U.S. Chemical Safety and Hazard Investigation Board

SUBJECT: Records Management Program

Contents

1. PURPOSE

This Order establishes principles, responsibilities, and requirements for managing CSB records. It provides the framework for specific guidance and operating procedures governing records management organization and implementation.

2. EFFECTIVE DATE

This order is effective upon passage by the Board.

3. SCOPE

This Order addresses all records made or received by the CSB. This Order applies to all employees, agents, and contractors (pursuant to the Federal Acquisition Regulation) performing work for the CSB.

4. BACKGROUND

The Federal Records Act of 1950, as amended, requires all federal agencies to make and preserve records containing adequate and proper documentation of their organization, function, policies, decisions, procedures, and essential transactions. These records are public property and must be managed according to applicable laws and regulations.

The Federal Records Act also requires agencies to establish a records management program, which is a planned, coordinated set of policies, procedures, and activities to manage its recorded information. Essential elements include: up-to-date records management directives, proper training for employees responsible for implementation, and careful evaluation to ensure adequacy, effectiveness, and efficiency.

Records serve a number of purposes, including: administrative and program planning, including continuation of key functions in the event of an emergency or disaster, evidence of CSB activities, protection of legal and financial rights, and oversight by Congress and other authorized agencies. Records also capture the Agency's institutional memory and preserve the historical record.

5. REFERENCES

a. 44 U.S.C. Chapter 22 - The Presidential and Federal Records Act Amendments of 2014;

b. 44 U.S.C. Chapter 31 – Records Management by Federal Agencies (Federal Records Act) 44 U.S.C. Chapter 33 – Disposal of Records;

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

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

e. OMB Circular A-123 – Management's Responsibility for Internal Control;

f. OMB Circular A-130 – Management of Federal Information Resources;

g. Federal Emergency Management Agency (FEMA) Federal Preparedness Circular 65 - Federal Executive Branch Continuity of Operations (COOP);

h. Presidential Memorandum, Managing Government Records, November 28, 2011; and

i. Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies, from The Office of Management and Budget and the National Archives and Records Administration, Managing Government Records Directive, August 24, 2012.

6. POLICY

a. CSB's Responsibility and Commitment

The CSB is committed to managing the Agency's records properly to comply with legal requirements and to support the Agency's mission. Accurate and consistent records identification, capture, storage, and retrieval are essential to help the Agency achieve its mission.

This policy establishes requirements whereby CSB records are effectively and efficiently managed throughout their lifecycle to facilitate the accomplishment of CSB's programmatic and administrative missions, to preserve official CSB records in accordance with applicable statutory and regulatory requirements, and to promote access to information by CSB staff, CSB partners, and the public.

b. Creating and Receiving Records

Records contain the information that documents how CSB carries out its mission. All CSB staff generate and receive records and are legally required to maintain them.

Records document the Agency's business and can be found in forms such as paper, e-mail, instant messaging (IM), text messages, voice mail messages, presentations, websites, word processing documents, spreadsheets, and information systems. If electronic records are created using any of these media, they must be transferred to a CSB records management system.

Not all information created or received constitutes a record. Non-records include: reference material, extra copies of records, draft documents or working papers with no substantive comments, and personal information unrelated to CSB business.

Some records are transitory in nature, which means they are of short-term interest (180 days or fewer), and have minimal or no documentary or evidential value.

Official Agency business should first and foremost be done on official CSB information systems (e.g., e-mail, instant messaging (IM), computer work stations, shared service solutions). When extraordinary circumstances occur and CSB business is completed outside CSB systems, the creator must ensure that his/her use of a non-governmental system does not affect the preservation of Federal records for Federal Records Act purposes, or the ability to identify and process those records, if requested, under the Freedom of Information Act (FOIA) or for other official business (e.g.,

litigation, Congressional oversight requests). In this very rare occasion, staff should forward e-mail (or "cc" e-mail) or electronic file(s) to their CSB e-mail account within 20 days of the records creation in order for records to be captured in an approved CSB records management system. Once the electronic files have been captured in an approved CSB records management system, they should be removed from non-CSB information systems, unless there is a specific obligation to maintain the files on all systems on which they appear.

