applied.

This document and its appendices describe the existing records management requirements in statutes, regulations and NARA guidance that apply to email records. NARA views use of these success criteria as fundamental to successful electronic management of email. The appendices provide additional information on managing email records. Appendix A provides questions for agencies to review and answer with internal stakeholders. Appendix B provides an analysis of specific email management requirements as they relate to portions of the records management lifecycle.

Agencies should use this document to identify areas of strength and weakness in their current program, guide internal discussions with stakeholders, and identify any steps required to meet the 2016 email target. NARA will ask agencies questions related to the four categories of success criteria in future reporting period. NARA recognizes the complexities of email management and encourages agencies to contact us with any questions.

## 2. Success Criteria

NARA categorized the records management considerations for email into the following groups: policies, systems, access, and disposition. Agencies may have specific email management requirements that go beyond the scope of this document related to the Freedom of Information Act, Privacy Act, cyber security, security classified information, controlled unclassified information, litigation, or other requirements. Agencies that create and maintain email records containing classified national security information must manage the records in accordance with 32 C.F.R. Subtitle B Chapter XX Part 2001 and Executive Order 13526.

**Policies:** Agency-wide policies and training must inform account holders of their responsibilities for managing email records. Policies should be developed with all relevant stakeholders and should address the requirements of the Federal Records Act, 36 C.F.R. Chapter XII Subchapter B, and NARA guidance.

> *What Success Looks Like*: Your agency’s policies and training programs explain staff responsibilities for managing email records. The policies and training should instruct staff how to

distinguish between permanent, temporary, transitory, and non-record email messages and how to appropriately handle email messages containing classified national security information and those created on non- official or personal electronic messaging accounts.

**Systems:** Agencies must have systems in place that can produce, manage, and preserve email records in an acceptable electronic format until disposition can be executed. Additionally, systems must support the implementation of agency policies and provide access to email records throughout their lifecycle.

*What Success Looks Like*: Your agency's systems and business processes support the management of email records in accordance with all applicable requirements including the manual or automatic execution of their disposition whether using a Capstone-based or content-based record schedule.

**Access**: Email records must remain usable and retrievable throughout their lifecycle. Access supports an agency's ability to carry out its business functions. Access should address internal agency needs and accommodate responses to requests for information.

*What Success Looks Like*: Your agency's email records are maintained in a system that preserves their content, context and structure, protects against their unauthorized loss or destruction, and ensures that they remain discoverable, retrievable, and useable for the period specified in their retention schedule.

**Disposition:** The agency must have a NARA-approved schedule in place to be able to carry out the disposition of permanent and temporary email records – using either agency-specific schedules or General Records Schedule (GRS) 6.1: Email Managed under a Capstone Approach.

*What Success Looks Like*: Your agency has identified appropriate retention periods for email records and implemented systems and policies to support the disposition as specified in an approved records schedule.

### 3. Overview of agency responsibilities for managing email records

The Federal Records Act (FRA) and NARA's regulations require that all Federal records be appropriately managed for as long as needed. Agency-administered email accounts contain messages that meet the definition of Federal records. This includes email accounts with multiple users such as public correspondence or individual email accounts with multiple users. Agencies will need to access email of current and former employees, contractors, volunteers, and others to be responsive to information requests.

The 2014 amendments to FRA made several substantive changes that impact electronic records management. The changes include an updated definition of "record," to include all "recorded information…created, manipulated, communicated, or stored in digital or electronic form" (44 U.S.C. § 3301). FRA also added requirements for managing email records created or received in non-official and personal electronic messaging accounts (44 U.S.C. § 2911). The new requirements state employees may not create or send a record using a non-official or personal account unless they:

- copy an official electronic messaging account during the creation, receipt, or transmission of the record; or
- forward a complete copy of the record to an official electronic messaging account not later than 20 days after creation, receipt, or transmission of the record.

All persons who use agency email accounts or conduct business on behalf of the agency should be trained on their records management responsibilities related to email. In order to protect against loss, agencies should provide clear instructions on the use of personal accounts or devices.

NARA's regulations describe the requirements for managing electronic information systems that create or provide access to email (36 C.F.R. Part 1236). NARA also produces Bulletins that provide fundamental records management guidance to Federal agencies. Agencies must then determine the most appropriate ways to incorporate the requirements into their business processes and identify the specific means by which their agencies will fulfill their responsibilities.

In 2013, NARA issued Bulletin 2013-02 describing a new, role-based approach to managing email records called Capstone. In September 2014, NARA issued Bulletin 2014-06, reminding agencies of their responsibilities for managing email. In 2015, NARA released a GRS for Capstone email records. Agencies should select the approach for managing email records that best supports their business requirements and complies with relevant laws, regulations, NARA guidance, and the Directive.

Agencies must have records management controls built into electronic information systems, services, and applications in combination with appropriate policies and procedures to ensure that records:

- maintain their content, context, and structure;
- can be associated with their creators and agency;
- accurately represent the transactions, facts, or information they document;
- are protected against unauthorized alteration, deletion, or use; and
- can be located, retrieved, presented, and interpreted for business use until the NARA-approved retention period is met and disposition can be executed.

Agencies should continually evaluate and monitor their programs' management of email for compliance with all records management requirements.

The rest of M-14-16 can be found at: https://www.archives.gov/files/records-mgmt/email-management/2016-email-mgmt-success-criteria.pdf [6]

[6] Accessed 10 December 2016: https://www.archives.gov/files/records-mgmt/email-management/2016-email-mgmt-success-criteria.pdf

# Appendix 1F: Electronic Records Transfer Formats

The information below was taken directly from NARA 2014-04: Revised Format Guidance for the Transfer of Permanent Electronic Records – Appendix A: Tables of File Formats[7].

These transfer guidance format tables are organized by categories of electronic records. For each category there are tables identifying preferred, acceptable, and in some cases, acceptable for imminent transfer formats. Each format is identified by name, and the relevant specification that defines appropriate encoding methods. Many file formats, especially those used with digital audio and video, are composed of multiple parts including a wrapper, which is the file format, and an embedded encoding stream or codec. In these cases, the format category table will include a column that specifies the codec or codecs that may be used with each format. Agencies must submit electronic records in files that are valid according to both the wrapper and any specified codec standards.

## 1. Computer Aided Design (CAD)

Computer aided design (CAD) – CAD formats are vector graphics files that rely on mathematical expressions to create multi-dimensional computer graphics intended for use in engineering and manufacturing design. CAD programs can generate representations and animations of two and three-dimensional surface projections of objects.

| Preferred Formats | Format Specifications |
|---|---|
| **Extensible 3D (X3D)** | ISO/IEC 19775-1:2008:<br>( http://www.web3d.org/files/specifications/19775-1/V3.2/index.html ) |
| **Standard for the Exchange of Product Model Data (STEP)** | ISO 10303-21:2002:<br>( http://www.iso.org/iso/home/store/catalogue_tc/ catalogue_detail.htm?csnumber=33713 )<br>ISO 10303-28:2007:<br>( http://www.iso.org/iso/home/store/catalogue_tc/ catalogue_detail.htm?csnumber=40646 ) |

| Acceptable Formats | Format Specifications |
|---|---|
| **Portable Document Format/Engineering (PDF/E)** | ISO 24517-1:2008 Document management -- Engineering document format using PDF -- Part 1: Use of PDF 1.6 (PDF/E-1):<br>( http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=42274 ) |
| **Universal 3D (U3D)** | Universal 3D File Format. Standard ECMA-363. 4th edition (June 2007):<br>( http://www.ecma-international.org/publications/standards/Ecma-363.htm ) |
| **Product Representation Compact (PRC)** | Acrobat 3D PRC Specification (Version 7094):<br>( http://livedocs.adobe.com/acrobat_sdk/9/Acrobat9_ HTMLHelp/API_References/PRCReference/PRC_Format_Specification/ ) |

[7] Accessed 31 January 2019: https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html

## 2. Digital Audio

The digital audio category encompasses formats used to encode recorded sound as machine readable files by converting acoustic sound waves into digital signals. Digital audio formats are generally composed of both a wrapper format, usually the common name associated with the file extension, and an encoding method or codec.

General requirements for digital audio records:

- Digitize to standards appropriate for the accurate preservation of the original audio, when converting analog material (e.g., audio cassettes, record albums, and reel-to-reel audio tapes). Examples of appropriate methods and formats are available on NARA's Digitization Services Products and Services page;
- Transfer digital audio at a minimum of 16 bits per sample, but 24 bits per sample is encouraged; and
- Transfer digital audio at a minimum sample rate of at least 44.1 KHz, but sampling at 96 KHz is encouraged.

| Preferred Formats | Format Version | Codecs | Format Specifications |
|---|---|---|---|
| **Broadcast Wave (BWF)** | 0, 1 & 2 | Linear Pulse Code Modulated Audio (LPCM) | European Broadcast Union (EBU). Tech Specification of the Broadcast Wave Format (BWF) – Version 1: ( http://web.archive.org/web/20091229093941/http://tech.ebu.ch/ docs/tech/tech3285.pdf )<br>Specification of the Broadcast Wave Format (BWF) - Version 2: ( https://tech.ebu.ch/docs/tech/tech3285.pdf ) |
| **Free Lossless Audio Codec (FLAC)** | 1.21 | FLAC | FLAC Format Specification version 1.21: ( http://flac.sourceforge.net/format.html ) |

| Acceptable Formats | Format Version | Codecs | Format Specifications |
|---|---|---|---|
| **Audio Interchange Format (AIFF)** | 1.3 | Linear Pulse Code Modulated Audio (LPCM) | Audio Interchange File Format: "AIFF" A Standard for Sampled Sound Files Version 1.3 Apple Computer, Inc.: ( http://www-mmsp.ece.mcgill.ca/Documents/AudioFormats/AIFF/Docs/AIFF-1.3.pdf ) |

| | | | |
|---|---|---|---|
| **MPEG Audio Layer III (MP3)** | | MP3enc, Lame | ISO/IEC-11172-3 Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 3: Audio: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22412 )<br>ISO/IEC 13818-3:1995 Information technology – Generic coding of moving pictures and associated audio information – Part 3: Audio: ( http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=26797 ) |
| **Wave Waveform Audio File Format (Wave)** | | Linear Pulse Code Modulated Audio (LPCM) | Multimedia Programming Interface and Data Specifications 1.0: ( http://www-mmsp.ece.mcgill.ca/Documents/AudioFormats/WAVE/Docs/riffmci.pdf ) |

## 3. Digital Moving Images

Digital moving images consist of bitmap digital images or “frames” displayed in rapid succession at a constant rate, giving the appearance of movement. This category includes two subcategories: digital cinema which encompasses digitized film; and digital video (including both video digitized from analogue sources and born digital video).

General requirements for digital moving image records:

- Agencies must digitize to standards appropriate for accurate preservation of the original video and audio components, when converting analog material. Examples of appropriate methods and formats are available on NARA’s Digitization Services Products and Services page; and
- For reformatted video, 8-bit is acceptable but 10-bit is preferred.

### 3.1 Digital Cinema

| Preferred Formats | Format Version | Codecs | Format Specifications |
|---|---|---|---|
| **Digital Moving Picture Exchange Bitmap (DPX)** | 1 & 2 | Uncompressed | Society of Motion Picture Television Engineers. SMPTE Standard 268M-1994 (DPX Version 1.0): ( http://standards.smpte.org/ )<br>Society of Motion Picture Television Engineers. SMPTE Standard 268M-2003 (DPX Version 2.0): ( http://standards.smpte.org/ ) |

## 3.2 Digital Video

| Acceptable Formats | Format Version | Codecs | Format Specifications |
|---|---|---|---|
| **Audio Video Interleaved Format (AVI)** | | Uncompressed | Multimedia Programming Interface and Data Specifications 1.0: (http://www.kk.iij4u.or.jp/~kondo/wave/mpidata.txt ) |
| **QuickTime File Format (MOV)** | | Uncompressed 4:2:2 | Apple QuickTime File Format Specification (ISO/IEC 14496-14:2003): (https://developer.apple.com/library/mac/documentation/QuickTime/QTFF/QTFFPreface/qtffPreface.html#//apple_ref/doc/uid/TP40000939) |
| **Windows Media Video 9 File Format (WMV)** | 9 | VC-1 | Advanced Systems Format (ASF) Specification<br>Revision 01.20.03<br>Microsoft Corporation<br>December 2004:<br>(http://msdn.microsoft.com/en-us/library/bb643323.aspx )<br><br>Windows Media Video 9 encoder:<br>(http://msdn.microsoft.com/en-us/library/windows/desktop/ff819505(v=vs.85).aspx) |
| **MPEG 4** | | H.264 | ISO/IEC 14496-10:2003. Information technology -- Coding of audio-visual objects -- Part 10: Advanced Video Coding (formal name) MPEG-4, Advanced Video Coding:<br>(http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37729) |
| MPEG-2 Video (MPEG2) | | | ISO/IEC 13818-2:2000 Information technology -- Generic coding of moving pictures and associated audio information: Video:<br>(http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31539) |
| Material Exchange Format (MXF) | | J2K-losslessly-compressed | ST 377-1:2011<br>Material Exchange Format (MXF) — File Format Specification:<br>(http://standards.smpte.org/content/978-1-61482-517-3/st-377-1-2011/SEC1.abstract?sid=63bac43b-e0e1-40a3-8019-d379a103987e)<br><br>ISO/IEC 15444-1:2004Information technology -- JPEG 2000 image coding system: Core coding system: |

| | | | |
|---|---|---|---|
| | | | (http://www.iso.org/iso/ catalogue_detail.htm?csnumber=37674) |

## 4. Digital Still Images

Digital still images are files that are sampled and bitmapped as a grid of rectangular dots, picture elements (pixels) or points of color. This category encompasses two subcategories: digital photographs (digitally captured photographs or digital scans of photographic prints or negatives), and scanned text.

### 4.1 Digital Photographs

Digital photographs include still photographs of natural, real-world scenes or subjects produced by digital cameras, and scanned images of photographic prints, slides, and negatives. The guidance applies to master image files of digital photographs created using medium to high quality resolution settings appropriate for continued preservation.

General requirements for digital photographic records:

- Agencies should use appropriate, professional quality, dedicated photographic equipment when capturing images;
- When converting analog material (photographic prints, glass plate negatives, slides, etc.), agencies must digitize to standards appropriate for the accurate preservation of the original image. Examples of appropriate methods and formats are available on NARA's Digitization Services Products and Services page;
- Agencies must digitize analog originals at a minimum resolution of 3,000 pixels across the long dimension; and
- NARA prefers images that are uncompressed or which make use of lossless compression.

The requirements for digital photographic records such as aerial photography are described in section 5. "Geospatial formats". Additional special requirements for digital photographs are described in 36 C.F.R. § 1237.28.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| Tagged Image File Format (TIFF) | 4, 5, & 6 | TIFF Revision 6.0 Final — June 3, 1992 Adobe Systems Incorporated: ( http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| JPEG File Interchange Format (JFIF) with Joint Photographic Experts Group (JPEG) compression | 1.02 | ISO/IEC 10918-5 Information technology – Digital Compression and coding of continuous-tone still images: JPEG Interchange File Format: (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54989)<br>ISO/IEC 10918-1: 1994 Information technology – Digital Compression and coding of continuous-tone still images: Requirements and guidelines: (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902) |

| | | |
|---|---|---|
| Digital Negative (DNG) | 1.4.0.0 | Adobe Digital Negative (DNG) Specification Version 1.4.0.0: ( http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/products/photoshop/pdfs/dng_spec_1.4.0.0.pdf ) |
| Portable Network Graphics (PNG) | 1.2 | ISO/IEC 15948:2004 Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29581 ) |
| Jpeg2000 (JP2) | JP-Part 1 | ISO/IEC 15444-1:2004 Information technology – JPEG 2000 image coding system: Core coding system: ( http://www.iso.org/iso/catalogue_detail.htm?csnumber=37674 ) |

## 4.2 Scanned Text

Scanned text is a photograph of a printed page produced either by a digital camera or scanner.

General requirements for scanned text include the following:

- Agencies must digitize to standards appropriate for the accurate preservation of the information on the printed page. When converting analog or film based material (microfilm, microfiche, slides, etc.), agencies must digitize to standards appropriate for the accurate preservation of the original image. Examples of appropriate methods and formats are available on NARA's Digitization Services Products and Services page;
- Bitonal (1-bit black and white) images must be scanned at 300-600 ppi. Scanning at 600 ppi is recommended. This is appropriate for documents that consist exclusively of clean printed type possessing high inherent contrast (e.g., laser printed or typeset on a white background);
- Gray scale (8-bit) must be scanned at 300-400 ppi. Scanning at 400 ppi is recommended.
- This is appropriate for textual documents of poor legibility because of low inherent contrast, staining or fading (e.g., carbon copies, thermofax, documents with handwritten annotations or other markings), or that contain halftone illustrations or photographs; and
- Color (24-bit RGB [Red, Green, Blue]) must be scanned at 300-400 ppi. Scanning at 400 ppi is recommended. Color mode (if technically available) is appropriate for text containing color information important to interpretation or content.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| Tagged Image File Format (TIFF) | 4, 5, & 6 | TIFF Revision 6.0 Final — June 3, 1992 Adobe Systems Incorporated: ( http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf ) |
| Jpeg2000 (JP2) | Part 1 (JP2) | ISO/IEC 15444-1:2004 Information technology – JPEG 2000 image coding system: Core coding system: ( http://www.iso.org/iso/catalogue_detail.htm?csnumber=37674 ) |
| Portable Network Graphics (PNG) | 1.2 | ISO/IEC 15948:2004 Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification: (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=2958 ) |

| | | |
|---|---|---|
| Portable Document Format/Archival (PDF/A) | PDF/A-1 | ISO 19005-1:2005 Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1): ( http://www.iso.org/iso/catalogue_detail?csnumber=38920 ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| JPEG File Interchange Format (JFIF) with Joint Photographic Experts Group (JPEG) compression | 1.02 | ISO/IEC 10918-5 Information technology – Digital Compression and coding of continuous-tone still images: JPEG Interchange File Format: (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54989 )<br>ISO/IEC 10918-1:1994 Information technology – Digital Compression and coding of continuous-tone still images: Requirements and guidelines: (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902 ) |
| Graphics Interchange Format (GIF) | 87a & 89a | Graphics Interchange Format (sm) Version 89a: ( http://www.w3.org/Graphics/GIF/spec-gif89a.txt ) |
| PDF/A-2 | PDF/A-2 | ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2): ( http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50655 ) |

## 4.3 Digital Posters

Digital posters include both posters created digitally and scanned images of analog posters. Posters are generally large in format and usually printed and displayed for advertising and publicizing purposes.

