



U.S. Chemical Safety and Hazard Investigation Board

SUBJECT: Records Management Program

Contents

1.	PURPOSE	2
2.	EFFECTIVE DATE.....	2
3.	SCOPE.....	2
4.	BACKGROUND	2
5.	REFERENCES	2
6.	POLICY	3
7.	RESPONSIBILITIES.....	3
8.	DEFINITIONS.....	6
9.	RECORDS MANAGEMENT REQUIREMENTS.....	8
10.	WAIVERS	14
11.	RECORDKEEPING	14
12.	REVIEW AND UPDATE	14

1. **PURPOSE.** This Order establishes principles, responsibilities, and requirements for managing Chemical Safety and Hazard Investigation Board (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 created or received by the CSB. This Order applies to all employees, agents, and contractors (pursuant to the Federal Acquisition Regulation (FAR)) performing work for the CSB.
4. **BACKGROUND.** The Federal Records Act of 1950 (FRA), as amended, requires all federal agencies to create 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 FRA 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 of a records management program 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 but not limited to, 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. 5 U.S.C., § 552, The Freedom of Information Act, as amended by Public Law 104-231
 - b. 44 U.S.C. Chapter 22 - The Presidential and Federal Records Act Amendments of 2014
 - c. 44 U.S.C. Chapter 29 - Records Management by the Archivist of the United States
 - d. 44 U.S.C. Chapter 31 – Records Management by Federal Agencies (Federal Records Act)
 - e. 44 U.S.C. Chapter 33 – Disposal of Records
 - f. 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)
 - g. 18 C.F.R. Chapter I, Subchapter W – Organization, Mission, and Functions;

Operations During Emergency Conditions

- h. 36 C.F.R. Chapter XII, Subchapter B – Records Management
 - i. M-19-21 Transition to Electronic Records
 - j. M-23-07 Update to Transition to Electronic Records
 - k. OMB Circular A-123 – Management’s Responsibility for Internal Control
 - l. OMB Circular A-130 – Management of Federal Information Resources
6. **POLICY.** This Order establishes requirements whereby CSB records are effectively and efficiently managed throughout their lifecycle to facilitate the accomplishment of the 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.
7. **RESPONSIBILITIES.**
- a. **Chairperson and Board** – As the agency head, the CSB Board, along with the Chairperson, is responsible for the entire records management program in the agency. The FRA states that the head of each federal agency shall:
 - (1) Make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency’s activities. (44 U.S.C., §3101)
 - (2) Establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. (44 U.S.C., §3102)
 - b. **Agency Records Officer (ARO)** – has the authority, subject to the direction of the Chairperson and the Board, to take all actions necessary and proper to ensure that the CSB meets all federal recordkeeping requirements. The ARO is responsible for creating, implementing, and managing the CSB’s records management program, subject to the direction of the Chairperson and the Board, including:
 - (1) Ensuring that senior agency officials are aware of their programmatic and individual records management responsibilities and requirements.
 - (2) Serving as the official responsible for overseeing the agency’s records management program.
 - (3) Ensuring that the agency has an up-to-date records management directive.
 - (4) Creating and maintaining a network of Records Liaisons responsible for overseeing the program in cooperation with the ARO.

- (5) Serving as the primary agency official who coordinates records management matters with the National Archives and Records Administration (NARA) and other oversight agencies such as the Office of Management and Budget (OMB) and the General Services Administration (GSA).
- (6) Coordinating the development of records schedules with NARA and agency staff and officials.
- (7) Ensuring that recordkeeping requirements are established, implemented, and periodically updated for all offices at all levels and for all record media, including electronic and other special records.
- (8) Providing technical advice and training to all agency offices on establishing and maintaining effective records management programs.
- (9) Evaluating recordkeeping practices to determine the effectiveness of the program.
- (10) Obtaining NARA's Agency Records Officer Credential.

c. **Records Liaisons** – are responsible for:

- (1) Being the office-level representative for records management matters and complying with guidance issued by the ARO subject to the review and approval of the Chairperson.
- (2) Ensuring that the office's records are listed on the office file plan and are described accurately in the agency's records schedule.
- (3) Following assigned records schedules to ensure proper disposition of the office's records including the disposal of temporary records when their retention periods expire and the timely transfer of permanent records to NARA with approval from the ARO.
- (4) Assisting the office manager in reminding the staff not to mix personal papers and non-record materials with federal records and not to remove records from the office without proper authorization.
- (5) Assisting the office manager in implementing procedures to prevent departing employees from destroying active records or removing records from the agency's custody.
- (6) Cooperating with the ARO in periodic evaluations of the office's records.

d. **Chief Information Officer (CIO)** – is responsible for:

- (1) Serving as the agency official responsible for the information resources management program, which is the process of managing information resources to accomplish agency missions and encompasses both information itself and related resources or assets, such as personnel, equipment, funds, and information technology.

- (2) Coordinating with the ARO to ensure that the design and implementation of the agency's information systems incorporate federal and agency records management requirements.

e. **General Counsel** – is responsible for:

- (1) Providing legal advice and counseling on records management issues in accordance with pertinent federal recordkeeping requirements.
- (2) Placing litigation holds on records that are responsive to litigation involving the agency.

f. **Continuity of Operations Program (COOP) 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.

g. **Managers and Supervisors** – are responsible for:

- (1) Ensuring that a records management program is implemented within their respective offices.
- (2) Ensuring that the office has a designated Records Liaison who coordinates the office's records management activities with the ARO.
- (3) Providing support, time, and resources for Records Liaisons to successfully carry out their recordkeeping responsibilities.
- (4) Ensuring that staff creates and maintains records documenting the office's program and administrative activities.
- (5) Working with the ARO to ensure that all of the office's records are listed on the office file plan (see section 9 below) and are described accurately in the agency's records schedules.
- (6) Reviewing the office file plan annually.
- (7) Understanding and emphasizing the importance of records management to staff, reminding staff not to mix personal papers and non-record materials with federal records and not to remove records from the office without proper authorization.
- (8) Obtaining training so that they and their staff can carry out recordkeeping responsibilities.
- (9) Implementing procedures to prevent departing employees from destroying active records or removing records from the agency's custody.

(10) Ensuring that staff follows assigned records schedules in carrying out the disposition of the office's records.

(11) Cooperating with the Records Liaison and the ARO in efforts to promote and evaluate the office's records management activities.

h. **Users** – All CSB employees and contractors are responsible for:

(1) Creating and managing the records necessary to document the agency's official activities and actions, including filing records for safe storage and efficient retrieval in accordance with the CSB's recordkeeping requirements.

(2) Obtaining basic records management training and guidance from the Records Liaison or the ARO and participating in records management activities.

(3) Cooperating with the Records Liaison to ensure that all records are listed in the office file plan and are described accurately in the agency's records schedules.

(4) Recognizing that the office's records are government property and consist of recorded information (documentary materials) required by law or used to conduct agency business.

(5) Not mixing personal papers and non-record materials with federal records and never removing records from CSB without authorization.

(6) 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.

(7) Cooperating with the Records Liaison and ARO in transferring permanent records to NARA.

(8) Cooperating with the Records Liaison in destroying records only as authorized by the assigned records schedule and approved by the ARO.

(9) Identifying all records, in any format, in the employee's possession, and transferring them to another CSB custodian before separating from the CSB or transferring to another agency or organization.

8. **DEFINITIONS.** Below is a list of common records management terms.

a. **Archive** – a place where records are stored and preserved, 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. **Destruction** – The disposal of documents of no further value by incineration, maceration, pulping, or shredding.