Additionally, the CSB discourages the use of text messaging on a mobile device for sending or receiving substantive (or non-transitory) Agency records. However, some Agency staff perform time-sensitive work that may, at times, require the creation of substantive (or non-transitory) records in the form of text messages for emergency purposes. In those limited instances, CSB staff must continue to save and manage any text message records related to their work, as discussed below.

c. **Managing Records**

Records are managed for the benefit of the CSB and its staff, partners, stakeholders and the public. The CSB is committed to maintaining and converting its records to electronic formats, where practical, to facilitate more effective and efficient electronic solutions. Non-transitory records should be stored in approved records management systems with records management capabilities or registered information management systems associated with an approved records schedule.

It is important not to use non-CSB systems to conduct Agency business, since such use could lead to the mismanagement of CSB records and/or the unauthorized disclosure of CSB information. In the rare situation when a non-CSB messaging system must be used and a federal record is created or received on a non-CSB messaging system (such as a personal e-mail account or personal mobile device), staff must either: (1) copy a CSB e-mail account at the time of initial creation or transmission of the record, or (2) forward a complete copy of the record to a CSB e-mail account within 20 days of the original creation or transmission of the record. Once the message is sent or forwarded to the CSB messaging system, staff must save the record in an approved CSB electronic records management system. Once the electronic files have been captured in an approved CSB records management system, they should be removed from non-CSB systems, unless there is a specific obligation (such as a litigation hold) to maintain the files on all systems on which they appear.

Additionally, e-mails forwarding a news article or web link from a personal e-mail account into CSB's system and e-mails forwarding a document to a personal e-mail account to enable printing or viewing both create a copy of the e-mail in CSB's e-mail system. Users can properly preserve the copy of the e-mail that is on the CSB's system to meet their preservation requirements.

Users of instant messaging (IM), text messaging or other transient technologies are responsible for ensuring that messages that create substantive (or non-transitory)

federal records are saved and placed in a CSB recordkeeping system.

Use of personal social media tools (for example, but not limited to: Facebook, Twitter, LinkedIn) is prohibited for conducting CSB business.

d. **Access**

CSB records must be maintained, captured, and organized to ensure that their timely search and retrieval is possible. Sensitive records (e.g., personally identifiable information (PII)) must be restricted access in accordance with Board Order 44 and statutory requirements.

e. **Implementation**

Each CSB office is required to establish and maintain a records management program with the following minimum requirements:

a. Create, receive, and maintain official records to provide adequate and proper documentation and evidence of CSB's activities.

b. Manage records, in any format (e.g., paper, e-mail, IMs, electronic documents, spreadsheets, presentations, images, maps, video, blogs, and other social media tools that generate communications), in accordance with CSB policy and guidance.

c. Maintain electronic records, (e.g., e-mail, IMs, electronic documents, spreadsheets, presentations, images, video, blogs, and other social media tools that generate communications), in an approved electronic records management system.

d. Migrate electronic records in legacy systems to a CSB approved electronic records management system, when feasible.

e. Maintain records according to the Agency-wide file structure to allow for timely access and retrieval.

f. Secure records to protect the legal and financial rights of the government and anyone affected by such records.

g. Implement a plan to protect essential records and assess damage and recovery of any records affected by an emergency or disaster.

h. Ensure instructions for disposition of records as specified in the approved records schedules are followed.

f. **Information/Record Sensitivity Categorization and Marking Requirements**

a. **General principles.** The selection and use of Information Technology security controls, records management retention and destruction requirements and public releases of information (e.g., FOIA) must reflect the fact that not all information is equally sensitive. The CSB uses the sensitivity categorization

hierarchy described in this section to determine the level of protection required. This hierarchy is strictly an internal CSB tool to help ensure the consistent handling of information and the appropriate application of security controls. It is not related to the separate, established processes for making national security classifications (e.g., Secret, Top Secret), and no national security classification attaches to CSB information by virtue of its categorization under the agency's internal hierarchy.