General requirements for digital posters include the following:

- Agencies must digitize to standards appropriate for the accurate preservation of the information of the image. When converting analog or film based material (microfilm, microfiche, slides, etc.), agencies must digitize to standards appropriate for the accurate preservation of the original image. Examples of appropriate methods and formats are available on NARA's Digitization Services Products and Services page;
- Bitonal (1-bit black and white) images must be scanned at 300-600 ppi. Scanning at 600 ppi is recommended. This is appropriate for documents that consist exclusively of clean printed type possessing high inherent contrast (e.g., laser printed or typeset on a white background);
- Gray scale (8-bit) must be scanned at 300-400 ppi. Scanning at 400 ppi is recommended.
- This is appropriate for textual documents of poor legibility because of low inherent contrast, staining or fading (e.g., carbon copies, thermofax, documents with handwritten annotations or other markings), or that contain halftone illustrations or photographs; and
- Color (24-bit RGB [Red, Green, Blue]) must be scanned at 300-400 ppi. Scanning at 400 ppi is recommended. Color mode (if technically available) is appropriate for text containing color information important to interpretation or content.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| Tagged Image File Format (TIFF) | 4, 5, & 6 | TIFF Revision 6.0 Final — June 3, 1992 Adobe Systems Incorporated: ( http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf ) |
| Jpeg2000 (JP2) | Part 1 (JP2) | ISO/IEC 15444-1: 2004 Information technology – JPEG 2000 image coding system: Core coding system: ( http://www.iso.org/iso/catalogue detail.htm?csnumber=37674 ) |
| Portable Network Graphics (PNG) | 1.2 | tableISO/IEC 15948 :2004 Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=29581 ) |
| Portable Document Format/Archival (PDF/A) | PDF/A-1 | ISO 19005-1: 2005 Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1): ( http://www.iso.org/iso/catalogue_detail?csnumber=38920 ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| JPEG File Interchange Format (JFIF) with Joint Photographic Experts Group (JPEG) compression | 1.02 | ISO/IEC 10918-5 Information technology – Digital Compression and coding of continuous-tone still images: JPEG Interchange File Format: (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm ?csnumber=54989 )<br>ISO/IEC 10918-1: 1994 Information technology – Digital Compression and coding of continuous-tone still images: Requirements and guidelines: (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902 ) |
| Graphics Interchange Format (GIF) | 87a & 89a | Graphics Interchange Format (sm) Version 89a: ( http://www.w3.org/Graphics/GIF/spec-gif89a.txt ) |

## 5. Geospatial Formats

Geospatial records include digital cartographic data files and aerial photography that are created and processed in Geographic Information Systems (GIS) or other software applications for spatial analysis.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| Geospatial Tagged Image File Format | 1.8.2 | Geo TIFF Format Specification: ( http://www.remotesensing.org/geotiff/spec/geotiffhome.html ) |

| | | |
|---|---|---|
| Geographic Markup Language | 2.0 through 3.2 | ISO 19136:2007 & Version 3.2, OGC document 07-036: ( http://www.opengeospatial.org/standards/is ) |
| Topologically Integrated Geographic Encoding and Referencing Files | 2006 Second Edition | 2006 Second Edition TIGER/Line®: ( https://www.census.gov/geo/maps-data/data/pdfs/tiger/tiger2006se/tgr06se.pdf) |
| Keyhole Markup Language | 2.2 | Open Geospatial Consortium Inc. OGC 07-147r2: ( http://www.opengeospatial.org/standards/kml/ ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| Vector Product Format | | MIL-STD-2407: ( http://earth-info.nga.mil/publications/specs/printed/2407/2407_VPF.pdf ) |
| ESRI ARC/INFO Interchange File Format | | Reverse engineered specification: ( http://avce00.maptools.org/docs/v7_e00_cover.html ) |
| TerraGo Geospatial PDF | GeoPDF Encoding Best PracticeVersion 2.2 | Open Geospatial Consortium Inc. OGC 08-139r2: ( http://www.opengeospatial.org/standards/is ) |
| ESRI Shapefile (Compound) | 1997-current version | ESRI Shapefile Technical Description: ( http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf ) |

| Acceptable for Imminent Transfer Formats | Format Version | Format Specifications |
|---|---|---|
| Spatial Data Transfer Standard (SDTS) | All versions | ANSI NCITS 320-1998: ( http://mcmcweb.er.usgs.gov/sdts/standard.html) |

## 6. Presentation Formats

Presentation formats are used to convey graphical information to audiences in the form of a slide show. Presentation formats are not acceptable for use as transfer containers for permanent digital still images.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| OpenDocument Presentation Format (ODP) | 1.0 | ISO/IEC 26300: 2006 Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485 ) |
| Portable Document Format Archival (PDF/A-1) | PDF/A-1 | ISO 19005-1:2005 Electronic document file format for long-term preservation<br>– Part 1: Use of PDF 1.4 (PDF/A-1):<br>( http://www.iso.org/iso/catalogue_detail?csnumber=38920 ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| Microsoft Powerpoint 1997-2007 Binary Format (PPT) | 8.0 | [MS-PPT]: PowerPoint (.ppt) Binary File Format: (http://msdn.microsoft.com/en-us/library/cc313106(v=office.12).aspx ) |
| Microsoft Powerpoint Office Open XML Format (PPTX) | | [MS-OI29500]: Office Implementation Information for ISO/IEC 29500 Standards Support: ( http://msdn.microsoft.com/en-us/library/ee908652%28v=office.12%29 ) |
| PDF/A-2 | PDF/A-2 | ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2): (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50655 ) |

## 7. Textual Data

The textual data category refers to two general content types: unformatted (plain text) or formatted. Unformatted plain text (defined in MIME as text/plain) contains basic character information and control or non-printing characters but lacks styling information. Formatted text files include all of the attributes of plain text files but have extended formatting capabilities, for "stylized" or "rich" text features including italics, bold, colors, hyper-linking, etc.

Agencies must identify the character encoding method used with each text file.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| ASCII Text | 7 bit | ISO/IEC 646: 1991 Information technology -- ISO 7-bit coded character set for information interchange: ( http://www.iso.org/iso/catalogue_detail.htm?csnumber=4777 ) |
| Unicode Text | UFT-8<br>UTF-16 | RTF 3629: UTF-8, A Transformation Format of ISO 10646: ( http://tools.ietf.org/html/rfc3629 ) |

| | | |
|---|---|---|
| | | RFC 2781 UTF-16: An Encoding of ISO 10646: ( http://www.ietf.org/rfc/rfc2781.txt ) |
| OpenDocument Text Format (ODF) | OpenDocument 1.0 | ISO/IEC 26300:2006 Information technology -- OpenDocument Format for Office Applications (OpenDocument) v1.0: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485 ) |
| PDF/A-1 | PDF/A-1 | ISO 19005-1: 2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1): ( http://www.iso.org/iso/catalogue_detail?csnumber=38920 ) |
| PDF/A-2 | PDF/A-2 | ISO 19005-2: 2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2): ( http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50655 ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| PDF | PDF 1.7<br>PDF 1.0-1.6 | ISO 32000-1:2008 Document management -- Portable document format -- Part 1: PDF 1.7: ( http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502 )<br>Adobe® Portable Document Format Version 1.6: (http://www.adobe.com/devnet/pdf/pdf_reference_archive.html ) |
| Microsoft Word (DOCX) Office Open XML | OOXML Microsoft Word for Windows, version 2007-2010 | [MS-OI29500]: Office Implementation Information for ISO/IEC 29500 Standards Support: ( http://msdn.microsoft.com/en-us/library/ee908652%28v=office.12%29 ) |
| Microsoft Word 97 Binary Document Format (DOC) | 8.0 | [MS-DOC]: Word (.doc) Binary File Format: ( http://msdn.microsoft.com/en-us/library/cc313153%28v=office.12%29.aspx ) |

## 8. Structured Data Formats

Structured data comprises the broad category of data that is stored in defined fields. Categories for structured data are as follows:

- Database formats are organized collections of associated data that conform to a logical structure. Database formats are determined by "data models" that describe specific data structures used to model an application and generally include navigational, relational, and hybrid models;
- Spreadsheets are tables made up of columns and rows and which contain cells of data. Relationships between cells can be pre-defined as mathematical formulas;
- Statistical data is the result of quantitative research and analysis. Statistical data formats contain collections of data presented in both tabular and non-tabular form; and

- Scientific data refers to research data collected by instrumentation tools during the scientific process. Scientific data formats are either domain specific within a single field of study, or are multi-domain formats used for transfer of scientific data between domains.

General requirements for structured data include the following:

- Agencies must transfer structured data that is both well-formed according to the syntactical conventions of the format, and valid according to the structural rules defined in any associated schemas or document type definitions (DTD);
- Value Separated Files, e.g. CSV or comma separated value files, may use a character other than the comma. The pipe or caret are recommended delimiters because they are not commonly found in free text fields. Alternatively, text files encoded with ASCII characters and where each field is a fixed width, is also an acceptable transfer format for use with structured data, even though ASCII is technically a data encoding type. ASCII text files must be accompanied by complete documentation of the record lengths and field widths;
- Data files and databases shall be transferred as flat files or as rectangular tables, that is, as two-dimensional arrays, lists or tables. All records in a database, or rows (tuples) in a relational database, should have the same logical format. Each data element within a record should contain only one data value. A record should not contain nested repeating groups of data items; and
- Structured data must be transferred together with any associated files necessary to verify the validity of the data, e.g., DTDs, schemas, and data dictionaries.

| Preferred Formats | Format Version | Format Specifications |
|---|---|---|
| Comma Separated Value (CSV) | N/A | Common Format and MIME Type for Comma-Separated Values (CSV) Files: ( http://tools.ietf.org/html/rfc4180 ) |
| OpenDocument Format Spreadsheet (ODS) | | ISO/IEC 26300: 2006Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0: ( http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485 ) |
| ASCII Text | 7 bit | ISO/IEC 646:1 991 Information technology -- ISO 7-bit coded character set for information interchange: ( http://www.iso.org/iso/catalogue detail.htm?csnumber=4777 ) |
| JavaScript Object Notation (JSON) | | The application/json Media Type for JavaScript Object Notation (JSON): ( http://www.ietf.org/rfc/rfc4627.txt?number=4627 ) |
| Extensible Markup Language (XML) | 1.1 | Extensible Markup Language (XML) 1.1 (Second Edition): ( http://www.w3.org/TR/2006/REC-xml11-20060816/ ) |

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| Microsoft Excel Office Open XML | OOXML Workbook Excel | [MS-OI29500]: Office Implementation Information for ISO/IEC 29500 Standards Support: ( http://msdn.microsoft.com/en-us/library/ee908652%28v=office.12%29 ) |

| | | |
|---|---|---|
| | 2007-2010 XLXS<br>Microsoft Excel for Windows, version 2007 | |
| Microsoft Excel 97 Binary Document Format (XLS) | Version 8.0 | [MS-XLS]:  Excel Binary File Format (.xlsx) Structure: ( http://msdn.microsoft.com/en-us/library/cc313154(v=office.12).aspx ) |

| Acceptable for Imminent Transfer Formats | Format Version | Format Specifications |
|---|---|---|
| Extended Binary Coded Decimal Interchange Code (EBCDIC) | U.S. EBCDIC | IBM EBCDIC Code Page 0037: ( http://www-01.ibm.com/software/globalization/cp/cp00037.html ) |

## 9. Email

Email is defined as discrete electronic communications transmitted over the Simple Mail Transfer Protocol (SMTP), between two or more people or entities, in compliance with applicable IETF's Request for Comments (RFC) specifications.  Email does not include other functions commonly available via email programs such as calendars, tasks, appointments, newsgroups, or instant messaging. In order for information in a calendar, contact list, address book etc. to be transferred to NARA, it must be scheduled as a separate item.

Please note that NARA considers email attachments to be a component of the email record and does not require that unseparated email attachments meet the transfer standards specified by the format category under which the attachment alone would fall.

General requirements for email:

- Transfers of email records must consist of an identifiable, organized body of records (not necessarily a traditional series);
- Email messages should include delimiters that indicate the beginning and end of each message and the beginning and end of each attachment, if any.  Each attachment must be differentiated from the body of the message, and uniquely identified;
- Email messages transferred as XML files must be accompanied by any associated document type definitions (dtds), schemas, and/or data dictionaries;
- Labels to identify each part of the message (Date, To [all recipients, including cc: and bc: copies], From, Subject, Body, and Attachment) including transmission and receipt information (Time Sent, Time Opened, Message Size, File Name, and similar information, if available).  To ensure identification of the sender and addressee(s), agencies that use an email system that

identifies users by codes or nicknames, or identifies addressees only by the name of a distribution list should include information with the transfer-level documentation; and

- Email converted to formats not natively used by the email program, and which do not maintain header information (such as RTF or Word documents) are not accepted. Printouts of emails are also not accepted under this Bulletin.

| Preferred Formats for Individual Messages | Format Version | Format Specifications |
|---|---|---|
| Internet Message Format (EML) | | Internet Message Format:<br>( http://www.ietf.org/rfc/rfc2822.txt )<br><br>And MIME:<br>( http://tools.ietf.org/html/rfc2045 ),<br>( http://tools.ietf.org/html/rfc2046 ),<br>( http://tools.ietf.org/html/rfc2047 ),<br>( http://tools.ietf.org/html/rfc4288 ),<br>( http://tools.ietf.org/html/rfc4289 ),<br>( http://tools.ietf.org/html/rfc2049 ) |
| MBOX Email Format (MBOX) | | MBOX Email Format:<br>( https://tools.ietf.org/html/rfc4155 )<br><br>And MIME:<br>( http://tools.ietf.org/html/rfc2045 ),<br>( http://tools.ietf.org/html/rfc2046 ),<br>( http://tools.ietf.org/html/rfc2047 ),<br>( http://tools.ietf.org/html/rfc4288 ),<br>( http://tools.ietf.org/html/rfc4289 ),<br>( http://tools.ietf.org/html/rfc2049 ) |

| Acceptable Formats for Individual Messages | Format Version | Format Specifications |
|---|---|---|
| Extensible Markup Language (XML) | 1.1 | Extensible Markup Language (XML) 1.1 (Second Edition):<br>( http://www.w3.org/TR/2006/REC-xml11-20060816/ ) |
| Microsoft Outlook Item Message Format (MSG) | | Microsoft Outlook Item Message Format:<br>( http://msdn.microsoft.com/en-us/library/cc463912(v=exchg.80).aspx ) |

| Preferred Formats for Aggregations of Email | Format Version | Format Specifications |
|---|---|---|
| Microsoft Personal Folders Format (PST) | | Outlook Personal Folders File Format:<br>( http://msdn.microsoft.com/en-us/library/ff385210%28v=office.12%29.aspx ) |

| | | |
|---|---|---|
| MBOX Email Format (MBOX) | | MBOX Email Format:<br>( https://tools.ietf.org/html/rfc4155 )<br><br>And MIME:<br>( http://tools.ietf.org/html/rfc2045 ),<br>( http://tools.ietf.org/html/rfc2046 ),<br>( http://tools.ietf.org/html/rfc2047 ),<br>( http://tools.ietf.org/html/rfc4288 ),<br>( http://tools.ietf.org/html/rfc4289 ),<br>( http://tools.ietf.org/html/rfc2049 ) |

## 10. Web Records

Web records consist of web sites and social media sites created and maintained to provide information and services of the United States Government via the World Wide Web. This Bulletin applies to web records managed by an agency that have been appraised and scheduled for permanent retention by NARA. Agencies should harvest websites using a utility that will package component files in a manner that meets the following general requirements.

General requirements for web content records:

- Web records must be accessible via Hypertext Transfer Protocol (HTTP) from a server to a client browser when a URL has been activated;
- Web content records that share a domain name including content managed under formal agreement and residing on another site must be transferred together;
- All component parts of web content records that have been appraised as permanent including image, audio, video and all other proprietary formats, must be transferred in a manner that maintains all of the original links, functionality and data integrity;
- Dynamic content such as calendars or databases either must be transferred in an acceptable format, or be made accessible as static content;
- All internally referenced URLs must be included with the transfer set; and
- All control information from the harvesting protocol must be maintained.

The following will not be accepted for transfer under this Bulletin:

- Program or administrative records documenting the management of web sites;
- Externally referenced content (e.g., accessed via hyperlink) that resides in a different domain and is not managed for an agency under a formal agreement;
- Static images, (such as screen shots), of web content records, because they do not retain hypertext functionality.

| Acceptable Formats | Format Version | Format Specifications |
|---|---|---|
| Web ARChive Format (WARC) | .18 | ISO 28500: 2009 Information and documentation -- WARC file format:<br>( http://www.iso.org/iso/catalogue_detail.htm?csnumber=44717 ) |
| Archive File Format (ARC) | 1.0 | Arc File Format:<br>( http://archive.org/web/researcher/ArcFileFormat.php ) |

# Appendix 1G: DHS Directive 142-03: Electronic Mail Usage and Maintenance

**Department of Homeland Security DHS Directives System**

**Directive Number: 142-03**
**Revision Number: 00**
**Issue Date: 01/19/2018**

## ELECTRONIC MAIL USAGE AND MAINTENANCE

## I. Purpose

This Directive establishes the Department of Homeland Security (DHS) policy regarding electronic mail (e-mail) usage and maintenance.

## II. Scope

A. This Directive applies throughout DHS and applies to all DHS E-mail users.

B. Management Directive (MD) 4500.1, "DHS E-Mail Usage," is hereby cancelled.

## III. Authorities

A. Title 5, United States Code (U.S.C.), Section 552, "Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings"

B. Title 5, U.S.C., § 552a, "Records Maintained On Individuals"

C. Title 5, U.S.C., §§ 7501-7543, "Adverse Actions"

D. Title 18, U.S.C., § 2071, "Concealment, Removal, or Mutilation Generally"

E. Title 44, U.S.C., §§ 2901-2911, "Records Management by the Archivist of the United States and by the Administrator of General Services," Chapter 31, "Records Management By Federal Agencies," and Chapter 35, "Coordination of Federal Information Policy"

F. Title 5. Code of Federal Regulations (CFR), Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch"

G. Title 36, CFR, Parts 1220-1249, “Records Management”

H. Office of Management and Budget (OMB) and National Archives and Records Administration (NARA) M-12-18, “Managing Government Records Directive”

I. OMB and NARA M-14-16, “Guidance on Managing E-mail”

J. DHS Delegation 04000, “Delegation for Information Technology”

K. DHS Directive 141-01, “Records and Information Management”

L. DHS Directive Policy 4300A, “DHS Sensitive Systems”

M. DHS MD 4600.1, “Personal Use of Government Office Equipment”

# IV. Responsibilities

A. The ***<u>DHS Chief Information Officer (CIO):</u>***

1. Issues guidelines on the security, accessibility, retention, and use of e-mail within the Department;

2. Defines standards for DHS e-mail systems ensuring interoperability and interconnectivity;

3. Defines special configurations and processes for Department-wide services;

4. Manages and maintains the DHS Directory Services/E-mail System, including managing and maintaining anti-virus software for e-mail systems;

5. Provides the DHS standard e-mail server and client applications; and

6. Ensures retention of e-mail records in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed, as well as provide the technical means to transfer e-mail records deemed permanent federal records.