- d. **Disposition** – Instructions for what is to be done with records that are no longer needed to support agency business. There are two types of dispositions for records: (1) Temporary – Records with a temporary disposition will eventually be destroyed or deleted when all relevant business needs have expired, and (2) Permanent – Permanent records that contain historically significant materials, provide evidence of agency actions, or document important events in national history, will be preserved by NARA for the life of the republic.
- e. **Electronic Records** – Records stored in a form that be accessed or processed only with a computer or other electronic device. Records can be numeric, graphic, and text information; media can include, but are not limited to, flash drives, compact disks, and external hard drives.
- f. **Essential Records** – Records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster 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”).
- g. **General Records Schedule (GRS)** – the GRS is issued by the Archivist of the United States under the authority of 44 U.S.C., §3303a to provide disposition authority for records common to several or all federal agencies. The GRS covers records documenting administrative functions rather than program functions. Agencies must apply the GRS to the greatest extent possible.
- h. **Inventory** – Annual survey of agency records and non-record materials conducted to develop records schedules and to identify various records management challenges.
- i. **Lifecycle** – The management concept that records pass through three stages: creation, maintenance and use, and disposition.
- j. **Metadata** – Data describing stored data: that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records.
- k. **Non-record Materials** – Non-record materials are documentary materials that do not meet the statutory definition of records. The United States Code defines “non-record materials” to include material such as unofficial copies of documents kept only for convenience or reference, stocks of publications and near-print documents, and library or museum material intended solely for reference or exhibition.
- l. **Permanent Records** – Records appraised by NARA as having sufficient historical or other value to warrant preservation for the life of the republic in the National Archives beyond the time it is needed for administrative, legal, or fiscal purposes.
- m. **Personal Papers** – Personal Papers are documentary materials belonging to an individual that are not used to conduct agency business.
- n. **Records** – Per 44 U.S.C. §3301, the term “record,” “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.”

- o. **Record Series** – A group of records that are related to each other and typically managed together. These records are usually linked by a specific function, subject, activity, or transaction, and are organized within a filing system.
- p. **Records Management** – The field of management responsible for the systematic control of the creation, maintenance, use, and disposition of records.
- q. **Temporary Records** – Record approved by NARA for disposal after a specified retention period.
- 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
 - (6) Pamphlets
- s. **Transitory Records** – Transitory records are required for only a short time (generally less than 180 days). They are not required to meet legal or fiscal obligations or to initiate, sustain, evaluate, or provide evidence of decision-making. The following are possible examples of transitory records. Even with these examples, however, the records must meet the conditions defined above:
 - (1) Transmittal documents such as email, letters, cover memos, and facsimile cover sheets.
 - (2) Received copies of circulated internal information such as agency instructions, notifications, circulars, newsletters, and email blasts to employees.
 - (3) Received copies of circulated internal information such as agency instructions, notifications, circulars, newsletters, and email blasts to employees.
 - (4) “To-do”, task lists, or assignments, including for custodial services or minor repair work.
 - (5) Data output files from electronic systems for information sharing or short-term reference.

9. **RECORDS MANAGEMENT REQUIREMENTS**

- a. **Managing Records.** Records are managed for the benefit of the CSB and its staff, stakeholders and the public. Records are managed throughout the record lifecycle (creation/capture, classification, maintenance, retention, and disposition) by being properly identified, classified using a taxonomy, inventoried, and scheduled. The CSB must ensure that all federal records are created, retained, and managed in electronic formats with appropriate metadata and consistent with records management laws and regulations. Federal records are defined in 44 U.S.C., § 3301, as “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.” Non-record materials include library or museum material; duplicate copies of records for reference; copies of stocks or publications; most draft or non-final documents; and personal files. Below are the basic categories of record and non-record materials.

- (1) Permanent Records are records that NARA deems as having enduring historical value to be preserved for the life of the republic in the NARA archives. Only a small percentage of federal records are of permanent value. These records are accumulated at federal agencies and transferred to NARA once they no longer serve a business purpose for the agency.

NARA appraises records to determine appropriate retention periods and assigns record schedules to them that give agencies the authority to dispose of federal records, any record that is unscheduled is to be treated as a permanent record pending the assignment of a record schedule.

- (2) Temporary Records are not considered to have enduring historical or informational value and are therefore authorized for destruction by the agency after the retention period specified in the record schedule.
- (3) Non-Record Materials are related to agency business but do not meet the statutory definition of federal records, these documents are not to be filed with record material; however, they are still government-owned and must be protected from unlawful removal. Non-record materials must be reviewed annually to determine if they are needed to conduct agency business.
- (4) Personal Papers are documentary materials belonging to an individual that are not used to conduct agency business. Personal papers are excluded from the definition of federal records and are not owned by the government and therefore must not be intermingled with government-owned records or documents.