b. **Sensitivity categorization hierarchy.** The sensitivity of particular information is defined in terms of the extent and severity of the negative consequences that would result from the compromise of that information. Information may be categorized as sensitive due to requirements to protect its confidentiality, integrity, and/or availability.

i. Non-sensitive. Compromise of non-sensitive information would have no negative consequences.

ii. Low sensitivity. Compromise of this category of information would cause only minor injury to government interests. Compromise would cause only minor financial loss or operational disruption, or require only administrative action for correction.

iii. Medium sensitivity. Compromise of this category of information would cause serious injury to government interests. Compromise could cause significant financial loss or operational disruption, or require legal action for correction.

iv. High sensitivity. Compromise of this category of information would cause extremely grave injury to government interests. Compromise could cause loss of life, imprisonment, major financial loss or operational disruption, or require legal action for correction.

c. **Confidentiality labels.** To ensure the easy identification and proper handling of information that is categorized as sensitive because of a requirement to protect its confidentiality, ***users must assign the labels of "For Internal Use Only" and "Confidential" as described below***. Records made or received by the CSB Office of General Counsel must be labeled "Privileged" and/or "Attorney Work Product," as appropriate. The default status for CSB information is unlabeled, which means the information may be treated as non-sensitive. If the creators of information believe it warrants greater protection, they are responsible for assigning the appropriate confidentiality label to their products. Once such a label is assigned, users or recipients of that information must consistently maintain the assigned label. When a label is used, it should be placed in the subject field of electronic mail messages, in the header of memoranda and other documents, or stamped on a physical record. Electronic

storage media (e.g., CD/DVD, flash drive, external hard drive) that contain sensitive information should be clearly labeled with the appropriate confidentiality designation. If possible, users should avoid creating information collections or storage volumes (e.g., a single CD/DVD, flash drive) that combine information with different sensitivity categories. When such a compilation cannot be avoided, the entire volume or collection should be assigned the label of the most sensitive information it contains.

i. Non-sensitive information. Information that is categorized as "non-sensitive" from a confidentiality standpoint is not labeled. This is information that is not covered by any of the disclosure exemptions or exclusions of the Freedom of Information Act (FOIA), or any legal prohibition on disclosure. This information may be released to the public through the FOIA or other appropriate official channels. Examples include press releases and transcripts of public Board meetings.

ii. "For Internal Use Only" – This label is applied to information that is categorized as "low sensitivity" from a confidentiality standpoint. This is information that may be exempt from disclosure under the FOIA, and requires a full legal and security analysis before public disclosure. An example would be CSB internal personnel policies or Board Orders that may contain security sensitive information.

iii. "Confidential" – This label is applied to information that is categorized as "medium sensitivity" or "high sensitivity" from a confidentiality standpoint. Medium sensitivity confidential information would be exempt from disclosure under the FOIA, but not necessarily covered by a specific statutory disclosure prohibition. Examples include: investigative documents reflecting preliminary opinions and analysis, companies' comments on CSB draft reports, and the confidential staff list. High sensitivity confidential information would be exempt from disclosure under the FOIA, and may also be covered by a specific statutory disclosure prohibition. Any information covered by the Privacy Act (e.g., Official Personnel Folders) or the Trade Secrets Act (e.g., confidential business information) is, by definition, high sensitivity. Other examples include: security plans, vulnerability assessments, and attorney-client privileged information.

Notwithstanding the labeling of any information, the CSB may exercise its discretion in determining whether any information is appropriate for public or other disclosure in accordance with applicable law.