B. The ***<u>DHS Chief Records Officer:</u>***

1. Maintains a list of names and dates of tenure of DHS Capstone Officials, ensuring Capstone Officials’ e-mail records are designated as permanent records;

2. In coordination with the DHS CIO and CIO counterparts, prepares and approves the transfer of permanent e-mail records to NARA for accession in accordance with approved records schedules and existing preservation obligations;

3. Conducts periodic reviews of all e-mail systems to identify electronic records and ensure the records are scheduled;

4. Establishes a training program for employees that provides for the management of electronic messages as records; and

5. Reports annually to the DHS CIO on the management of both permanent and temporary e-mail records in an electronically accessible format. This report is submitted annually to OMB and NARA by the DHS Chief Records Officer.

C. The ***Component Heads***:

1. Ensure development and implementation of Component-specific policies for approved and prohibited uses of e-mail that are consistent with this Directive;

2. Ensure that all e-mail records are maintained in accordance with applicable records retention schedules;

3. Ensure appropriate security for their e-mail systems is provided; and

4. Ensure that all Component employees have been provided training or written instructions appropriate to their role and responsibilities for the Component under this Directive, including approved and prohibited use of Component e-mail.

D. ***Component Chief Information Officers:***

1. Work with the DHS CIO and Component Records Managers/Officers to provide tools and approaches to maintain e-mail for the required retention period;

2. Ensure that Component processes allow for removal of non-record and personal e-mail records;
and

3. Retain e-mail records in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify and retrieve records as well as provide the technical means to transfer e-mail records deemed permanent federal records in accordance to NARA standards; and

4. Ensure that Component processes allow for the required disposition of temporary e-mail records.

E. ***DHS E-mail Users:***

1. Comply with the provisions of DHS Directive 141-01 and this Directive;

2. Use only DHS-issued e-mail accounts to send and receive DHS business-related communications;

3. Follow Department and Component policies and procedures for appropriate use of DHS e-mail systems, including the accurate and timely designation of the record status of an e-mail; and

4. Consult upon request with appropriate personnel (e.g., Freedom of Information Act Officials, Privacy Officers, security managers, Records Management Officials, legal staff, etc.) on e-mail issues.

# V. Policy and Requirements

It is the policy of the Department to manage e-mail messages pursuant to NARA Bulletin 2013-02, “Guidance on a New Approach to Managing Email Records,” also known as “Capstone.” The Capstone approach aims to improve the management of e-mail records by simplifying and automating it in an electronic recordkeeping system.

This Directive applies to Departmental and Component communications that are federal records whether the applications are hosted by DHS or hosted on non-DHS servers.

A. ***Under this policy, DHS:***

1. Manages all e-mail messages electronically, in a manner that complies with applicable law, policy, OMB, and NARA guidance;

2. Manages e-mail messages based upon the account holder’s position in the Department, rather than the specific content of individual e-mail messages;

3. Designates e-mail messages of specific account holders (“Capstone Officials”) as permanent records;

4. Preserves e-mail messages that are designated as permanent records for transfer to NARA in approved format and in accordance with federal regulations; and

5. Manages e-mail messages of account holders who are not Capstone Officials as temporary records, to be preserved in accordance with approved records retention and disposition policies.

B. ***Non-DHS E-Mail Accounts*** (per DHS Directive Policy 4300A):

1. DHS employees may not use non-DHS e-mail accounts to create or send e-mail records that constitute DHS records. In case of an emergency, employees may use a non-DHS e-mail account, but thereafter must ensure the e-mail record is submitted to an official DHS e-mail account within 20 days and removed from the non-email account once the employee has ensured the capture of e-mail information.

2. DHS employees who are on detail to another agency may use that agency’s e-mail system to send e-mail records during the course of their detail. This permission also extends to task force, working group, or other project or application-based e-mail accounts established by another federal agency for use by DHS employees.

3. Auto-forwarding or redirecting of DHS e-mail to any e-mail address outside of the .gov or .mil domain is prohibited. DHS employees may manually forward individual messages after determining that the risks or consequences are minimal.

# VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer.

# Appendix 2: Approaches for Organizing a Shared Drive[8]

This appendix is an outline for developing a Shared Drive clean-up/organization project.

**Task** | **Description**

**Plan project**

Developing a project plan:

- Develop communications plan
- Identify shared drives to be organized
- Identify and procure necessary services and technologies
  - Conduct market survey
  - Interview vendors
  - Prepare Statement of Work (SOW)
- Conduct pilot to test process and develop rules for deployment
- Document pilot lessons learned

**Identify key stakeholders – establish roles and responsibilities**

Involve stakeholders:

- Senior management – project champions
- RIM staff – ensure RIM policies and process compliance
- Information technology staff – manage network operations, information security, and helpdesk services
- SMEs and end-users – provide information about existing content
- Chief Counsel's Office, Privacy Act and FOIA staff – ensure internal controls prevent deletion of content responsive to litigation holds and information requests

**Assess current state of shared drive**

Organization of shared drives involves analysis of current shared drive structure and practices:

- Review IT platforms, enterprise architecture, and security requirements to understand impacts on project
- Collect data regarding current status:
  - Number of shared drives within the organization
  - Volume of content stored on each shared drive
  - Directory structure of each shared drive
  - File types and formats found on shared drives
  - File dates, such as date created or last modified
- Identify pending IT plans that may impact project, such as planned migration, consolidation, or technology refreshes
- Identify and review current internal controls, such as naming conventions, version management, file plans, and applied metadata
- Interview SMEs and stakeholders to understand shared drive use

**Identify unwanted content**

Apply rules and queries to identify unwanted content, such as:

[8] Adapted from NARA https://www.archives.gov/records-mgmt/bulletins/2012/2012-02.html

| | |
|---|---|
| | • System-generated backup files, temp files, old applications, and old install files<br>• Multiple copies that contain identical content and may be in different formats<br>• Digital photos and videos that could be stored in another location or on other media<br>• Personal files with no business value |
| **Review and remove unwanted content** | Work with SMEs to review and remove unwanted content:<br>• Establish deadlines for file reviewing<br>• Schedule group meetings to review files<br>• Document lessons learned to assist in developing future policies and processes |
| **Manage remaining content** | Work with SMEs to identify to review remaining content:<br>• Identify records<br>• Apply appropriate disposition authorities<br>• File related records appropriately (e.g., case files, disposition authorities, etc.)<br>• Develop a standardized folder/directory structure that implements approved office-level file plan<br>• Add more granular folders as necessary.<br>• Implement file naming conventions as appropriate<br>• Execute disposition actions in accordance with NARA-approved schedules |
| **Develop day-forward policies and processes** | Develop policies and processes to maintain organized shared drives:<br>• Configure network to attribute file properties correctly<br>• Develop maintenance strategies (e.g., running periodic queries and reports, annual clean-up day)<br>• Implement folder structure and naming conventions<br>• Develop written guidance and reference materials for shared drive users<br>• Provide staff training on the proper use of shared drives<br>• Include shared drives in internal records program reviews<br>• Establish clear roles and responsibilities for shared drive maintenance as staff separate or move to different roles. |

# Appendix 3: Transferring Records to a Federal Records Center (FRC)

CBP RIM will prepare an SF-135 for transferring records to FRC for the Program Office. Direct questions or concerns to: (b) (7)(E)

**Note:** Generally, temporary electronic records are not transferred to an FRC for retention or disposal. Contact CBP RIM for information on off-site ESI storage requirements and alternatives. Acceptable formats for permanent electronic records transferring to NARA are located in Appendix 1F.

**Successful transfer of materials to a FRC requires the Program Office to complete these actions:**

1. Separate the records by series.
   a. Handle each record series as a separate transfer.
   b. Mixed series may only be transferred in one box if their disposition date is the same.
   c. Only one closing year date for a series of records is allowed.
   d. Records must be in file folders and labeled.
2. Pack the boxes, leaving a 1-to-2-inch space for ease of reference. Each transfer must consist of at least one box.
3. Boxes **cannot contain mixed media** (e.g., compact disks, paper, microfilm, etc.)
4. Do not write on the boxes until the transfer is approved and you're instructed to do so by CBP Records Management.
5. Prepare a box listing (inventory).
6. Prepare the request in Archives and Records Centers Information System (ARCIS). For more guidance on using ARCIS, including instructions on how to obtain access, see CBP RIM website.
7. Once the request is complete, submit it for approval using ARCIS.
8. If the request is approved, the CBP RIM Team will submit it to NARA for their approval, using ARCIS.

a If the request is **not** approved, the CBP RIM Team will return it to you using ARCIS along with instructions on what needs to be corrected.

9. Once approval has been received from NARA, a copy of the SF-135 will be returned to you by the CBP RIM Team.
10. Place a copy of the approved SF-135 and box listing inside each box.
11. Prepare boxes for transfer by writing the transfer number and box number on each box using a black permanent marker.
12. Contact the FRC and arrange for the shipment and pallet delivery (if needed). The FRC location can be found on the approved SF-135.
13. Send the email shipping date to (b) (7)(E) Also, provide the date the items will be transferred to FRC.
14. Once the shipment is complete, NARA will update ARCIS with the location information at FRC.

# Appendix 4: Detailed Legislative and Regulatory References

The Federal Records Act US CODE: Title 44, CHAPTER 31—RECORDS MANAGEMENT BY FEDERAL AGENCIES and the relevant requirements of Title 36, Code of Federal Regulations (C.F.R.), 1220 through 1239, contain the statutory and regulatory requirements for all federal records management programs. NARA administers the records management program for the Federal Government. NARA's regulations on records creation, maintenance, and disposition are set forth in Subchapter B of 36 Code of Federal Regulations Chapter XII.

Agencies are required to integrate records management into the overall information resources management program (36 C.F.R. § 1222 and OMB Circular A-130, *Management of Federal Information Resources*). The controlling statutes, regulations, and OMB circulars appear below:

## United States Code:

**5 U.S.C. Chapter 5, Subchapter II** – Administrative Procedure

- § 552. Public information; agency rules, opinions, orders, records, and proceedings (Freedom of Information Act, as amended)
- § 552a. Records maintained on individuals (Privacy Act of 1974, as amended)
- § 553. Rulemaking (Administrative Procedures Act)

**18 U.S.C. Chapter 101** – Records and Reports

- § 2071. Concealment, removal, or mutilation generally

**40 U.S.C. Subtitle III** – Information Technology Management (Clinger-Cohen Act of 1996)

**44 U.S.C. Chapter 21** – National Archives and Records Administration

**44 U.S.C. Chapter 29 –** Records Management by the Archivist of the United States and by the Administrator of General Services

**44 U.S.C. Chapter 31 –** Records Management by Federal Agencies (Federal Records Act)

**44 U.S.C. Chapter 33 –** Disposal of Records (Federal Records Disposal Act)

**44 U.S.C. Chapter 35 –** Coordination of Federal Information Policy (Paperwork Reduction Act of 1980, as amended; Paperwork Reduction Reauthorization Act of 1995; E-Government Act of 2002, and Government Paperwork Elimination Act)

## Code of Federal Regulations:

**5 C.F.R. Chapter III, Subchapter B – OMB Directives**

- Part 1320. Controlling Paperwork Burdens on the Public

**36 C.F.R. Chapter XII, Subchapter B – Records Management**

- Part 1220. Federal Records; General

- Part 1222. Creation and Maintenance of Records
- Part 1223. Managing Vital Records
- Part 1224. Records Disposition Program
- Part 1225. Scheduling Records
- Part 1226. Implementing Disposition
- Part 1227. General Records Schedule
- Part 1228. Loan of Permanent and Unscheduled Records
- Part 1229. Emergency Authorization to Destroy Records
- Part 1230. Unlawful or Accidental Removal, Defacing, Alteration or Destruction of Records
- Part 1231. Transfer of Records from the Custody of One Executive Agency to Another
- Part 1232. Transfer of Records to Records Storage Facilities
- Part 1233. Transfer, Use, and disposition of Records in a NARA Federal Records Center
- Part 1234. Facility Standards for Records Storage Facilities
- Part 1235. Transfer of Records to the National Archives of the United States
- Part 1236. Electronic Records Management
- Part 1237. Audiovisual, Cartographic, and Related Records Management
- Part 1238. Microform Records Management
- Part 1239. Program Assistance and Inspections

## OMB Circulars:

- **OMB Circular A-123 –** Management's Responsibility for Internal Control
- **OMB Circular A-130 –** Management of Federal Information Resources

## Executive Orders:

- **Executive Order 10346 –** Preparation by Federal Agencies of Civil Defense Emergency Plans
- **Executive Order 12656 –** Assignment of Emergency Preparedness Responsibilities
- **Executive Order 13231 –** Critical Infrastructure Protection in the Information Age

## Presidential Memorandum:

- **Managing Government Records** dated Nov 28, 2011

## Implementing Directives:

- **OMB M-12-18 –** Managing Government Records Directive
- **OMB M-14-16 –** Guidance on Managing Email

## DHS Policy:

- **Directive 141-01 –** Records and Information Management Directive
- **Directive 141-03 –** Electronic Records Management Updates for Chat, Text, and Instant Messaging
- **Directive 142-03 –** Electronic Mail Usage and Maintenance
- **Instruction 141-01-001 –** Records and Information Management Instruction

## CBP Policy:

- **Directive 2120-010 –** Privacy Policy, Compliance, and Implementation
- **Handbook 1400-05D –** Information Systems Security Policies and Procedures

# Appendix 5: Reporting Unauthorized Disposal of Federal Records

CBP employees must promptly report unauthorized disposition of federal records, including unlawful or accidental destruction, defacement, alteration, or removal from federal custody. See Federal Regulations at 36 C.F.R. § 1230. Prompt reporting is important to ensure appropriate steps are taken to recover the records, if possible. CBP is legally required to report missing or destroyed records to NARA as soon as possible.

Unauthorized disposition of federal records is against the law (44 U.S.C. § 3106) and may lead to a $2,000 fine, a three-year imprisonment, or both (18 U.S.C. § 2071); termination from federal employment; and permanent disqualification from holding any office under the United States.

To report unauthorized disposition (e.g., loss, destruction, removal, defacement, or alteration) of federal records, please contact CBP RIM at (b) (7)(E) and provide the following information:

- A complete description of the records, along with volume and dates, if known.
- The office of origin.
- An explanation of the exact circumstances surrounding the unauthorized action, including names and titles of any persons having relevant information.
- Details, when appropriate, of the actions taken to salvage, retrieve, or reconstruct the records.

CBP RIM will notify NARA and DHS RIM Program Office of the incident.

# Appendix 6: Retrieval of Records from a Federal Records Center (FRC)

The Component Office must use ARCIS to retrieve records from an FRC. The following information is necessary:

1. Record group (ARCIS will default to "568" unless requested to do otherwise)
2. Nature of service (ARCIS will default to "Temporary Loan of Records" unless requested to do otherwise)
3. Service level (ARCIS will default to "Standard" unless requested to do otherwise)
4. Transfer number (formerly accession number)
5. Container number(s) (box number(s))
6. Case file/information, including folder name/number. Indicate "whole container", if applicable
7. Security classification
8. Security level
9. Charge account number
10. Location of FRC (choose the location from the dropdown menu)
11. Complete name, address, telephone number, and email address for the agency employee receiving records.

A reference request number will be automatically generated by ARCIS.

For any records requested under the provisions of the FOIA, Privacy Act, or due to congressional interest, note the applicable reason in the "Comments" section of the OF-11 in ARCIS. This section may also be used for any other clarifying remarks deemed appropriate.

# Appendix 7: Maintaining Analog Audiovisual Records

This appendix from NARA guidance provides instructions for maintaining analog audiovisual records as may be required by the record's retention requirements.

Audiovisual records[9] are among the most fragile record forms, and adverse storage conditions hasten their deterioration. Placing them in close contact with some materials causes deleterious chemical reactions. Mishandling and other abusive treatment can damage them beyond repair, causing catastrophic loss of valuable information.

Many federal agencies are unable to establish programs that meet archival standards for the preservation of audiovisual records. Such programs require optimum storage conditions, specialized processing facilities, and professional archivists. Nonetheless, agencies should employ safeguards and procedures that will protect audiovisual records from damage.

## Storage Conditions

Poor storage conditions for audiovisual records impede their preservation. High relative humidity (for example, above 60 percent) encourages the growth of mold and other fungi on film-based materials, whose binders are derived from organic compounds. High relative humidity also causes oxidation of silver content in film and metal compounds in audio and video tape. In addition, it causes deterioration of the oxide coating on magnetic tapes, leading to clogged magnetic tape heads and scratched tapes. Warm temperatures tend to accelerate undesirable chemical and physical changes in audiovisual records (including x-ray photographs), such as shrinkage of film materials, embrittlement, separation of film base and emulsion, and fading of color film images.

In recent years, preservationists have become increasingly concerned about the longevity of a major class of safety film composed of cellulose-acetate. Several scientific studies have independently shown how adverse storage conditions create a form of hydrolysis in acetate-based film that develops free acid and the emission of acetic gas, leading to the total degradation of the film. Identified as the "vinegar syndrome," this destructive chemical process potentially affects all forms of acetate film.

Polyester-based film, widely used for sheet film since the 1970s, is much less prone to self-destructive tendencies because the base resists chemical and physical changes, although the emulsion is still vulnerable to damage from excessive heat, humidity, and harmful gases. Nonetheless, when there is a choice such as in motion picture stocks, polyester is preferable to cellulose triacetate because of its superior long-term stability.

The fading of color film images is also of great concern. Color dyes, made of organic materials, are not permanent. Heat, humidity, and exposure to light accelerate color dye fading, resulting in the discolored images that may be found in many older collections. Cold storage below freezing combined with low relative humidity effectively retards color fading.

[9] Accessed 12 December 2016 12:33PM from: https://www.archives.gov/records-mgmt/publications/managing-audiovisual-records.html

Pollutant gases in urban or suburban environments are potentially harmful as are off-gases from newly painted rooms, new furniture or flooring, and chemical storage areas.  Agencies should store audiovisual records in areas not subject to gases and fumes.

Providing proper storage conditions for audiovisual materials is a complex problem, one that probably cannot be fully solved in the facilities available to most agencies.  Nevertheless, audiovisual records (including x-ray photographs) should not be stored where the temperature exceeds 72 degrees Fahrenheit and the relative humidity is higher than 50 percent.  Even cooler and drier storage conditions are desirable to increase the life expectancy of audiovisual records.  The storage environment should be cool and dry and relatively free from harmful gases.

### Storage Enclosures

Choosing the right storage enclosure or container helps to lengthen the useful life of audiovisual records. Agencies should store still-picture negatives and long-term x- ray photographs in acid- and peroxide-free envelopes or sleeves.  Archival storage containers made of polypropylene, polyethylene, or noncorroding metal for originals or master copies of roll film, open-reel sound recordings, and video cassettes are commercially available; NARA encourages their use for permanent and long-term records.

