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

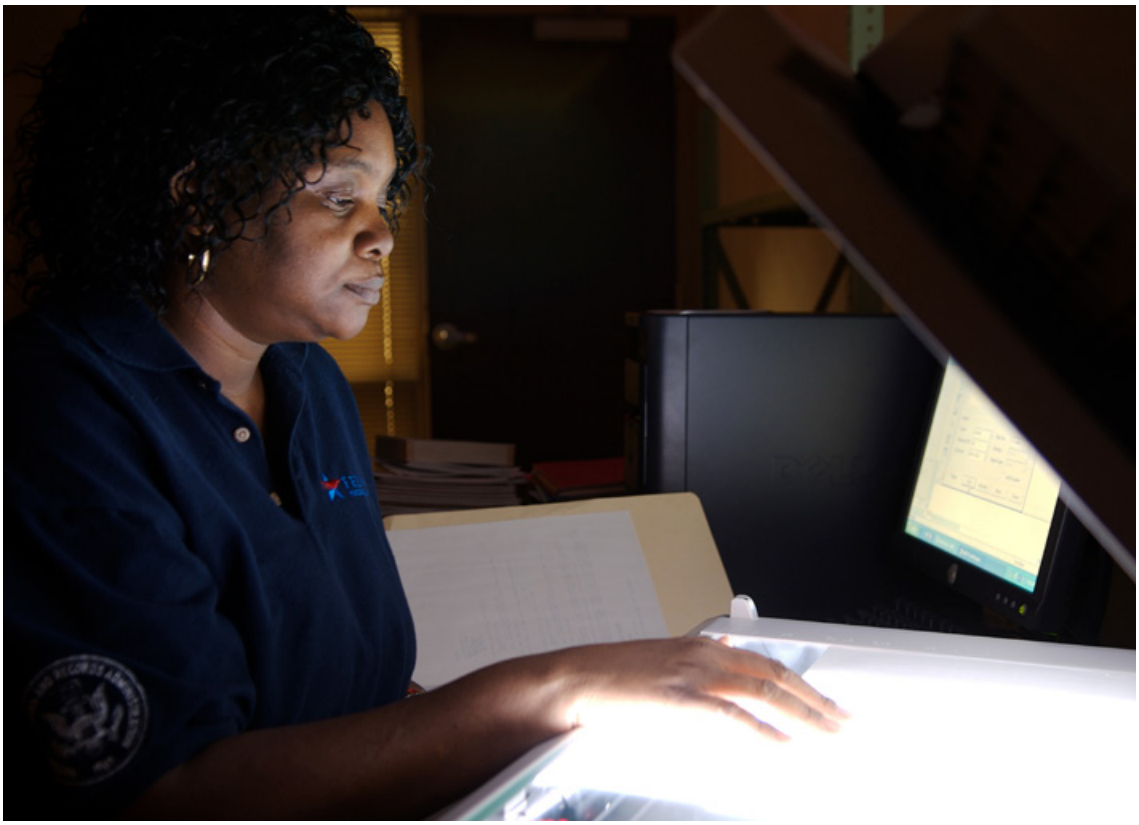

FIGURE 4.
Scanning of essential Federal records at a NARA facility so that the digital surrogate of the records can be used in an emergency situation. Scanning the records provides an extra layer of protection since the digital records can easily be made available for access at multiple locations within 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 Inter-agency 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: **"**[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)." 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"*. 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. • 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")* • 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"— (1) IN GENERAL.—As used in this chapter, the term "records"— (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 (B) does not include — (i) library and museum material made or acquired and preserved solely for reference or exhibition purposes; or (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: a) A SF-115, Request for Records Disposition Authority, that has been approved by NARA to authorize the disposition of Federal records b) A General Records Schedule (GRS) issued by NARA 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 • 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 • Assists in effectively managing / protecting agency information assets • Coordinates essential records training for agency personnel • Coordinates agency inventory of essential records and outlining measures to protect them • Periodically tests emergency plans and procedures to determine that essential records are properly identified, protected, and managed • Oversees or assists in development and maintenance of the agency's Records Disaster Mitigation and Recovery Program / Plan • 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 • Agency official responsible for managing Records Disaster and Recovery Program • Works with others to develop and implement protective measures to mitigate potential records disasters • Works with emergency coordinator and others in developing Records Disaster and Mitigation Recovery Plan • Notifies appropriate persons immediately in emergencies – re. nature of emergency and level of threat to the records • Assesses damage to records and takes steps to stabilize them • Consults 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 • 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 • 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 • 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

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