7. RESPONSIBILITIES

a. **Director of Records Management –** has the authority to take all actions necessary and proper to ensure the CSB meets all federal recordkeeping requirements. He/she is responsible for creating, implementing, and managing the CSB's records management program, including:

1. Ensuring that senior Agency officials are aware of their programmatic and individual records management responsibilities and requirements.
2. Advising the CSB on records management issues and developing Agency-wide records management procedures, guidance, and training materials.
3. Coordinating the approval of the Agency's records schedules and the transfer of records to the National Archives and Records Administration (NARA).
4. Coordinating records management issues with other federal agencies, including federal oversight agencies such as the Office of Management and Budget (OMB), NARA, and the General Services Administration (GSA).
5. Providing technical advice and training to all Agency offices on establishing and maintaining effective records management programs.
6. Evaluating recordkeeping practices to determine the effectiveness of the program.
7. Obtaining NARA's Certificate in Federal Records Management.

b. **General Counsel** – provides legal advice and counseling on records management issues in accordance with pertinent federal recordkeeping requirements.

c. **EEO Director** – is responsible for maintaining records in their unit in accordance with pertinent federal recordkeeping requirements.

d. **Continuity of Operations (COOP) Program Planners -** are responsible for:

1. Working with records management staff to implement the essential records plan to ensure the continuation of designated COOP essential functions; and
2. Ensuring that essential records are accessible from designated COOP locations.

e. **Managers and Supervisors** are responsible for:

1. Ensuring that a records management program is implemented within their organization.
2. Understanding and emphasizing the importance of records management to staff.
3. Designating selected staff as records contacts in order to meet recordkeeping requirements and responsibilities as described in this document and the CSB Investigation Protocol (Board Order 40).
4. Providing support, time, and resources for records contacts to successfully carry out their recordkeeping responsibilities.
5. Certifying the completion of files and the authenticity of records when requested, or designating appropriate staff to do so (e.g., for litigation and FOIA requests).
6. Coordinating timely file retrieval for the FOIA Officer or OGC.

7. Ensuring that the organization's file plans are current.
8. Obtaining training so that they and their staff can carry out recordkeeping responsibilities.
9. Implementing an essential (vital) records program within the organization.
10. Participating in records program reviews and assessments and developing and implementing corrective action plans to address gaps.
11. Supporting initiatives to move from paper to electronic recordkeeping.
12. Ensuring that all records of separating employees have been identified, that temporary records that have met their retention are properly disposed of according to applicable records schedules, and that records that must be preserved have been assigned to other employees.

f. **Users** – All CSB employee are responsible for:

1. Creating and managing the records necessary to document the Agency's official activities and actions, including those records generated by CSB contractors, in accordance with CSB recordkeeping requirements.
2. Destroying records only in accordance with approved records schedules and never removing records from CSB without authorization.
3. Filing records for safe storage and efficient retrieval and maintaining personal papers and non-record materials separately from official CSB records.
4. Ensuring that if secondary e-mail accounts for individuals, groups or systems are created or used for business reasons, any records created are appropriately stored and managed.
5. Identifying all records, in any format, in the employee's possession, and transferring them to another CSB custodian before separating or transferring to another organization. Note: Non-records and records that have met their disposition per appropriate records schedule should be destroyed unless subject to FOIA, litigation or audit. Records containing PII must be disposed of in accordance with Board Order 44.
6. Taking annual records management training and any other related training and participating in records management activities such as records management days and records clean-up days.
7. Contractors, grantees, and others doing work on behalf of the CSB are required to take annual records management training, as appropriate.

8. DEFINITIONS

Below is a list of common records management terms. For a more comprehensive list, visit the CSB intranet.

a. **Archive –** a place where records are stored and preserved permanently, not to be confused with the IT term "archiving" which means backing up files.

b. **Audiovisual Records –** records created or stored in an audio, visual or combination media, such as video tapes, digital photos, and audio tapes.

c. **Disposal –** destruction of records by shredding or burning.

d. **Electronic Records –** all information meeting the definition of records that is created, maintained, or stored on electronic media, such as magnetic tapes, magnetic disks, optical disks, CD's and drums.

e. **Permanent Records –** archival records appraised by NARA as having enduring value because they document the organization and function of the agency that created or received them or because they contain significant information on persons, things, and problems concerning the agency. These records have historical value.