### Storage Practices

Agencies should ensure that storage areas for audiovisual records are protected against unauthorized access and damage from fire, water, chemicals, insect infestation, or other potentially harmful conditions.  Originals, masters, and access or reference copies of audiovisual records all should be stored separately and, if necessary, off-site.  The greater the separation of these different sets, the greater the chance of survival of at least one copy after a catastrophe.  Separation also reduces errors in retrieving copies for use.

Audiovisual records that do not constitute discrete series in themselves (for example, audio or video cassettes in case files) should be removed, appropriately cross-referenced, and stored where environmental conditions will provide the most benefit.  Still photographs, however, interfiled with documents should be left in place.

### Handling Practices

Only experienced staff with requisite skills should handle original and master copies of audiovisual records. In addition, equipment for projection or playback of audiovisual records should be in good working order, properly cleaned in areas that touch the film or tape, and used only in rooms that are free from dust and other particulate matter.

Copies should be made to fill loan requests.  Loans of permanent or unscheduled records to nonfederal recipients require prior written approval from NARA (36 C.F.R. § 1228.72).  However, NARA approval is not required for loan of non-record copies.  NARA recommends that agencies lend only reference copies to other federal agencies.  If an agency loans original records, the agency should require that appropriate storage and handling procedures are followed.  In addition, the agency should set a specific time period for the duration of the loan and follow up with the recipient to ensure that the records are returned.

Every effort should be made to prevent accidental or deliberate erasure or alteration of magnetic recordings. The record mode on players should be disengaged or the record button or tab at the bottom or on the spine of cassettes should be removed. Although accidental erasure from stray magnetic fields is rare, agencies should not store magnetic media near high-voltage lines or transformers. Agencies should control access to original images created digitally in order to protect the authenticity and integrity of the record.

Agencies should discourage use of original motion picture film for excerpt copying and, above all, prevent the use of A and B rolls for the reproduction of excerpts or stock footage. These matched camera original reels contain numerous editing splices that are easily damaged and difficult to repair.

Although few agencies still have nitrocellulose film, it is critical that nitrate film and safety acetate film be stored separately. Chemically unstable and highly inflammable, nitrate film can be identified by a pungent odor of deterioration similar to nitric acid, a yellowish color of the film base, and stickiness. Nitrate motion picture film was manufactured until 1951 and only in the 35mm gauge. Manufacturers phased out nitrocellulose film for x-ray photographs, still pictures, and motion pictures between 1933 and 1951. Federal agencies should offer all film materials of this vintage to the National Archives. Agencies should also contact NARA if they discover deteriorating cellulose-acetate film. A strong acetic odor, buckling, channeling, and crystalline residue are all signs of acetate deterioration.

**Arrangement and Identification**

Disposable and permanent audiovisual records, as indicated in an approved records schedule, should be stored separately. Unnecessary, redundant, duplicate, and poor-quality copies should be screened out and discarded as authorized by General Records Schedule 21, Audiovisual Records. Non-record copies of audiovisual records received from other sources should also be weeded and discarded when no longer needed. The abundance of contemporary photography can become unmanageable if files are not periodically weeded.

Agencies need to identify records with captions or appropriate markings. Persons, places, dates, or circumstances that seem familiar today easily fade into obscurity tomorrow and unidentified audiovisual records become useless for research. For still pictures, a consistent format for recording captions, typically consisting of dates, locations, names, subjects, events, copyright ownership if applicable, and identification numbers should be used. Moving image media and sound recordings require similar identification. Captioning or other descriptive information does not have to be affixed to the record itself but may be maintained in a parallel file, catalog, or database if the correlation is clear.

All enclosures and containers should be marked with identification numbers. Enclosures for negatives and corresponding prints should be marked with the same number. Prints without negatives should be numbered on the back edge with a soft pencil. Annotations should never be made on the face or on the middle of the back. Negatives and prints should be filed in separate locations.

Photographs should be arranged numerically, chronologically, or alphabetically by subject in blocks that permit easy transfer to the National Archives according to the cutoff dates indicated in agency records schedules.

For more specific requirements on storage conditions and maintenance operations of audiovisual records, see NARA regulations 36 C.F.R. Sections 1232.26 and 1232.28 respectively, as well as NARA’s website for the most current information:  https://www.archives.gov/records-mgmt/publications/managing-audiovisual-records.html.

# Appendix 8: Acronyms

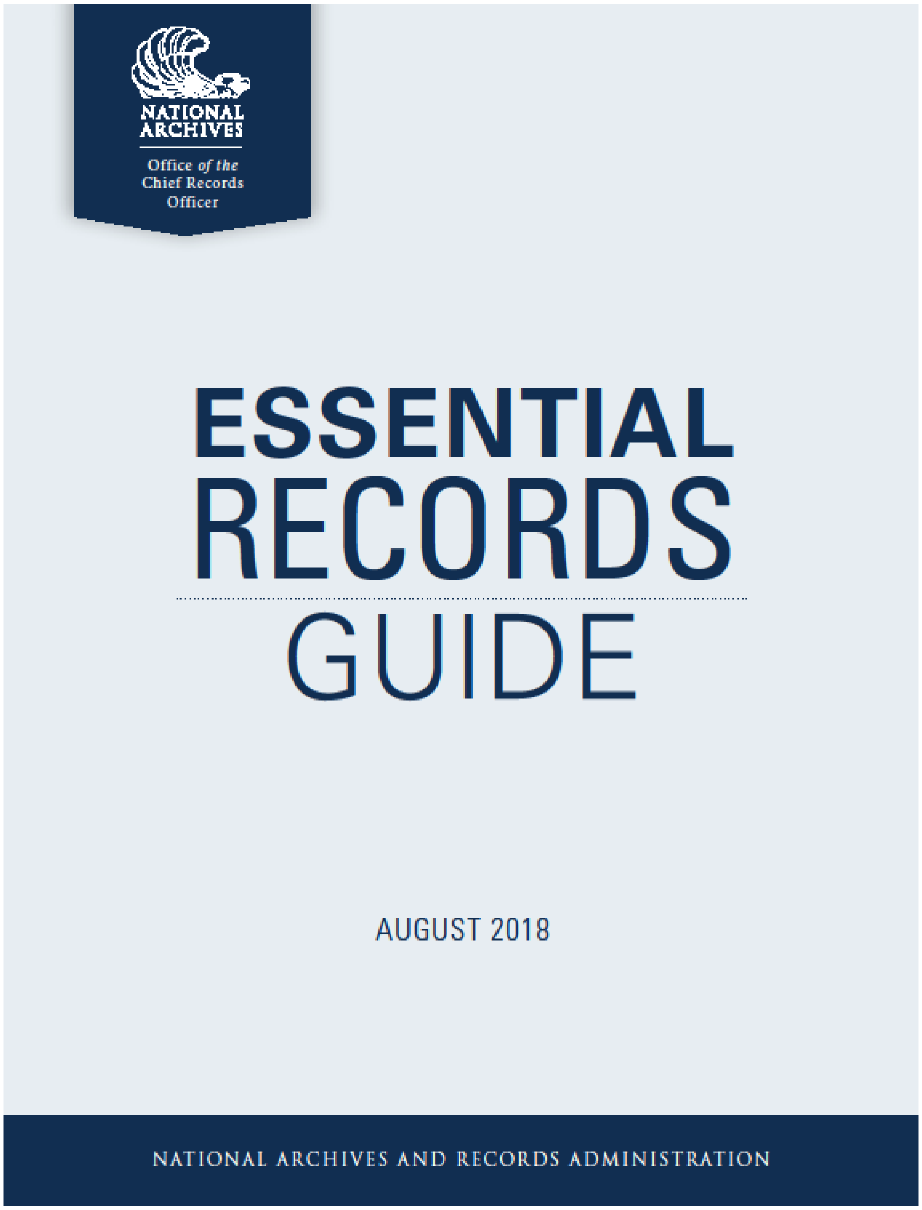
| | | |
|---|---|---|
| AC | – | Assistant Commissioner |
| ARCIS | – | Archives and Records Centers Information System |
| BRM | – | Business Reference Model |
| CBP | – | U.S. Customs and Border Protection |
| CFR | – | Code of Federal Regulations |
| CIO | – | Chief Information Officer |
| CoOP | – | Continuity of Operations |
| CRO | – | Chief Records Officer |
| CUI | – | Controlled Unclassified Information |
| DHS | – | Department of Homeland Security |
| EAC | – | Executive Assistant Commissioner |
| EO | – | Executive Order |
| ESI | – | Electronically Stored Information |
| ERMS | – | Enterprise Records Management System |
| FACA | – | Federal Advisory Committee Act |
| FEA | – | Federal Enterprise Architecture |
| FOIA | – | Freedom of Information Act |
| FRA | – | Federal Records Act |
| FRC | – | Federal Records Center |
| GRS | – | General Records Schedules |
| GSA | – | General Services Administration |
| HRM | – | Human Resources Management |
| LRIM | – | Local Records and Information Manager |
| NARA | – | National Archives and Records Administration |
| OCC | – | Office of the Chief Counsel |
| OIT | – | Office of Information and Technology |
| OMB | – | Office of Management and Budget |
| PALMS | – | Performance and Learning Management System |
| PDO | – | Privacy and Diversity Office |
| PII | – | Personally Identifiable Information |
| POC | – | Point of Contact |
| PODS | – | Policy Online Document Search |
| PTA | – | Privacy Threshold Analysis |
| RAE | – | RIM Accountable Executive |
| RCS | – | Records Control Schedule |
| RIM | – | Records and Information Management |
| RMWG | – | Records Management Working Group |
| SME | – | Subject Matter Expert |
| SORN | – | System of Record Notice |
| SOW | – | Statement of Work |
| USBP | – | U.S. Border Patrol |
| USC | – | United States Code |

# Appendix 9: Records and Information Management Evaluation and Certification Process

The Guidance, process, and forms for conducting annual records evaluation and certification will be developed in FY 2019.

# Appendix 10: Essential/Vital Records

This section includes NARA’s Guide to Essential Records.



NATIONAL ARCHIVES

Office *of the* Chief Records Officer

ESSENTIAL RECORDS GUIDE

AUGUST 2018

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

NATIONAL ARCHIVES

Office *of the* Chief Records Officer

# ESSENTIAL RECORDS GUIDE

AUGUST 2018

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

# Table of Contents

# SECTION 1 – PURPOSE AND SCOPE

The purpose of this *Guide* is to assist agencies with establishing an Essential Records Program and meeting their emergency records management responsibilities. An Essential Records Program is a crucial part of a Federal agency's Continuity of Operations Program (COOP).

Many people are involved in an Essential Records Program, including Senior Agency Officials for Records Management (SAORMs), Agency Records Officers, Essential Records Managers, other records management personnel, Continuity Managers, Risk Managers, program managers, information resource managers and related personnel. The intended audience for this *Guide* is anyone who identifies, declares, manages, protects, and makes accessible the essential records of a Federal agency. Non-Federal government organizations, such as state and municipal archives, tribes, historical societies, libraries, museums, colleges, or universities, may find the *Guide* to be useful as well.

This *Guide* addresses the identification and protection of records, whether uncontrolled unclassified, classified, or controlled unclassified information (CUI). It highlights accessing information that Federal agencies need to conduct business under emergency operating conditions or to protect the legal and financial rights[1] of the Federal government and the people it serves. This *Guide* also provides information to assist agencies assessing damage and implementing recovery of records affected by an emergency or disaster.

This *Guide* was first published in 1996 as the *Vital Records Guide*. Soon after Hurricane Katrina struck the Gulf Coast in 2005, officials in the nation's state archives suggested to the Federal Emergency Management Agency (FEMA) that use of the term "vital records" be changed. Many state archives deal with "vital records" programs that primarily focus on birth and death certificates, marriage licenses, divorce decrees, and wills. These records are created by local authorities and are not considered to be Federal records. In response, FEMA adopted the term "essential records" to describe any documentation needed for emergency operating conditions and disaster recovery.

[1] NARA formerly referred to these records as "Rights and Interests" records.

# SECTION 2 – ESSENTIAL RECORDS – DEFINITION AND PROGRAM

## 2.1) ESSENTIAL RECORDS DEFINITION

In Chapter 36 Section 1223 of the Code of Federal Regulation (36 CFR 1223), NARA defines essential records as:

> “[R]ecords an agency needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).”

The two essential records categories in the regulation are defined as:

1) **Emergency Operating Records** - records an organization needs to continue functioning or to reconstitute after an emergency. Examples include:
   - Emergency plans and directive(s) which specify how an agency will respond to an emergency. The information content of records series[2] and electronic records systems determines which records are essential;
   - Orders of succession;
   - Delegations of authority;
   - Staffing assignments; and
   - Selected program records needed to continue the most critical agency operations under emergency conditions and to resume normal operations after an emergency.

2) **Legal and Financial Rights Records** – records needed to protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Much of this information is likely to be CUI. Examples include:
   - Accounts receivable records;
   - Titles, deeds, and contracts;
   - Licenses and long-term permits;
   - Social security records;
   - Payroll records;
   - Retirement records;
   - Insurance records; and
   - Military service and medical records *[not in original CFR text]*

[2] 36 CFR 1220.18(3)(Series) – “Series means file units or documents arranged according to a filing or classification system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use. Also called a records series.”

FEMA expands on the NARA definition of essential records by tying that in to emergency management functions. FEMA identifies emergency management functions as Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs), based on eight National Essential Functions (NEFs). PMEFs and MEFs are essential functions that agencies must continue throughout, or rapidly resume after, an emergency or disruption of normal activities. FEMA's definition of essential records includes those records needed to perform PMEFs and MEFs during emergencies.

## 2.2) ESSENTIAL RECORDS PROGRAM

The foundation of an agency's approach to identifying and managing its essential records is to establish, develop, and maintain an Essential Records Program.

The Essential Records Program includes those policies, plans, and procedures the agency develops and implements – and the resources needed – to identify, use, and protect essential records. This is an important program element of an agency's emergency management function.

The primary objectives for an agency's Essential Records Program are to:

- Identify and protect records that specify how an agency will operate in an emergency or disaster;
- Identify and protect records necessary for the resumption of normal operations; and
- Identify and properly manage records needed to protect the legal and financial rights of the Government and citizens.

Elements of an Essential Records Program include:

- An Essential Records Plan (See Section 3);
- Essential records and CUI training for all applicable staff (See Section 7);
- Identified roles and responsibilities for all key personnel (See Section 9);
- Processes to designate essential records;
- Processes to ensure essential records are kept current and complete;
- Protection for essential records; and
- Provisions for prompt access to essential records when needed.

Agencies must designate an Essential Records Manager to manage the Essential Records Program. Essential Records Managers are designated by a written appointment letter to the Agency Records Officer. One role of the Essential Records Manager is to ensure that Essential Records Programs are part of Federal Continuity Programs. Continuity Programs are required by FEMA's *Federal Continuity Directive 1 (FCD 1)* (See Appendix A of this *Guide*).

Viable continuity programs include comprehensive processes for identification, protection, and accessibility of electronic and hardcopy essential records at continuity facilities. Staff at these facilities should have access to their essential records within 12 hours of COOP activation, regardless of media or format of records. Accessibility of essential records must consider whether staff will be accessing and using electronic records on standalone computers, via networks from telework locations or if they will need to use hardcopy records stored in secured locations or containers. Security requirements must also be considered for the information.

## 2.3) ESSENTIAL RECORDS RISK PLANNING

Essential Records Program planning addresses potential risks that could adversely affect agency operations and the preservation of records. In planning, agency officials will identify the types of risks to which each of its facilities may be subjected and also assess the level of each type of risk to determine the type of protection or response that may be required.

A partial possible list of threats includes fires, hurricanes, earthquakes, tornadoes, floods, acts of sabotage, cyber-attacks, civil disturbance, disgruntled citizens or employees, terrorist attacks, and even infestation by vermin such as rodents and even paper-eating insects. Poor building conditions and maintenance are also contributing factors and are common causes of water and fire damage.

Consider regional differences when evaluating risks. Federal agencies located on the East coast and along the Gulf coast of the United States must consider the potential impact of hurricanes on their operations and their

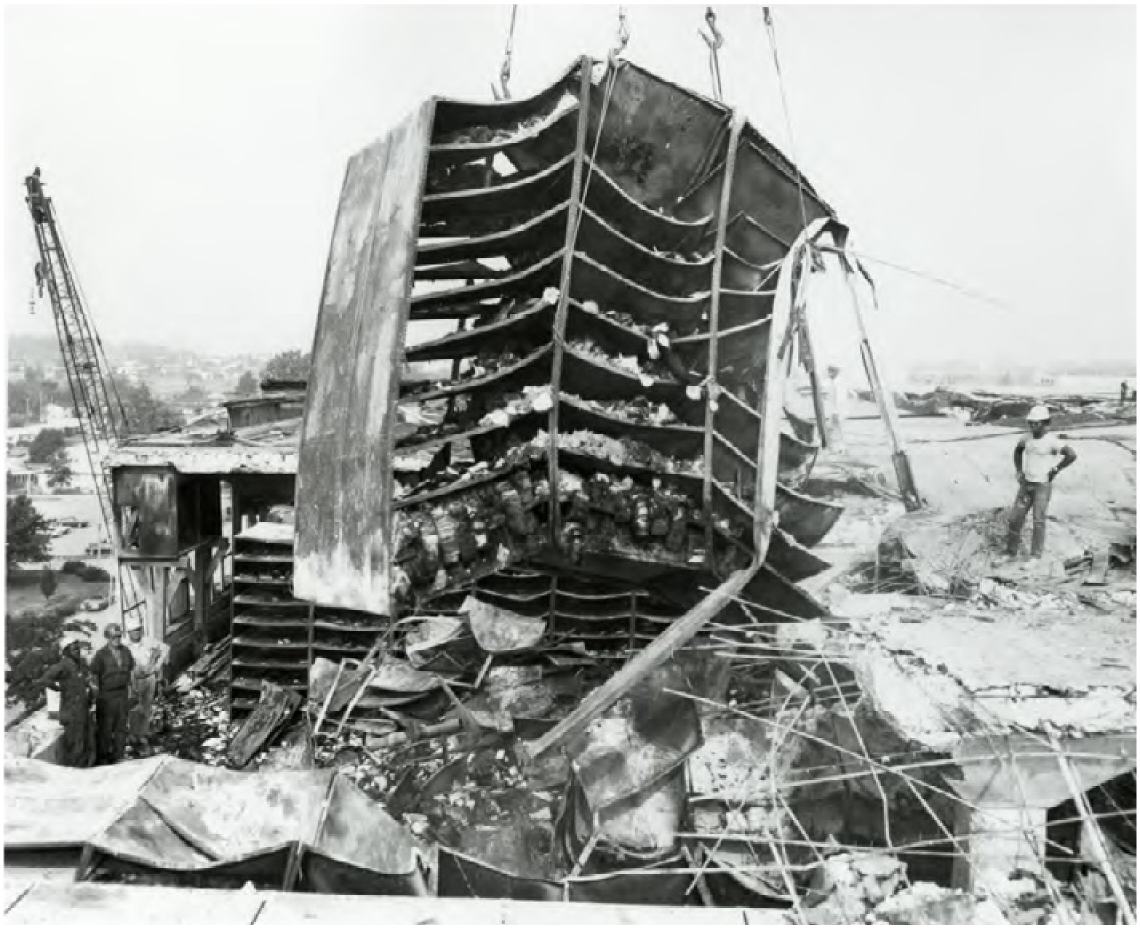


FIGURE 1.
Aftermath of the 1973 fire at the National Archives, Military Personnel Records facility, in St. Louis, Missouri. Photo shows shelving being pulled from the damaged building. This disastrous fire destroyed approximately 16-18 million Official Military Personnel Files. There were no duplicate copies, no microfilm copies, and no indexes created prior to the fire. - *Prologue, July 16, 2013* and *NARA website*

records. Those located in the South and Midwest may be more subject to tornadoes. The West coast may be more susceptible to earthquakes and wildfires – although such activity occurs in other parts of the country as well. All regions are subject to the possibility of floods and fires. Terrorist attacks and emergencies caused by people can happen anywhere.

## Partial List of Disasters that Impacted Federal Agencies Since 1970

| Year | Location | Agency(ies) Impacted | Cause |
|---|---|---|---|
| 1970 | Los Angeles, California | Veterans Affairs Hospital | Earthquake |
| 1973 | St. Louis, Missouri | NARA – National Military Personnel Center | Fire |
| 1991 | Philippines | U.S. Air Force – Clark Air Force Base | Volcano |
| 1992 | Florida | U.S. Air Force - Homestead Air Force Base | Hurricane (Andrew) |
| 1993 | St. Louis, Missouri | National Mapping Agency | Flooding |
| 1995 | Oklahoma City, Oklahoma | Multiple Agencies – Murrah Federal Building | Domestic Terrorist Bombing |
| 2000 | Fort Worth, Texas | FBI | Tornado |
| 2001 | New York City and Washington, DC | DoD, U.S. Customs Service, Multiple Agencies | Terrorist Attack (September 11, 2001) |
| 2005 | Louisiana and Mississippi | Multiple Agencies | Hurricane and Flooding (Katrina) |
| 2010 | Austin, Texas | IRS | Plane Crash Into Building by Disgruntled Citizen |
| 2012 | Northeastern U.S. | Multiple Agencies | Hurricane (Superstorm Sandy) |
| 2017 | Caribbean - Puerto Rico and U.S. Virgin Islands | Multiple Agencies | Hurricanes Irma and Maria |

FIGURE 2. Some actual examples of disasters since 1970 affecting Federal facilities or agencies are included in the table above. Such disasters continue to reoccur with regularity and their causes are varied.

# SECTION 3 - ESSENTIAL RECORDS PLAN

The Essential Records Plan documents all aspects of the Essential Records Program.

Both NARA and FEMA provide guidance to agencies describing the development and maintenance of an Essential Records Plan. The descriptions of the relevant guidance text are outlined below:

- FEMA's Federal Continuity Directive 1 (FCD 1) Annex F (Requirements and Criteria) states that agencies are to develop and maintain an Essential Records Plan and include a copy of their Plan at alternate sites.
- NARA (36 CFR 1223.16) states: "Vital [essential] records also include emergency plans and related records that specify how an agency will respond to an emergency."

Agencies need to develop instructions in the Essential Records Plan for moving essential records that have not been prepositioned from the primary operating facility to the alternate site. These instructions must be included in the agency's Continuity Plan and Essential Records Plan. The Essential Records Manager should typically be charged with this and related essential records management tasks.

When essential records are in electronic format, physical relocation may be unnecessary. However, when agencies plan for the potential loss of power or network access over an extended period, making hardcopy essential records available onsite is a viable option. A good example of this situation occurred during the unprecedented hurricanes in 2017, (Hurricanes Harvey, Irma, and Maria), in which some agencies, especially in the Caribbean, were without power for very long periods of time.

In addition, the instructions need to account for protection requirements associated with types of CUI and classified information.

## 3.1 ESSENTIAL RECORDS PACKET

FEMA also requires agencies to develop and maintain an Essential Records Packet as part of their Plan. The Packet is an electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation.

The Packet must include:

1) A hard and / or electronic copy of the Emergency Relocation Group (ERG) list of members with up-to-date telephone numbers;

2) An Essential Records Inventory indicating the media format, along with the precise locations of the essential records;

3) Necessary access mechanisms such as keys or access readers / codes;

4) Continuity facility locations;

5) Access requirements and lists of sources of equipment necessary to access the records (this may include hardware and software, microfilm readers, Internet access, dedicated telephone lines, and information systems security requirements);

6) Description of records salvage and recovery vendors and services that may be needed; and

7) A copy of the agency's Continuity Plans. (Note: the Essential Records Plan is a part of the agency's Continuity Plan).

Typically, the Essential Records Manager ensures the current Packet is maintained at the agency's continuity facility and dispersed as needed for backup purposes. The Essential Records Manager must annually review the Packet and document the date of the review and the names of all reviewing personnel.

# SECTION 4 – IDENTIFYING AND INVENTORYING ESSENTIAL RECORDS

## 4.1) COMMON ESSENTIAL RECORDS

Essential records include those listed in *Section 2.1* "Essential Records Definition", but may also include:

- Emergency staffing assignments, including lists of personnel, along with their addresses and telephone numbers (and comparable data for alternates), assigned to the Emergency Operations Center (EOC) or other emergency duties or authorized access to damaged facilities to assess the extent of damage;
- Access credentials for the EOC and classified or restricted access container documentation (as required);
- Building plans and building systems operations manuals for all agency facilities;
- Equipment inventories for all agency facilities;
- File plans, (specifically referring to essential records), describing the records series and electronic information systems maintained by records custodians for all agency facilities;
- Copies of agency program records (whatever the media) needed to carry out continuing critical functions (also referred to as mission essential functions); and
- System documentation for any electronic information systems designated as emergency operating records.

As agency officials are making the difficult and judicious decisions in reviewing candidates for essential records, they must also conduct, at least annually, an essential records risk assessment. The assessment must consider the list of actions (below) in designating their candidate essential records, information, and data:

- Identify the risks associated with retaining essential records in their current locations and media, and attempt to determine the difficulty of reconstituting the records if they are destroyed;
- Identify offsite storage locations and requirements, including CUI and classified safeguarding requirements;
- Determine if alternative storage media is available; and
- Determine requirements to duplicate records and provide alternate storage locations to provide readily available essential records under all conditions.

(See Section 2.3 for Essential Records Risk Planning.)

## 4.2) ESSENTIAL RECORDS INVENTORY

Identifying and designating an agency's essential records in an inventory is a crucial step in the Essential Records Program. The inventory contains a list of carefully vetted essential records needed to perform mission essential functions during a continuity activation.

Agencies must maintain a complete Essential Records Inventory, along with the locations of and instructions on accessing those records. The Essential Records Inventory is prepared and maintained by the agency's various program managers' designees under the direction of the Essential Records Manager. This inventory must be maintained at a back-up/offsite location to ensure continuity if the primary operating facility is damaged or unavailable. Agencies should consider maintaining these inventories at a number of different sites to support continuity operations. Because of power reliability issues in emergency situations, it may be prudent for agencies to consider maintaining a hardcopy of some or all of their essential records, and the related inventory. However, some agency staff, not deployed to the agency's COOP site would not be able to access any records maintained in only hardcopy format.

The Essential Records Inventory includes**:**

- Name of the office responsible for the records series or electronic information system containing essential information;
- Title of each records series or information system containing essential information;
- Identification of each records series or system that contains emergency operating essential records or records relating to legal and financial rights;
- Medium on which the records are recorded;
- Physical location for offsite storage of copies of the records series or system;
- Frequency with which the records are to be cycled or updated, which is the recurring removal of obsolete copies of essential records and replacing them with current copies. This process may occur daily, weekly, monthly, quarterly, annually or at other designated intervals; and
- Minimum security requirements for the information systems and the information.

## 4.3) STEPS TO IDENTIFYING AND INVENTORYING ESSENTIAL RECORDS

Agency program managers – especially those who are responsible for performing MEFs and PMEFs in the event or an emergency – are responsible for identifying and maintaining an inventory of their essential records. Program managers perform the following steps to identify and inventory their essential records:

- Consult with the agency official responsible for emergency coordination, e.g., COOP Manager – unless otherwise directed by the agency;
- Review the wording of the agency's PMEFs and MEFs and determine which records  support those functions;

- Review agency statutory and regulatory responsibilities and any existing emergency-related plans for insights into the functions and records to be included in the Essential Records Inventory;
- Review documentation created for the contingency planning and risk assessment phases of emergency preparedness. The offices performing those functions are an obvious focus of an inventory;
- Review current file plans of offices responsible for performing critical functions (such as PMEFs and MEFs) or may be responsible for preserving rights; and
- Review the agency records schedule to determine which records series potentially qualify as essential.

Also consider the protection and use of complementary information systems, technology, applications, infrastructure, and references needed to support the continued performance of essential functions and continuity operations during an activation, including CUI and classified requirements depending on the type(s) of information involved. The identification, protection, and availability of electronic and hardcopy essential records and electronic information systems needed to support essential functions during emergencies are critical elements of a successful continuity plan and program. See also, *Section 11 - Appendix B - Glossary of Terms* – "*Information System Contingency Plan (ISCP)"* for more information on IT related needs.

Exercise caution in designating records as essential when creating the Essential Records Inventory. Maintaining essential records requires agency commitment of staff time and effort. Include only those records series or elec-tronic information systems (or portions of them) *most* critical to emergency operations or the preservation of legal or financial rights. In most agencies only a relatively small number of records series will be essential records.

# SECTION 5 – STORING AND PROTECTING ESSENTIAL RECORDS

## 5.1 Protective Measures

Establish easy to understand procedures for retrieving and accessing essential records. Staff may be unfamiliar with the records they may need to use in an emergency. Appropriate measures to protect essential records include:

- **Duplication** - Agencies may choose to duplicate essential records as the primary protection method. Duplication can be to the same or different medium as the original records. When choosing duplication as a protection method, use a copy of the original essential record as the version stored offsite. The agency may store the original records offsite for protection or as a space savings measure. Ensure duplicated records include all CUI and classified designators from the original and that offsite storage meets the safeguarding requirements for such information.
- **Dispersal** - Once agencies duplicate the records, they must disperse the copies to sites a sufficient distance away to avoid them being subject to the same emergency. Agencies may use other office locations, offsite locations, or proper storage facilities maintained by a third party as dispersal sites. Ensure the storage meets CUI and classified safeguarding requirements.

FIGURE 3. As an important lesson learned from Hurricane Katrina in 2005, NARA designed and built an Electronic Records Vault (ERV) for storing Federal agency essential records away from the most disaster prone areas of the country. The ERV is a secure, controlled access, environmentally controlled storage unit for Federal agencies' essential electronic records. Photos credit – NARA – Federal Records Centers Program

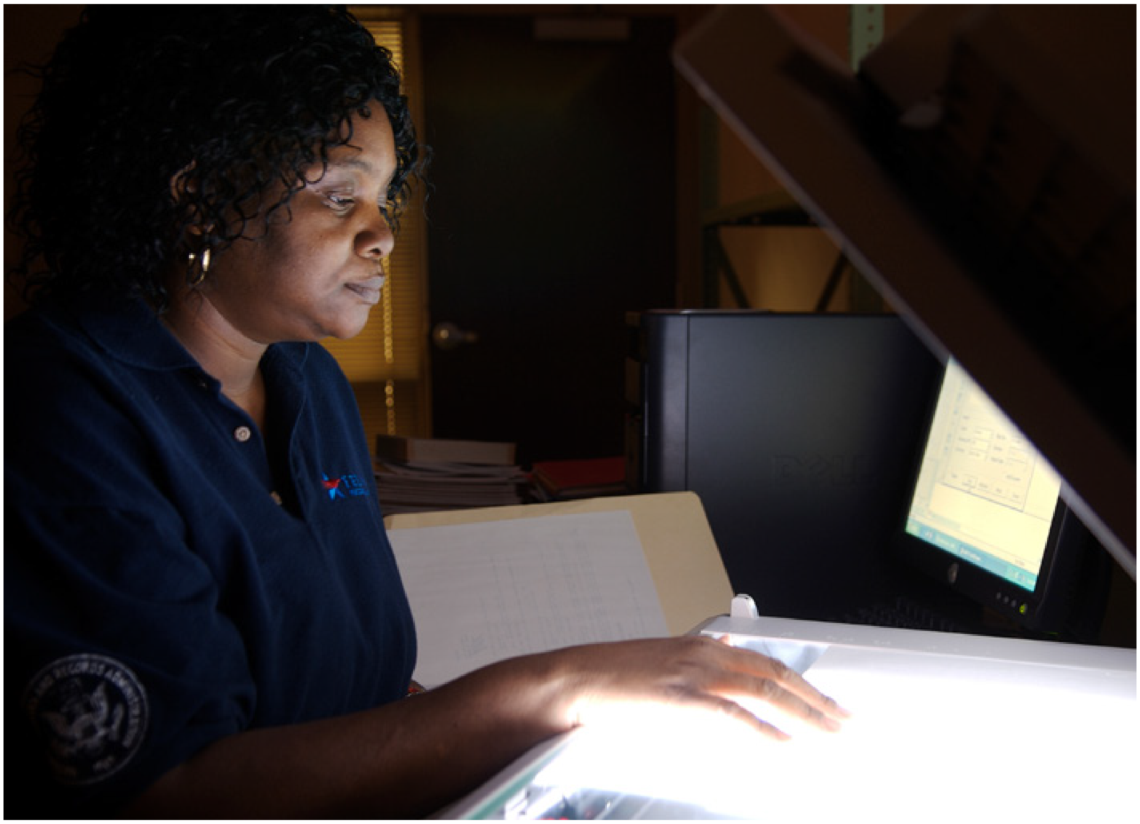


FIGURE 4.
Scanning of essential Federal records at a NARA facility so that the digital surrogate of the records can be used in an emergency situation. Scanning the records provides an extra layer of protection since the digital records can easily be made available for access at multiple locations within an agency during a disaster. Photo credit – NARA Federal Records Centers Program.

- **Storage considerations –** *Within 12 hours following the activation of agency continuity plans* agencies must make copies of emergency operating records accessible. Agencies may not need copies of legal and financial rights records as quickly. When deciding where to store essential record copies, agencies must treat records that have the properties of both categories, that is, both emergency operating and legal and financial rights records, the same as emergency operating records. Some storage considerations specifically include:

a) Agencies may store copies of legal and financial rights essential records at an offsite agency location or at a NARA records storage facility, in accordance with 36 CFR 1223.22. Additional general facility-type information can be found at the NARA website - Records Storage Standards Toolkit;

b) When using a NARA records storage facility for storing legal and financial rights essential records that are duplicate copies of original records, the agency must specify on the *SF 135, Records Transmittal and Receipt*, or equivalent per 36 CFR 1232.16, that they are essential records (duplicate copies) and the medium on which they are maintained[3]; and

c) Agencies may maintain essential records on a variety of media. In selecting the media, agencies must ensure the hardware, software, and documentation it needs to access complete records will be available and that it meets CUI and classified safeguarding requirements.

[3] Per NARA 2018-2022 Strategic Plan (Feb 2018) By December 31, 2022, NARA will no longer accept new transfers of analog records for storage, [including paper copies of essential records], by the Federal Records Centers Program (FRCP) to the fullest extent possible.

## 5.2 Offsite Storage

Agencies choose protection methods and proper storage sites for their essential records. Protection methods may include using existing duplicates of the records designated as essential and digitizing hardcopy records as appropriate. In addition, these methods must meet applicable CUI and classified safeguarding requirements. Increasingly, agencies are storing essential records electronically for ease of use, access, updating, timeliness, dispersal, and protection.

Given the importance of essential records, agencies want to consider arranging for offsite storage of copies in a facility not immediately subject to the same emergency or disaster, but still reasonably accessible to agency staff. The storage site for copies of emergency operation records may be different from the storage site for copies of records needed to protect legal and financial rights.

Whenever feasible, store copies of emergency operating records in a properly equipped, environmentally-controlled, secure, Emergency Operations Center (EOC). If essential records are recorded on a medium other than paper, check with the center before initiating a transfer to ensure that appropriate environmentally-controlled space is available and that it meets CUI and classified safeguarding requirements. It is also important to ensure that appropriate equipment is available to provide access to the records.

If an agency has not established such an operations center, it may store emergency operating records at an appropriate facility (commercial or agency-operated) or a Federal Records Center operated by NARA. Periodic cycling or updating of copies of essential records is crucial. In order to meet its information needs and responsibilities, the agency must decide the frequency of cycling or updating based on how current its emergency operating records and legal and financial rights records need to be[3]. *[see footnote 3 on previous page]*

NARA-approved records schedules or NARA's General Records Schedule (GRS) govern disposition of essential records (see *36 CFR 1225, Scheduling Records*). GRS 4.1 addresses retention of copies of essential records. Agencies cannot destroy original records that are not scheduled.

# SECTION 6 – REVIEW AND TESTING

The Essential Records Manager conducts annual reviews with other appropriate agency program managers to determine whether the agency's essential records are adequately protected, current, and accessible to the staff who use them. Reviews are particularly important should the agency's functions or activities change significantly. Such changes might require a modification of the Essential Records Plan (*see Section 2.3)*.

During the annual review of the Essential Records Program and the Plan, the Essential Records Manager will:

- Address new security issues;
- Identify problem areas;
- Update information; and
- Incorporate any additional essential records generated by new agency programs or functions or by organizational changes to existing programs or functions.

Federal Continuity Directive 1 (FCD 1) states in Annex K (Testing – 2 (a) and (b)) that an organization's testing program must include and document the testing for information systems and essential records by specifically doing the following:

a) Annual testing of recovery strategies (i.e., disaster recovery plans and/or IT contingency plans) for essential records (uncontrolled unclassified, classified, and controlled unclassified information (CUI)), critical information systems (both classified and unclassified), services, and data; and

b) Annual testing of the capabilities for protecting essential records and information systems (uncontrolled unclassified, classified, and controlled unclassified information (CUI)) and for providing access to them from alternate locations.

The Essential Records Manager will work with other test participants to assess the results of the test and to make appropriate modifications where needed.

# SECTION 7 – TRAINING

All agency employees and contractors assigned responsibilities in the Essential Records Program are to receive appropriate training. Periodic briefings to senior managers, especially those new to the agency, are given about the Essential Records Program and their relationship to their records. Training will focus on the identification, inventorying, protection, storage, and updating of copies of the agency's essential records. Wherever possible integrate this training with existing agency training about records management and emergency coordination including fire drills or building evacuation drills and security, including CUI and classified. See NARA Bulletin 2017-01 Agency Records Management Training Requirements for more information.