f. **Personal Papers –**papers and files of a private non-official character that are kept in the office of a Federal employee, official, or contractor that are not federal records and pertain only to that individual's personal affairs.

g. **Record** – all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any agency of the Federal government or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the date in them (44 U.S.C. § 3301).

h. **Records Disposition** – the system designed to ensure efficient, prompt, and orderly reduction in the quantity of records to provide for the proper maintenance of records deemed appropriate for permanent preservation.

i. **Records Schedule** – specify how long an agency's noncurrent records will be retained at a Federal Records Center, possible transfer to the custody of the National Archives for permanent retention, or eventual destruction after a specific period of time based on administrative, fiscal, and legal values. General Records Schedules are issued by the National Archives and Records Administration (NARA) and govern the disposition of certain types of records common to most agencies.

j. **Records Management** – the field of management responsible for the systematic control of the creation, maintenance, use, and disposition of records.

k. **Records Management Official** – the official responsible for the direction of records disposition management for case file records is the CSB Director of Records Management.

l. **Unofficial Record** – "non-record materials," including: extra copies, such as distribution copies, stock copies, and copies maintained for convenience of reference, which are not Federal records. In addition, when a record exists in multiple formats, such as in paper and electronic form, then generally both the paper and the electronic copies are considered distinct records.

m. **Non-record** – a document, regardless of form or characteristic, that was used primarily for reference or is considered excess, including:

1. Blank copies of forms;
2. Duplicate copies of material not used for decision making;
3. Reference materials;
4. Data analysis and summaries;
5. Drafts (NOTE: Drafts and working copies should be filed and maintained as part of the agency's records if they explain how the agency formulated and executed significant program policies, decisions, actions or responsibilities; or contain unique information such as annotations or comments);
6. Routine requests for case reports and data;
7. Extra copies of documents preserved for convenience of reference;
8. Stocks of processed documents, such as publications; and
9. Preliminary worksheets.

n. **Personal Papers/Files** – materials that belong to an individual, not the agency.

o. **Vital Record** – records necessary for the CSB to continue operations during an emergency or disaster, such as fire, flood, or explosion.

p. **Permanent Record** – records appraised by NARA that have sufficient historical or other value to warrant preservation beyond the time they are needed for administrative, fiscal, or legal purposes.

q. **Temporary Record** – include administrative or obviously short-term program records. These records are pre-approved by NARA for disposal, either immediately or after a specified retention period through the use of the General Records Schedules, also known as the GRS. Examples include:

1. Correspondence below the office director level;
2. Convenience files;
3. Requests for printing services;
4. Contracts;
5. Travel documents;
6. Contracts;
7. Supervisors' personnel files;
8. Routine reports; and
9. Time and attendance (T&A) cards.

r. **Technical Reference Files** – reference material or publications directly related to the work of the office that have no record value. Examples include:

1. Periodicals;
2. Equipment and software manuals;
3. Technical reports;
4. Copies of reports or articles copied from the Internet;
5. Training manuals; and
6. Pamphlets.

9. WAIVERS

a. **Waiver Process.** The Director of Records Management may grant waivers to any provisions of this Order for sufficient cause.

b. **Applications.** Applications for waivers to specific provisions should contain (1) identification of the relevant provision; (2) a listing of reasons why the provision cannot be applied or maintained; (3) an assessment of impacts results from non-compliance.

c. **Notification.** The Agency Records Officer will notify the requesting office in writing of the disposition of the decision on the waiver request within 60 days of receipt of the request.

10. RECORDKEEPING

The Director of Records Management is responsible for establishing and maintaining the records systems for records management. Pertinent retention schedules for records management records must be retained in accordance with the applicable General Record Schedule from National Archives and Records Administration (NARA) and/or any CSB recordkeeping requirement.

11. REVIEW AND UPDATE

The Director of Records Management and General Counsel will review this Order every two years and make suggestions for appropriate revisions by September 30 of each fiscal year. The Director of Records Management is responsible for coordinating the review.

***

Adopted May 20, 2003; amended, April 16, 2016.