NARA provides a course entitled "Vital Business Information" that provides the knowledge and skills required to identify, protect, and make readily-available, essential records needed to support the resumption of critical business functions after a disaster, and to establish and administer an Essential Records Program. The course is based on the essential records requirements contained in FEMA's Federal Continuity Directives (FCD 1, FCD 2), and 36 CFR 1223. For more information on how to register for courses see NARA's Records Management Training webpage.

# SECTION 8 – RECORDS DISASTER MITIGATION AND RECOVERY

All Federal records, not just essential records, need protection from a variety of emergencies or disasters. When emergencies or disasters occur, even the best protective measures may not prevent damage to records. Consequently, agencies need to develop Records Disaster Mitigation and Recovery Plans for timely and economical response to records disasters in order to salvage or replace damaged records and the information that they contain. NARA, as the nation's record keeper, has Records Disaster Mitigation and Recovery Plans to help protect its vast holdings of important, permanent records and rapidly increasingl amounts of electronic information. Many Federal agencies also have significant accumulations of important information and therefore need to be prepared to respond to their own records disasters by developing and maintaining such Plans.

In addition to providing essential records guidance, NARA oversees two other related programs that specifically address:

- Emergency Destruction of Records – When NARA and the agency whose records are damaged, determine they are a continuing menace to human health or life, or to property, NARA will authorize the agency to eliminate the menace immediately by any method necessary. The agency that has custody of the records must obtain NARA's specific approval prior to destroying such records.

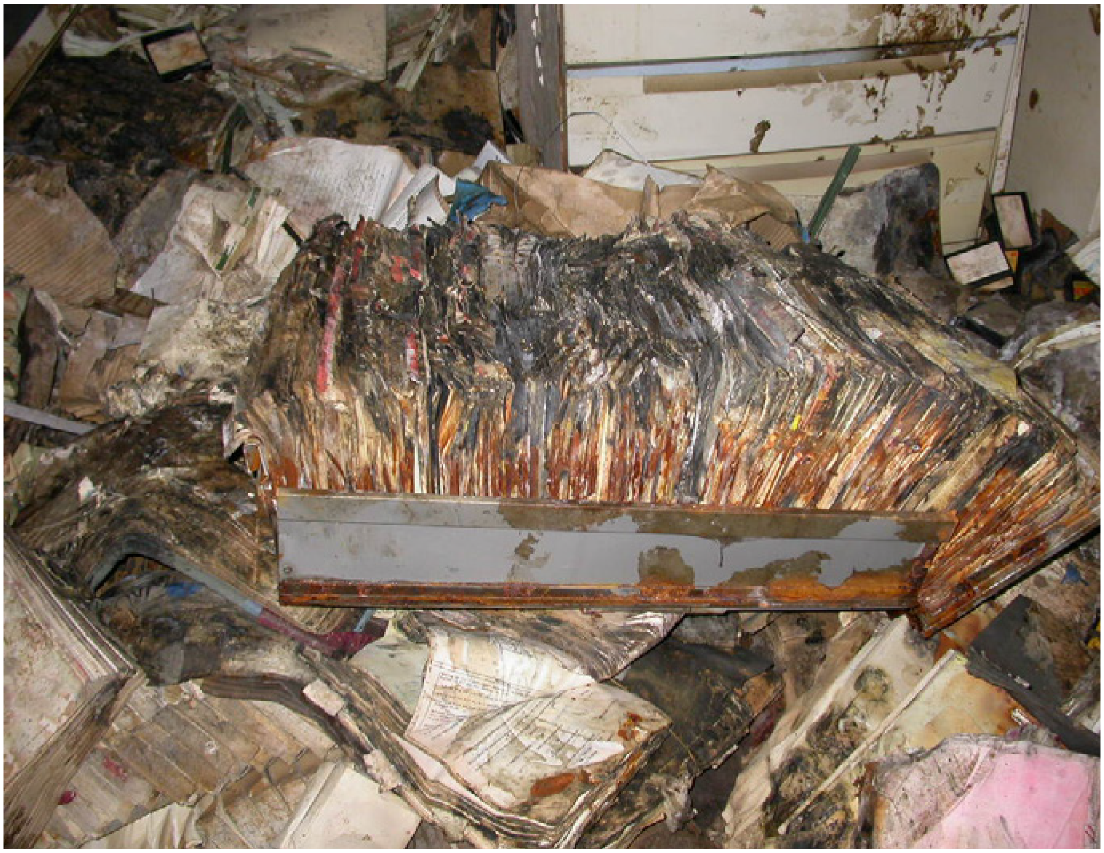


FIGURE 5.
Water damaged records in the aftermath of Hurricane Katrina in New Orleans, Louisiana in 2005. Records contained mold and other contaminants as well. These important records were treated by a records salvage and recovery vendor and later returned to New Orleans for further use. Records recovery can be very expensive. It is important to plan accordingly and protect essential records from any anticipated disasters. Photo credit – NARA Preservation Programs.

- Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records - Defines actions such as the alteration, defacing, removal, or destruction of records and outlines responsibilities, penalties, and reporting of such cases. Agencies must report to NARA any such occurrences and implement corrective measures before a case may be closed.

These two programs may or may not involve essential records in a given situation. They are mentioned here to remind agencies of their existence and that they are required by regulations that may in some cases also incidentally pertain to an agency's essential records.

The information that follows pertains to all agency records – not just essential records. It is important for agencies to know what to do to mitigate loss and address damaged records. In developing the agency's *Records Disaster Mitigation and Recovery Plan*, officials assess the varying intensity of each risk to which their records may be subjected. Risks may range from minor flooding affecting only one or two offices in a facility to a major earthquake that causes significant damage to an entire region. Fire, water, and smoke damage receive particular attention as they historically present the greatest danger of damage to records.

To properly address records disaster mitigation and recovery agencies first appoint a lead person to oversee the necessary steps in setting up a Records Disaster Mitigation and Recovery Program and Plan. This person is designated as the **Records Disaster Mitigation and Recovery Coordinator** (may be called Program Coordinator or similar title for this collateral duty).

Below are some of the duties associated with this role:

- Establish and maintain the Records Disaster Mitigation and Recovery Program;
- Serve as agency official responsible for managing Records Disaster Mitigation and Recovery Program;
- Document the Program's policies, authorities, responsibilities of agency officials, and procedures in appropriate issuances such as functional statements and procedural manuals. Documentation will include the definition of the Coordinator position and designation of other staff members of the Team (described below);
- Oversee establishing the Records Disaster Mitigation and Recovery Plan and making it available to applicable agency personnel. Maintain Plan to reflect changes;
- Work with continuity or records emergency-related staff and others in developing Records Disaster Mitigation and Recovery Plan;
- Work with others in developing and implementing protective measures to mitigate potential records disasters;
- Notify appropriate persons immediately in emergencies – regarding nature of emergency and level of threat to the records;
- Assess and documents damage to space and records and propose salvage options to management;
- Consult with records salvage and recovery vendors as needed in recovery of records and information and helping to resume normal operations using recovered records;

- Periodically review the Records Disaster Mitigation and Recovery Plan with assistance of selected officials to determine effectiveness of Plan; and
- Coordinate activities of the Records Disaster Mitigation and Recovery Team (aka Records Recovery Team) – which is designated agency staff that expedite stabilization of the records.

## RECORDS DISASTER MITIGATION AND RECOVERY PLAN STEPS

Plan steps are outlined as follows:

1) Identify and assign responsibility (committees, task forces, or teams. While these work in tandem, these are often carried out separately by different teams)
    - planning
    - response
    - recovery
2) Train members of the committees, task forces, or teams
3) Conduct a risk analysis
    - assess ability to protect people
    - identify potential building problems
    - survey fire protection policies and equipment
    - evaluate potential for damage from natural and human-caused disasters
4) Establish goals and a timetable
5) Develop a reporting schedule and reporting lines
6) Evaluate records and assign priorities
7) Identify potential sources of damage
8) Assess prevention and protection needs
    - stockpile supplies and equipment
    - replenish when necessary
9) Review fiscal implications
10) Prepare and obtain approval for the Plan
11) Distribute the Plan
    - train
    - drill

12) Evaluate the Plan and update it regularly

## RECORDS DISASTER MITIGATION AND RECOVERY PLAN ELEMENTS

Include records recovery in the agency COOP Plan with specific procedures for personnel to follow in the event that an emergency or disaster occurs. Records Disaster Mitigation and Recovery Plan Elements (see below) provide  an outline for use by the Records Disaster Mitigation and Recovery Program Coordinator in working with such agency officials as the Emergency Coordinator, the information management / technology staff, facilities managers, Essential Records Manager, records management staff, CUI Program staff, and security staff in developing the Records Disaster Mitigation and Recovery Plan. In addition, brief all other agency staff on their general responsibilities should such an emergency or disaster happen.

### Records Disaster Mitigation and Recovery Plan Elements (outline)

1) Table of Contents

2) Introduction
   - use of the document
   - how it is to be revised
   - responsible personnel
   - general information about the facility

3) Emergency information sheet
   - fire/police departments
   - hospitals
   - emergency shut-off
   - utility companies
   - brief list of emergency respondents

4) Telephone/reporting tree

5) Records priorities (establish a pack out order – since it may be impossible to remove all records at one time – but do not remove records until photo-documenting the existing conditions and ensuring there is a plan of action)

6) Response outline
   - lead personnel responsibilities
   - assess the situation, identify needed actions
   - organize/prioritize efforts

- establish a command post
- eliminate hazards
- control the environment
- deal with the media
- identify and estimate costs for supplies, equipment, and vendor  services
- obtain emergency funding/supplies
- provide security
- provide human comforts
- train in onsite salvage techniques

7) Supply lists and assistance/equipment vendors

8) Provide clear description of salvage techniques

9) Rehabilitation plans for conservation treatment (Note: if there is a plan to handle a response in-house, a designated area needs to be identified and outfitted with tables, plastic sheeting, and drying materials. If there is mold, it will be best to turn the project over to a records salvage and recovery vendor.)

10) Appendices (if needed)

In assessing the damage to records, take into account the recording medium. Water damaged photographic negatives and microfilm require different treatment from paper records. Agencies must ensure that records with access restrictions are handled only by personnel with proper clearance.

Before beginning an actual recovery process, separate damaged records from undamaged records, to speed up response and recovery. If possible, remove records from the affected area to a protected, secure, sorting space to allow open access to cleaners and contractors. Establishing a separate records work area will help to maintain records control and security, facilitate separation of damaged and undamaged records, and allow quick and efficient identification for different media and damage levels.

Ideally, conduct the planning for potential records recovery advice and services well before a disaster strikes. Establish contact details for sources of advice and identifying vendors to provide the required services. Make sure that any such documentation is easily accessible in an emergency. Prepare a list of records salvage and recovery vendors, including areas of expertise, addresses, telephone numbers, and an individual point of contact before a records emergency or disaster occurs. Periodically check this list to ensure that it remains accurate and current. NARA provides descriptions of services, contracting guidelines, and lists of records salvage and recovery vendors on its website. This vendor list is for informational purposes only; inclusion in the list is not to be viewed as a quality endorsement.

Salvage and recovery specialists often concentrate on very specific problems. One recovery specialist may focus on recovering water damaged paper records, while another may concentrate on recovery of water damaged magnetic tapes and computer hard drives. Consequently, develop as broad a listing of records disaster salvage and recovery specialists to be able to respond appropriately to all the potential risks to which all recorded media might be subjected.

Consider maintaining risk management and mitigation strategies during planning to reduce risk levels and potential impact of disasters. These strategies are particularly important for water damage, the most common source of disaster-related records damage. These can include installing water alarms in high-risk locations such as areas where past leaks occurred. Keep onsite supplies of plastic sheeting to protect records and data storage equipment during emergency situations. Have wet-vacuums and fans readily available to quickly dry out affected areas.

The Records Disaster Mitigation and Recovery Plan also provides details about the following processes:

1) Notifying the appropriate persons *immediately* in case of emergency to relate details about the nature of the emergency and the level of threat to the records;

2) Assessing the damage to records as soon as possible after the emergency and taking immediate steps to stabilize the condition of the records so further damage will not occur;

3) Assembling a Records Disaster Mitigation and Recovery Team of agency staff members to expedite stabilization of the records (generally only for major records disasters);

4) Consulting with contractors that provide records salvage and recovery services if the damage assessment shows a need for their expertise;

5) Recovering the records and the information that they contain, or providing replacement of any lost recorded information when recovery is not feasible; and

6) Resuming normal business using the recovered records and information.

# SECTION 9 – ROLES AND RESPONSIBILITIES

There are numerous positions that have roles for continuity and/or essential records that are described in *Section 11 – Appendix C – "Typical Agency Emergency Response Positions and Related Teams"*. Below is a short list of some of the most important positions along with brief descriptions of their roles and responsibilities.

Generally, Essential Records Programs will include descriptions of the following positions:

- Essential Records Manager;
- Agency Records Officer;
- Agency Program Managers (owners of the essential records for their unit).
- Continuity Manager;
- CUI Program Manager, and
- Records Disaster Mitigation and Recovery Program Coordinator.

## Essential Records Manager -

The designation of the agency's Essential Records Manager is made by sending a written appointment letter to the Agency Records Officer.

The duties of the Essential Records Manager are to:

- Coordinate the agency's Essential Records Program;
- Develop and maintain the agency's Essential Records Plan including the Essential Records Packet;
- Assist in effectively managing and protecting agency's mission essential information assets;
- Coordinate essential records training for agency personnel;
- Coordinate agency inventory of essential records and outline measures to protect them;
- Periodically test emergency plans and procedures to determine whether essential records are properly identified, protected, and managed; and
- Perform annual reviews to determine whether the essential records are adequately protected, current, and accessible as well as reflect any changes to agency functions.

The Essential Records Manager works with others to assess the test results of the plans and procedures and to make appropriate modifications where needed.

## Agency Records Officer -

The Agency Records Officer serves as the official responsible for overseeing the agency's records management program. Essential records are just one category of records in the overall agency records management program. The incumbent works closely with the Essential Records Manager to provide guidance and assistance in inventorying records and determining appropriate maintenance practices for copies of essential records. The Agency Records Officer and the Essential Records Manager work jointly with the agency's various program managers to ensure that current copies of an agency's essential records are properly maintained and accessible when needed.

## Agency Program Managers –

Agency program managers are the owners of the essential records. They are responsible for determining which records within their physical or legal custody are essential. This is based on the contingency planning/risk analysis and identification of both emergency operating records and those needed to protect legal and financial rights. Program managers, in consultation with the records management office and the Essential Records Manager, then take steps to ensure that copies of essential records are properly managed throughout their lifecycle as they are posted, stored, and updated. Any original essential records must be properly maintained until their NARA-approved disposition.

## Continuity Manager -

On behalf of the Continuity Coordinator, Continuity Managers oversee day-to-day continuity programs and represent their departments and / or agencies at inter-agency forums and working groups including the Interagency Continuity Working Group (ICWG) as appropriate. The Continuity Manager serves as the primary point of contact with the FEMA National Continuity Programs Directorate (NCP) for department / agency continuity program matters, including preparedness and operational activities.

The Continuity Manager works with the Continuity Coordinator (senior accountable Executive Branch official), program managers, Essential Records Manager, Agency Records Officer, and others in developing the agency's Records Disaster Mitigation and Recovery Plan.

## CUI Program Manager -

The CUI Program Manager is the agency official designated by the agency head or the CUI Senior Agency Official for the agency's day-to-day CUI Program operations, both with the agency and in inter-agency contexts.

## Records Disaster, Mitigation, and Recovery Program Coordinator –

The "Program Coordinator" has primary responsibility for the Records Disaster Mitigation and Recovery Program and Plan. Agencies may refer to this position by different names.

The Program Coordinator:

- Works with others to develop and implement protective measures to mitigate potential records disasters;
- Develops and maintains an up-to-date Records Disaster Mitigation and Recovery Plan;

- Notifies appropriate persons immediately in emergencies about the level of threat to the records and makes the Plan available to agency staff responding to the disaster;
- Assesses damage to records and takes steps to stabilize them;
- Consults with records salvage and recovery vendors as needed during recovery of records, obtains information from vendors, and helps to restore normal operations using recovered records;
- Periodically reviews the Records Disaster Mitigation and Recovery Plan with assistance of selected officials to determine effectiveness of plan; and
- Coordinates activities of the Records Disaster Mitigation and Recovery Team, (aka Records Recovery Team), to expedite stabilization of the records.

# SECTION 10 –ADDITIONAL RESOURCES AND CONTACT INFORMATION

This *Guide* was developed by NARA with substantial input from FEMA. The Office of the Chief Records Officer for the U.S. Government led the update of the *Guide* from the previous 1996 edition. NARA staff who participated in the drafting and review include Preston Huff (project lead), Judy Barnes, Eric 'Kyle' Douglas, Lisa Haralampus, Jack Kabrel, Joe Livingstone, Richard Marcus, Anne Mason, Scott Roley, and Shelby Sanett. Additional significant contributions were made by other NARA staff that were not assigned to the project working group including Patrick Viscuso, Michael Baimbridge, Richard Boyden, and Hilary Kaplan. The FEMA reviewer was Michelle McCurtain of the National Continuity Program. Any questions, suggestions, or comments may be addressed as follows:

## NARA INFORMATION

See the following suggestions for addressing any questions pertaining to Federal records management, records preservation, CUI and classified information:

- **General questions, suggestions, or comments about this *Guide* –** Contact PRMD@nara.gov. This *Guide* is not published in hardcopy and is only available electronically via the NARA website.
- **Federal agency questions about implementing your agency's records schedules –** contact the applicable Federal Agency Records Officer.
- **Questions about Federal records management and records scheduling and appraisal –** contact your agency's assigned NARA Appraisal Archivist.
- **Questions about sending records to a Federal Records Center (FRC) or fee-based services such as scanning and storing electronic essential records contact the applicable Federal Records Centers Account Manager –** *www.archives.gov/records-mgmt/appraisal/work-group-all.html*
- **Questions about NARA's records management training classes – including** Vital Business Information
- **Records recovery questions –** Preservation Programs – Federal Agencies – (also includes information on Records Salvage and Recovery Vendors) – *www.archives.gov/preservation/records-emergency*
- **Information security questions -** For advice and assistance on issues concerning classified national security information contact your agency's security office and CUI Program Manager.

# FEMA INFORMATION

FEMA has multiple resources and guidance that pertain to essential records (directives, essential records plan packet template, brochure, etc.):

- **General FEMA-related questions, suggestions, or comments**- contact FEMA-NCP-Federal-Continuity@dhs.gov.
- **FEMA Essential Records Plan Packet Template –** see Plan Packet.
- **FEMA Continuity Essential Records Management Brochure** – Continuity Essential Records Brochure.
- **DHS-FEMA Federal Continuity Directives 1 and 2** (FCD 1) (FCD 2)**.**

NOTE: FCD 1 provides direction to Federal departments and agencies for use in developing their continuity plans and programs. It includes information on essential records. FCD 2 provides guidance and direction to Federal departments and agencies on how to validate and update their mission essential functions using a risk management process.

# SECTION 11 – APPENDICES

These four appendices appear on the following pages:

- Appendix A – Resources (Laws, Regulations, and Guidance)
- Appendix B – Glossary of Terms
- Appendix C – Agency Emergency Response Positions and Teams
- Appendix D – Essential Records Checklist (Optional)

# APPENDIX A – RESOURCES - LAWS, REGULATIONS, & GUIDANCE

- **Presidential Policy Directive 40 (PPD 40), *National Continuity Policy (NCP)***, July 15, 2016, directs the Secretary of Homeland Security through the Administrator of the Federal Emergency Management Agency (FEMA) to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies (D/As). Specifically, the Administrator of FEMA is directed to *develop and promulgate Federal Continuity Directives to establish continuity program and planning requirements for executive departments and agencies.* **Federal Continuity Directive 1 (FCD 1)** – issued January 17, 2017, implements this requirement by establishing the framework, requirements, and processes to support the development of department and agency continuity programs and by specifying and defining elements of a continuity plan. These required elements include delineation of essential functions; succession to office and delegations of authority; safekeeping of and access to essential records; continuity locations; continuity communications; human resources planning; devolution of essential functions; reconstitution; and program validation through testing, training, and exercises (TT&E). PPD 40 replaced NSPD-51/HSPD-20 and the NCPIP. Note: parts of PPD 40 are classified. Contact your Federal agency continuity manager for questions or access. See Federal Continuity Directive (FCD 1) below for more information. See FEMA National Continuity Programs for contact information.

- **Presidential Policy Directive 8, National Preparedness,** March 30, 2011, referred to as the National Preparedness Goal, describes the approach to preparing for the threats and hazards that pose the greatest risk to the security of the Country. See also National Preparedness Goal.

- **Presidential Policy Directive 21, Critical Infrastructure Security and Resilience,** February 12, 2013, outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

- **FCD 1 Federal Continuity Directive 1**, Federal Executive Branch National Continuity Program and Requirements, approved by the FEMA Administrator on January 17, 2017, provides operational direction for the development of continuity plans and programs for the Federal Executive Branch. This directive supersedes FCD 1, dated February 2012. The new FCD 1 establishes minimum continuity standards for departments and agencies to incorporate into their daily operations to ensure seamless and immediate continuation of essential functions. All Federal Executive Branch departments and agencies, regardless of their size or location, shall have a viable continuity capability, based on the requirements and principles outlined in the guidance, to ensure resiliency and continued performance of their organization's essential functions under all conditions.

- **FCD 2 Federal Continuity Directive 2**, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification, approved by the FEMA Acting Administrator on June 13, 2017, provides direction and guidance for Federal organizations to identify their essential functions and the business process analysis (BPA) and business impact analysis (BIA) that support and identify the relationships between these essential functions.

  FCD 2 provides implementation guidelines for the requirements identified in FCD 1, Annex C. It provides direction and guidance to Federal entities for identification of their mission essential functions (MEFs) and potential primary mission essential functions (PMEFs). It also includes checklists to assist in identifying essential functions through a risk management process and identify potential PMEFs that support specific national essential functions (NEFs)—the most critical functions necessary for leading and sustaining our nation during a catastrophic emergency.

  FCD 2 provides guidance and direction for departments and agencies in the process for the identification and periodic review and verification of their Essential Functions, the Business Process Analyses and Business Impact Analyses that support and identify the relationships among these Essential Functions. NCP has developed a fillable PDF form to assist agencies in completing their Mission Essential Function (MEF) / Business Process Analysis (BPA) / Business Impact Analysis (BIA) process.

  The MEF Worksheet consists of a series of forms that identify requirements, inputs, outputs, interdependencies, and the critical elements that assist agencies in identifying their MEFs and candidate Primary Mission Essential Functions (PMEFs) and in completing the required BPAs. To obtain an electronic copy of the MEF/BPA/BIA worksheet, send an email request to FEMA-NCP-Federal-Continuity@fema.dhs.gov.

- 36 CFR 1223 “Managing Vital Records”. NOTE: pending revision – proposed new title is “Managing Essential Records”. Specifies policies and procedures needed to establish a program to identify, protect, and manage essential (vital) records as part of an agency’s continuity or operation plan designed to meet emergency management responsibilities.

- 36 CFR 1225 “Scheduling Records”. Describes which Federal records must be scheduled, how to develop records schedules, and other related scheduling topics.

- 36 CFR 1229 “Emergency Authorization to Destroy Records”. Describes conditions under which Federal records may be destroyed (under certain provisions).This addresses a situation in which an agency identifies records that pose a continuing menace to human health, life, or to property. The agency must immediately notify the National Archives and Records Administration. If NARA concurs in a determination that the records must be destroyed, NARA will notify the agency to immediately destroy the records.

- 36 CFR 1230 "Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records". Defines actions such as alteration, removal, destruction, etc., and outlines responsibilities, penalties, and reporting of such cases.

- 36 CFR 1236 "Electronic Records Management". Describes records management and preservation considerations for designing and implementing electronic information systems and other additional electronic records requirements.

- 44 U.S.C. 3101. "Records Management by Agency Heads; General Duties" – states that agency heads shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and 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.

- 44 U.S.C. 3553. "Federal Information Security Modernization Act of 2014" provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

- General Records Schedules (GRS 4.1) Records Management Records (includes essential records) (September 2016).

- General Records Schedules (GRS 5.3) Continuity and Emergency Planning Records (January 2017).

- National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010. Publication provides instructions, recommendations, and considerations for Federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption.

- National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Systems and Organizations*, April 2013 (includes updates as of January 22, 2015).

- National Preparedness Goal, September 2015 - National preparedness is described as a shared responsibility of the whole community. Describes security and resilience posture through the core capabilities that are necessary to deal with great risks.

- National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations," Rev. 1, December 2016.

- ISO 15489-1 (2016-04-15) – International Standard that covers best practices in records management including policies for protecting records. It contains information that addresses usability of records in the event of a disaster affecting records systems or storage areas, routine monitoring of storage conditions, and risk assessment. Note: 15489-1 is a copyrighted international standard available for purchase.

- Executive Order (EO) 10346 – “Preparation by Federal Agencies of Civil Defense Emergency Plans”. President Truman issued Executive Order (EO) 10346 in April 1952, making each Federal department and agency responsible for carrying out its essential functions in an emergency. Revoked by EO 10529 in 1969. See EO 10529 (1954).

- Executive Order (EO) 12656 “Assignment of Emergency Preparedness Responsibilities”. This 1988 order addresses national security emergency preparedness functions and activities. As used in this order, preparedness functions and activities include, as appropriate, policies, plans, procedures, and readiness measures that enhance the ability of the Federal government to mobilize for, respond to, and recover from a national security emergency.

- Executive Order (EO) 13526 “Classified National Security Information”. This 2009 order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

- Executive Order (EO) 13556 “Controlled Unclassified Information”. This 2010 order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

- Records Management Solutions – GSA’s Multiple Award Schedule (MAS) 36 – GSA’s Unified Shared Services Management (USSM) office and the National Archives and Records Administration (NARA) worked together to develop Universal Electronic Management (ERM) Requirements. Simultaneously, GSA’s Integrated Workplace Acquisition Center (IWAC) incorporated these new requirements into Multiple Award Schedule (MAS) 36. Records Management products and services (some having potential use in essential records management) are now structured under Schedule 36 as:

- SIN 51-504 – Physical Records Management Solutions

- SIN 51-600 – Electronic Records Management Solutions

- In conjunction with the above structured records management solutions, GSA MAS 36 also offers a wide range of related services, including:

- SIN 51-506 – Document Conversion Services, and

- SIN 51-409 – Network, Optical Imaging Systems and Solutions.

# APPENDIX B – GLOSSARY OF TERMS

NOTE: There are a variety of plans and positions included in the body of the *Guide* and the glossary below. Terms vary depending on sources used and how they have been adapted for agency use. Cross references are provided when known and as applicable. Agency emergency planners should focus on ensuring that their continuity program effectively addresses safety, minimizing loss of life, injuries, and damage or loss of property (including essential records), and sustaining the performance of essential functions of the agency regardless of the circumstance. Plans (or variations of these) typically include:

- Continuity of Operations Program Plan (COOP Plan)
- Essential Records Plan (formerly Vital Records Plan)
- Occupant Emergency Plan(s) (OEP) aka Emergency Action Plan(s) (EAP)
- Records Emergency Plan(s) (REP)
- Disaster Recovery Plan(s) (DRP), and
- Pandemic Influenza Plan

| TERM | DEFINITION |
|---|---|
| **Activation** | The implementation of a continuity plan, in whole or in part. |
| **All-Hazards** | A classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects. These include accidents, technological events, natural disasters, space weather, domestic and foreign-sponsored terrorist attacks, acts of war, weapons of mass destruction, and chemical, biological (including pandemic), radiological, nuclear, or explosive events. |
| **Business Impact Analysis (BIA)** | A method of identifying the consequences of failing to perform a function or requirement. |
| **Business Process Analysis (BPA)** | A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel, systems, data, interdependencies, and alternate locations inherent in the execution of a function or requirement. |

| TERM | DEFINITION |
|---|---|
| **Classified records and information (Classified National Security Information)** | Classified National Security Information is defined as information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. EO 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. See also - 32 CFR 2001 Classified National Security Information, Final Rule (ISOO implementing directive). This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information. |
| **Continuity** | The ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event or incident that disrupts normal operations. |
| **Contingency Plan (ISCP)** | See Information Systems Contingency Plan |
| **Contingency Planning** | Contingency planning is an element of business continuity, disaster recovery and risk management. It is an alternate plan to the original plan should conditions adversely change. |
| **Continuity of Operations Program (COOP)** | An effort within individual agencies to ensure they can continue to perform their Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. |
| **Continuity of Operations (COOP) Plan** | A documented plan that details how individual agencies can continue to perform its Mission Essential Functions (MEFs), Primary Mission Essential Functions (PMEFs), and any National Essential Functions (NEF's) during emergencies, including acts of nature, accidents, technological and attack-related emergencies during a wide range of events that impact normal operations. Covers devolution and reconstitution with appropriate delegations of authority for leadership and staff in order to increase survivability and perform the essential functions. Required by PPD 40. Other plans with names like Emergency Plan, Disaster Plan, Emergency Response Plan, Disaster Preparedness Plan, Contingency Plan, etc., are generally supportive plans and do not replace the COOP Plan. |

| TERM | DEFINITION |
|---|---|
| **Controlled Unclassified Information (CUI)** | Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. Executive Order 13556 "Controlled Unclassified Information" (the Order), establishes a program for managing CUI across the executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO). 32 CFR Part 2002 Controlled Unclassified Information was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. Many essential records fall under CUI categories, including privacy, physical security, personnel, financial, and others. |
| **Cycle** | Periodic removal of obsolete copies of essential records and their replacement with copies of current essential records. This may occur daily, weekly, quarterly, annually, or at other designated intervals. |
| **Delegation of Authority** | Identification, by position, of the authorities for making policy determinations and decisions. Generally, pre-determined delegations of authority will take effect when normal channels of direction have been disrupted and will lapse when these channels have been reestablished. |
| **DERG** | Devolution Emergency Response Group – Regional, interagency, and available headquarters staff that assume the responsibility and execution of headquarters essential functions during Devolution of Operations Plan activation. |
| **Devolution** | The continuation of essential functions in the event that the primary operating facility is incapacitated and personnel are unavailable or incapable of activating or deploying to the normal continuity facility. |
| **Devolution Plan** | Devolution Plan is one of the Continuity Plans required by PPD 40 and FCD 1. |
| **Disaster** | Unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations. Each agency defines what a long-term adverse effect is in relation to its most critical program activities. |
| **Disaster Plan** | Generic term – see also may be called Continuity Plan, Records Disaster Mitigation and Recovery Plan, Disaster Preparedness Plan, Disaster Recovery Plan, or Emergency Plan. |

| TERM | DEFINITION |
|---|---|
| **Disaster Preparedness Plan** | A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response. See also Disaster Plan. This requirement is briefly summarized in annex J of FCD 1 Requirements and Criteria for Reconstitution Operations which states "identify how the organization will determine if any records were affected by the incident to ensure an effective transition or recovery of essential records". However, FCD 1 does not use the term Records Disaster Mitigation and Recovery Plan or any similar name. |
| **Disaster Recovery Plan (DRP)** | Documented process or set of procedures to recover and protect assets of a unit in response to a disaster. See also Records Disaster Mitigation and Recovery Plan. |
| **Disaster Recovery Team** | See *Section 11 - Appendix* C *"Typical Agency Emergency Response Positions & Related Teams".* Applicable staff receive overall direction from the Program Coordinator or Emergency Coordinator but sometimes via local management who, in turn, work with the coordinators. See also Records Disaster Mitigation and Recovery Team. |
| **Dispersal** | Protection of essential records through production of duplicate copies stored at other locations and/or levels of an organization. |
| **Electronic Records Vault (ERV)** | NARA vault, operated by the Federal Records Centers Program, designed for optimal storage of an agency's essential electronic record formats. Currently available only at the Fort Worth FRC. |
| **Emergency** | Situation or an occurrence of a serious nature, developing suddenly and unexpectedly, and demanding immediate action. This is generally of short duration, for example, an interruption of normal agency operations for a week or less. It may involve electrical failure or minor flooding by broken pipes. |
| **Emergency Coordinator** | See *Section 11 - Appendix* C *"Typical Agency Emergency Response Positions & Teams".* |
| **Emergency Operating Records** | Types of essential records an organization needs to continue functioning or to reconstitute after an emergency. Such records support the execution of an agency's essential functions. |
| **Emergency Operations Center (EOC)** | EOC is the location directing the emergency response. The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. |

| TERM | DEFINITION |
|---|---|
| **Emergency Action Plan** | See Occupant Emergency Plan (OEP) |
| **EO** | Executive Order – Orders issued by the President. |
| **Emergency Relocation Group (ERG)** | Emergency Relocation Group – Staff designated to move to a relocation site [which may include teleworking if authorized] to continue essential functions in the event that their normal work locations are threatened or have been incapacitated by an incident. |
| **Essential Functions** | The critical activities performed by agencies, especially after a disruption of normal activities. There are three categories of essential functions: National Essential Functions (NEFs), Primary (Priority) Mission Essential Functions (PMEFs), and Mission Essential Functions (MEFs). |
| **Essential Records** | Essential records are defined by 36 CFR 1223 as:<br>**“**[R]ecords an agency needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).”<br>Previously referred to as vital records. |
| **Essential Records Checklist** | Optional checklist created by NARA combining FEMA’s Continuity Evaluation Tool – V.8 and the former NARA Appendix E Self-Evaluation Guide of the previous version of this Guide (then called *“Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide”.*<br>See current *Section 11 - Appendix D – “Essential Records Checklist”.* |
| **Essential Records Inventory** | A list which identifies the records that have been designated as essential. It includes other identifying information such as where the records are located, who is responsible for them, when they are cycled, format, and similar information useful for the agency to effectively manage the records. |
| **Essential Records Management Regulation** | See 36 CFR 1223 |
| **Essential Records Manager** | See *Section 11 - Appendix* C *“Typical Agency Emergency Response Positions & Teams”.* |

| TERM | DEFINITION |
|---|---|
| **Essential Records Plan** | The Plan contains a description of records that are essential to continued agency operations or for the protection of legal and financial rights. The Plan also includes specific measures for storing and periodically cycling (updating) copies of those records. The Plan should include appropriate position descriptions, functional statements, and procedure manuals and / or SOPs. Formerly known as Vital Records Plan. See also Essential Records Packet. |
| **Essential Records Packet** | Per FEMA guidance (FCD 1), agencies must develop and maintain an Essential Records Packet and include a copy of the Packet at their continuity facilities. An Essential Records Packet is an electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation. The Packet contains the fungible contents of the Essential Records Plan that need to be updated and maintained to ensure they are current. |
| **Essential Records Program** | Essential Records Program means the policies, plans, and procedures the agency develops and implements – and the resources needed – to identify, use, and protect essential records. This is an important program element of an agency's emergency management function. |
| **Event** | A planned, non-emergency activity. |
| **Executive Order (EO) 13526** | See Classified Records and Information (Classified National Security Information). |
| **Executive Order (EO) 13556** | See Controlled Unclassified Information (CUI). |
| **FCD (Federal Continuity Directive)** | Federal Continuity Directive – These directives issued by FEMA, direct executive branch departments and agencies to carry out identified continuity planning requirements and assessment criteria.<br>● FCD 1 – establishes the framework, requirements, and processes to support the development of agencies' continuity programs and by specifying and defining elements of a continuity plan. It includes essential records. (See *Section 11 - Appendix A "Resources, Laws, Regulations, and Guidance")*<br>● FCD 2 – provides guidance and direction to Federal departments and agencies on how to validate and update their mission essential functions using risk management process. (See *Section 11 - Appendix A "Resources, Laws, Regulations, and Guidance"*) |
| **FEMA** | Federal Emergency Management Administration |

| TERM | DEFINITION |
|---|---|
| **General Records Schedule 4.1** | Also referred to as GRS. Schedule that addresses disposition of essential records. See p. 21 and 29 of the GRS. |
| **Incident** | An occurrence or event, natural or human-caused, which requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wild land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response. |
| **Information System Contingency Plan (ISCP)** | All Federal agencies must have a contingency plan. Plan provides established procedures for the assessment and recovery of a system following a system disruption. The Plan provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems – May 2010. The relationship of this Plan to the COOP Plan depends on whether or not the system that is disrupted impacts the agency's ability to perform one or more of its essential functions, It is also related to the Continuity Plan reconstitution function of returning the agency to normal operations. |
| **Legal and Financial Rights Records** | Type of essential records needed to protect the legal and financial rights of the Government and of the individuals directly affected by its activities. |
| **Mission Essential Functions (MEFs)** | The limited set of agency-level Government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities. |
| **National Security Emergency** | Defined as any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or threatens the national security of the United States. See EO 12656. |
| **Occupant Emergency Plan (OEP)** | For Federal agencies the Occupant Emergency Plan is specifically required by the FMR 41 CFR 102—74.230 through 102.74.260, and the Interagency Security Committee Standard (ISC). Per the ISC the terms "occupant emergency plan" and "emergency action plan" are interchangeable. |
| **Orders of Succession** | Provisions for the assumption of senior agency offices during an emergency in the event that any of those officials are unavailable to execute their legal duties. |

| TERM | DEFINITION |
|---|---|
| **Pandemic Influenza Plan** | Since the threat to an agency's continuity of operations is great during a pandemic outbreak, it is important for an agency to have a Pandemic Influenza Continuity of Operations Plan (or annex) in place to ensure it can carry out its essential functions and services. While an agency may be forced to suspend some operations due to the severity of a pandemic outbreak, an effective COOP Plan can assist in its efforts to remain operational, as well as strengthen the ability to resume full operations. Essential records must be addressed in the Plan. See FEMA's website for a template of a Pandemic Influenza Plan (or annex to COOP Plan). FCD 1 requires agencies to have this Plan. It is up to the agency to decide if they want a Pandemic Plan as an annex to the COOP Plan or as a standalone plan. |
| **PPD 40 (Presidential Policy Directive 40)** | Presidential Policy Directive 40 (PPD 40), *National Continuity Policy*, directs FEMA to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies. Signed by the President on July 15, 2016, replaced NSPD-51/HSPD-20 and the NCPIP. PPD 40 created an Inter-agency Reconstitution Working Group (IRWG) which includes DHS/FEMA, OPM, GSA, and NARA. Parts of PPD 40 are classified. |
| **Program Coordinator** | See *Section 11 - Appendix* C *"Typical Agency Emergency Response Positions & Teams".* |
| **Program Managers** | See *Section 11 - Appendix* C *"Typical Agency Emergency Response Positions & Teams".* |
| **Reconstitution** | The process by which surviving and or replacement agency personnel resume normal agency operations from the original or replacement primary operating facility. |
| **Records (defined)** | 44 U.S.C. 3301(a)(1)(A) - As used in this chapter, the term "records"—<br>(1) IN GENERAL.—As used in this chapter, the term "records"—<br>(A) includes all recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of data in them; and<br>(B) does not include —<br>(i) library and museum material made or acquired and preserved solely for reference or exhibition purposes; or<br>(ii) duplicate copies of records preserved only for convenience. |

| TERM | DEFINITION |
|---|---|
| **Records Disaster Mitigation and Recovery Plan** | Plan that includes specific procedures for staff to follow in the event that an emergency or disaster occurs. Records recovery should be included in the agency's Disaster / Continuity Plan. Provides details on appropriate personnel to assist; assess damage and related details about impact; assembling a records recovery team to stabilize records; consult with records salvage and recovery vendors; recovery of damaged records; and resuming normal operations. May also be referred to as a Records Emergency Plan (REP or REMT). See also – Disaster Recovery Plan (DRP). |
| **Records Disaster Mitigation and Recovery Program** | An agency's records disaster recovery program should include: plan, procedures, SOPs, for how to recover damaged records following a disaster. Program needs to address: leaders, lists of staff to support function, training, communication strategy and information, points of contact for assistance, records inventories / locations, inventory of emergency supplies and equipment. An agency should include records recovery in its disaster plan with specific procedures for personnel to follow in the event that an emergency or disaster occurs. |
| **Records Disaster Mitigation and Recovery Program Coordinator** | Also referred to as Program Coordinator (See *Section 11 - Appendix* C *"Typical Agency Emergency Response Positions & Teams".*) |
| **Records Disaster Mitigation and Recovery Team** | Designated agency staff that expedite stabilization of damaged or threatened records. Receive overall direction from the Program Coordinator or Emergency Coordinator but sometimes via local management who, in turn, work with the coordinators. See also Disaster Recovery Team (*Section 11 - Appendix C "Typical Agency Emergency Response Positions & Teams"*). The Records Disaster Recovery Team and any designated alternate members assist the official coordinating the disaster recovery in time of need. At the minimum, team members should assist in assessing the nature and extent of the records disaster and identifying which records were affected and the physical media of the records, so the recovery manager can report accurately on the disaster and recommend specific recovery steps for approval by the agency's senior managers. |
| **Records Emergency Plan (REP or REMT)** | See Records Disaster Mitigation and Recovery Plan and / or Disaster Recovery Plan (DRP). |
| **Records Officer (RO)** | See *Section 11 - Appendix C "Typical Agency Emergency Response Positions & Teams".* |
| **Records Salvage and Recovery** | The portion or phase of disaster response in which efforts are made to salvage and reconstruct damaged records in order to restore normal operations. |

| TERM | DEFINITION |
|---|---|
| **Records Salvage and Recovery Vendors** | NARA has compiled a list of these specialized vendors at the NARA website. No endorsement of the companies is made by NARA. www.archives.gov/preservation/records-emergency |
| **Records Schedules** | A records schedule or schedule is:<br>a) A SF-115, Request for Records Disposition Authority, that has been approved by NARA to authorize the disposition of Federal records<br>b) A General Records Schedule (GRS) issued by NARA<br>c) A printed agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more SF-115s or issued by NARA in the GRS. |
| **Records Series** | 36 CFR 1220.18(3)(Series) - Series means file units or documents arranged according to a filing or classification system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use. Also called a records series. |
| **Records Storage Standard Toolkit** | This toolkit located on the NARA website provides agencies with information to comply with NARA regulations concerning the Records Storage Facility requirements. |
| **Recovery** | The implementation of prioritized actions required to return an agency's processes and support functions to operational stability following an interruption or disaster. |
| **Recovery Manager** | See *Section 11 – Appendix C "Typical Agency Emergency Response Positions & Teams".* |
| **Rights and Interests Records** | NARA formerly referred to legal and financial rights records as rights and interests records. Rights and interests records is a term that is no longer used. |
| **Risk Analysis** | The process by which risks are identified and evaluated. |
| **Senior Agency Official for Records Management (SAORM)** | See *Section 11 - Appendix C "Typical Agency Emergency Response Positions & Teams".* |

| TERM | DEFINITION |
|---|---|
| **Testing, Training, and Exercises (TT&E)** | Measures to ensure that an agency's continuity plan is capable of supporting the continued execution of the agency's essential functions throughout the duration of a continuity situation. |
| **Unclassified Records and Information (Uncontrolled Unclassified Information)** | Uncontrolled unclassified information is information that neither EO 13556 nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements. |
| **Vital Business Information Course** | Course offered by NARA. This course provides the knowledge and skills required to identify, protect, and make readily-available, essential records needed to support the resumption of critical business functions after a disaster, and to establish and administer an Essential Records Program. Course is based on the essential records requirements contained in FEMA's Federal Continuity Directives (FCD 1, FCD 2), and 36 CFR 1223. See Section 7 – "Training" for more information. |
| **Vital Business Information Program** | See also Essential Records Program. NARA Records Management Training unit also uses the name - Vital Business Information Program in its VBI course. Program is defined as the official program supporting an agency's actions to identify, protect, and make available vital (essential) information. |
| **Vital Records** | Now referred to in the Federal government as "essential records". Many state archives use the term "vital records" for birth and death certificates, marriage licenses, divorce decrees, and wills. |
| **Vital Records Plan** | See Essential Records Plan |

# APPENDIX C – AGENCY EMERGENCY RESPONSE POSITIONS & TEAMS

Typical agency emergency response positions, roles, and related teams are summarized in the table below:

| POSITION | ROLES | PAGE #(s) |
|---|---|---|
| **Agency Records Officer *(aka Records Officer)*** | See Records Officer. | NA |
| **Continuity Coordinator** | Senior agency official responsible for coordinating with the agency head and national continuity leadership to ensure the organization maintains a viable and effective continuity capability. (FCD 1) | P. 23 |
| **Continuity Program Manager (Continuity Manager)** | On behalf of Continuity Coordinator, oversees day-to-day continuity programs and represents agency at inter-agency forums and working groups as appropriate. (FCD 1). | P. 1, 22, 23, 28 |
| **Devolution Emergency Response Group (DERG)** | Devolution Emergency Response Group – Regional, interagency, and available headquarters staff that assume the responsibility and execution of headquarters essential functions during Devolution of Operations Plan activation. | P. 28, 33, 34, 49 |
| **Emergency Coordinator** | ● Works with Program Coordinator and others in developing records recovery plan<br>● Assists in identifying and inventorying of essential records – consulting with officials responsible for emergency coordination | P. 19, 35, 40, 45, 47 |
| **Emergency Relocation Group (ERG)** | Emergency Relocation Group – Staff designated to move to a relocation site [which may include teleworking if authorized] to continue essential functions in the event that their normal work locations are threatened or have been incapacitated by an incident. | P. 6, 36 |

| POSITION | ROLES | PAGE #(s) |
|---|---|---|
| **Essential Records Manager** | ● Coordinates the agency's Essential Records Program and Plan – working with continuity manager and planners to ensure essential records are available to support MEFs and the agency's continuity plans and program<br>● Assists in effectively managing / protecting agency information assets<br>● Coordinates essential records training for agency personnel<br>● Coordinates agency inventory of essential records and outlining measures to protect them<br>● Periodically tests emergency plans and procedures to determine that essential records are properly identified, protected, and managed<br>● Oversees or assists in development and maintenance of the agency's Records Disaster Mitigation and Recovery Program / Plan<br>● Designated in writing to the Agency Records Officer | P. 1, 3, 6, 7, 9, 14, 19, 22, 23, 36, 47, 48 |
| **Information System Contingency Plan Coordinator** | Pursuant to the National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 – Coordinator is typically a functional or resource manager within the organization. Develops the strategy in cooperation with other applicable managers and manages the development and execution of the ISCP. | P. 33 |
| **Information Technology Managers** | Responsible for ensuring the appropriate replication of databases containing essential records / information. Also play a role in making sure that the infrastructure / hardware / software is always capable of / ready for reading the essential information, that backups exist, and that essential information is migrated properly. | NA |

| POSITION | ROLES | PAGE #(s) |
|---|---|---|
| **Program Coordinator** ***(aka Records Disaster Mitigation and Recovery Program Coordinator)*** | ● Primary responsibility for ensuring up-to-date Records Disaster Mitigation and Recovery Plan and making it available<br>● Agency official responsible for managing Records Disaster and Recovery Program<br>● Works with others to develop and implement protective measures to mitigate potential records disasters<br>● Works with emergency coordinator and others in developing Records Disaster and Mitigation Recovery Plan<br>● Notifies appropriate persons immediately in emergencies – re. nature of emergency and level of threat to the records<br>● Assesses damage to records and takes steps to stabilize them<br>● Consults with records salvage and recovery vendors as needed in recovery of records and information and helping to resume normal operations using recovered records<br>● Periodically review the Records Disaster Mitigation and Recovery Plan with assistance of selected officials to determine effectiveness of plan<br>● Coordinate activities of the Records Disaster Mitigation and Recovery Team (aka Records Recovery Team) – which is designated agency staff that expedite stabilization of the records. | P. 17, 19, 22, 23, 35, 39, 40, 43 |
| **Program Managers** | Managers throughout the department or agency that are charged with overseeing the missions of the various units. Program managers must work closely with other continuity related officials named in this table to protect an organization's essential records. | P. 1, 9, 14, 22, 23, 39, 45 |
| **Records Disaster Mitigation and Recovery Coordinator** | See Program Coordinator. | NA |
| **Records Disaster Mitigation and Recovery** ***Team (aka Records Recovery Team)*** | ● Designated agency staff that expedite stabilization of the damaged or threatened records<br>● Receive overall direction from Program Coordinator or Emergency Coordinator but sometimes via local management who, in turn, work with the coordinators. | P. 18, 21, 24, 35, 40, 45, 46, 51 |

| POSITION | ROLES | PAGE #(s) |
|---|---|---|
| **Records Officer** ***(aka Agency Records Officer)*** | ● Serves as the official responsible for overseeing the agency's records management program. Essential records are just one category of records in the overall agency records management program<br>● Along with other records managers, as applicable, is responsible for guiding and assisting in inventorying records, identifying essential records, deciding on maintenance practices, and conducting or coordinating training. | P. 1, 3, 22, 23, 25, 40, 43, 44, 47 |
| **Recovery Manager** | Lead person that works in conjunction with the Continuity Program Manager (Continuity Manager) as directed, to implement recovery of agency records per the Records Disaster Mitigation and Recovery Plan. Generally position that identifies (in conjunction with the Records Disaster Mitigation and Recovery Team), which records were affected and the physical media of the records, so an accurate report on the disaster can be produced - and recommend specific recovery steps for approval by the agency's senior managers. | P. 40 |
| **Security Officer and CUI Program Manager** | Responsible for ensuring the proper identification of classified and CUI essential records / information, and the implementation of storage and access measures to protect the assets. | P. 22, 23, 25, 47 |
| **Senior Agency Official for Records Management (SAORM)** | On behalf of the agency head, the SAORM works closely with the Agency Records Officer and other appropriate agency officials to oversee the implementation of their records management program. While the Agency Records Officer has operational responsibility for the records management program, the SAORM is accountable for the agency's strategic direction of records management and ensures compliance with records management statutes and regulations. | P. 41 |

# APPENDIX D – ESSENTIAL RECORDS CHECKLIST

NATIONAL
ARCHIVES

## Essential Records Checklist

This optional checklist is largely based on combining FEMA's FCD 1 (Continuity Evaluation Tool – V.8) and the former NARA Appendix E. Self-Evaluation Guide of the 1996 version of the "Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide".

An effective continuity program is supported by the identification, protection, and ready availability of essential records and electronic information systems needed to support essential functions under the full spectrum of all-hazards emergencies. In the FCD 1 Continuity Evaluation Tool, version 8, metrics are recorded and used to measure an organization's ability to meet its continuity requirements.  Continuity planning is an effort to document the existence of, and ensure the capability to continue organization essential functions during a wide range of potential emergencies. FCD 1, Annex F, sets the critical elements and required criteria to meet and achieve mission readiness for this continuity element. This Essential Records Checklist is closely based on the FCD 1 (CET, v.8) – and is included here to provide the Essential Records Manager, and other applicable agency personnel, a tool to use to quickly determine the organization's readiness to meet Essential Records Program requirements.

| | |
|---|---|
| Organization: | Location: |
| Staff Member Completing Checklist: | Date Completed: |

Tasks Observed (check those that were observed and provide the time of observation).

Tasks/Observation Keys (Agency responses to questions re. Essential Records Program).

1 Have appropriate agency personnel, including the agency's Records Officer, Essential Records Manager, program officials, Risk Manager, Emergency Coordinator, facilities managers, Information Resources Managers, safety/security personnel, and CUI Program Manager, assessed the potential risks to the agency's operations and records?

□ YES □ NO □ NA

2 Has the agency designated in writing an Essential Records Manager? *(An Essential Records Plan must include appropriate policies, authorities, procedures and the written designation of an Essential Records Manager).*

□ YES □ NO □ NA

3 Has the agency determined which of its functions are most critical and would need to be continued if an emergency or disaster struck the agency? *(These critical functions are referred to as mission essential functions (MEFs)).*

□ YES □ NO □ NA

4 **Does the agency’s Essential Records Program identify and protect essential records that:**

a. Specify how the agency will operate in an emergency or disaster?

□ YES □ NO □ NA

b. Support the agency’s continuing essential functions and resumption of normal operations?

□ YES □ NO □ NA

c. Protect the legal and financial rights of the Government and citizens?

□ YES □ NO □ NA

5 **Does the agency’s Essential Records Program include:**

a. Appropriate policies, authorities, and procedures?

□ YES □ NO □ NA

b. Designation of liaison officers that been assigned responsibility for implementing the Program in the agency’s field offices?

□ YES □ NO □ NA

c. Requirement for annual training of all staff involved in the Essential Records Program – informing them of their responsibilities?

□ YES □ NO □ NA

d. Program promotion, regular testing, periodic review, evaluation, and update of the program?

□ YES □ NO □ NA

6 **Has the agency prepared and disseminated written information to appropriate agency staff (beyond the Essential Records Manager), describing the Essential Records Program, including the responsibilities of various agency officials?**

□ YES □ NO □ NA

7 **Does agency incorporate the Essential Records Program into its overall Continuity Plans?**

□ YES □ NO □ NA

8 **Has agency developed procedures to ensure that:**

a. As soon as possible after activation of continuity plans, but in all cases within 12 hours of an activation, ERG/DERG/RPT at the continuity facilities, and teleworkers, have access at appropriate security levels to the appropriate analog and/or electronic media, equipment, and instructions for easily retrieving essential records, including but not limited to, those records stored in a Cloud-based application and accessed via the Internet or a Virtual Private Network?

□ YES □ NO □ NA

b. Access at appropriate security levels is provided to essential records, electronic information systems and the robust communications necessary to sustain an agency's essential functions at the continuity/devolution facility and telework site locations?

□ YES □ NO □ NA

c. Instructions are included on moving essential records (those that have not been prepositioned) from the primary operating facility or system to the alternate one and incorporated in its continuity plan?

□ YES □ NO □ NA

d. Paper or digital copies are made of the essential records for offsite storage?

□ YES □ NO □ NA

e. Duplicates are stored at a remote location or on a cloud-based back-up not subject to the same fire or other risks (such as high-risk geographic areas prone to flooding or earthquakes) present in the storage areas where original records are kept?

□ YES □ NO □ NA

9 **Does agency's complete inventory of essential records include:**

a. Instructions on accessing those records as well as their locations?

□ YES □ NO □ NA

b. Information on the one or more back-up/offsite location(s) to ensure continuity if the primary operating facility or system is damaged or unavailable?

□ YES □ NO □ NA

| | |
|---|---|
| 10 | **Has agency implemented measures for properly storing and maintaining essential records in electronic formats including:**<br>a. Special protection and equipment for electronic storage system or media?<br>□ YES □ NO □ NA<br>b. The use of a variety of acceptable formats to secure electronic records?<br>□ YES □ NO □ NA<br>c. Using secure shared data and computing services via the Internet or a Virtual Private Network or the cloud?<br>□ YES □ NO □ NA<br>d. Maintaining and making available the current documentation on hardware and software?<br>□ YES □ NO □ NA<br>e. Authentications measures appropriate for classified and CUI access?<br>□ YES □ NO □ NA |
| 11 | **Has agency established protective measures to:**<br>a. Protect all records – including essential records?<br>□ YES □ NO □ NA<br>b. Safeguard its essential records, regardless of the media on which these are maintained?<br>□ YES □ NO □ NA |

12 **Has agency:**

a. Established written guidance for a Records Disaster Mitigation and Recovery Program?

□ YES □ NO □ NA

b. Disseminated the Program guidance to appropriate agency staff?

□ YES □ NO □ NA

c. Designated an official responsible for the Records Disaster Mitigation and Recovery Program?

□ YES □ NO □ NA

d. Designated a Records Disaster Mitigation and Recovery Team?

□ YES □ NO □ NA

e. Trained the Records Disaster Mitigation and Recovery Team?

□ YES □ NO □ NA

f. Made appropriate agency staff aware of information at the NARA website regarding available records recovery vendors?

□ YES □ NO □ NA

g. Established a mechanism to maintain supplies and equipment required to recover records damaged in an emergency or disaster?

□ YES □ NO □ NA

h. Conducted periodic reviews in the past of the Records Disaster Mitigation and Recovery Plan and updated it as necessary?

□ YES □ NO □ NA