- b. **File Plans.** File Plans are an accounting of a department or program’s record series and associated information. At a minimum, a file plan includes each record series’ description, records schedule, disposition instructions (retention period), disposition authority, storage locations, and the office with custodial responsibility. Each business unit or program at the CSB is required to maintain a file plan that documents all records series held by that department.
- c. **Record Schedules.** A records schedule is: (1a) An SF-115, Request for Records Disposition Authority, that has been approved by NARA to authorize the disposition of federal records, or (2b) Aa GRS item issued by NARA. A records schedule identifies records as either temporary or permanent and provides mandatory instructions for the disposition of the records (including the transfer of permanent records and destruction of temporary records) when they are no longer needed by the agency.

All records schedules must be approved by NARA, records not associated with a NARA-approved record schedule are unscheduled and must be treated as permanent. Federal

records must be scheduled either by an agency schedule or a record schedule from the General Records Schedules (GRS) provided by NARA. The GRS can be found on NARA.gov at <https://www.archives.gov/records-mgmt/grs>. Example below:

Item #	Records Description	Disposition Instructions	Disposition Authority
GRS 2.1 Item 060	Employment eligibility verification records. Employment eligibility verification form I-9 and any supporting documentation.	Temporary. Destroy 3 years after employee separates from service or transfers to another agency.	DAA-GRS-2017-0007-0007

Use of GRS records schedules are mandatory for records already identified in the GRS. A deviation may be requested from NARA if the agency requires a record series for longer than the retention period mandated by NARA. The record schedules in the GRS address administrative support records common across all agencies of the federal government, records related to the mission of a federal agency must be scheduled by the agency itself and approved by the Archivist of the United States at NARA. Agencies request disposition authority from NARA using standard form 115 (SF-115). The agency describes groups of records linked by specific functions, subjects, activities or transactions, and proposes retention periods and disposition instructions for those records. Approval of agency record schedules by NARA confers disposition authority to the agency for those records allowing for disposal or transfer.

Approved CSB record schedules are located on NARA.gov at <https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/independent-agencies/rg-0608>.

- d. **CSB Records Systems.** The CSB's primary means for records storage are the agency's shared drives, Hewlett-Packard Content Manager, Microsoft SharePoint, and the Microsoft 365 suite. These repositories are the preferred storage method for the CSB's records. Other electronic information systems (EIS) are also used to conduct agency business, such as EIS's or websites administered by other agencies. When CSB records or work processes are stored in/occur on an EIS, agency employees shall ensure that the records and processes are represented on the office's file plan with the associated EIS as the listed storage location.
- e. **E-mail and Messaging Records.**
 - (1) **CAPSTONE Records.** CAPSTONE is a role-based approach to managing federal email and messaging records. NARA Bulletins 2013-02 and 2023-02 provide guidance for agencies that choose to take this approach. The CSB's CAPSTONE form (NA-1005) was approved by NARA on 30 August, 2024. The associated record schedules are published in section 6.1 of the GRS. Senior agency officials who are responsible for policy and mission-related actions are designated as CAPSTONE officials. The email and messages of those officials are captured in an archiving system (Microsoft Purview) and are permanent records. Email and messages of non-CAPSTONE staff are also captured and archived using a CAPSTONE approach, although these are temporary records.

- (2) Archiving. The CSB uses Microsoft Purview to archive the agency's email and messaging records. Records of CAPSTONE Officials are permanent records and will be maintained for 25 years before being culled, then transferred to the National Archives in 5 year blocks. Email and messaging records of non-CAPSTONE staff are maintained for 7 years, then destroyed.
- (3) Managing E-mail and Messaging Records. Email and messaging records can be managed in one of three ways; using the CAPSTONE approach, filing an email as supporting documentation to another record, or through traditional records management.

Managing email and messaging records using the CAPSTONE approach described previously is a background process that requires no input from end users.

Supporting documentation refers to an email or message that contains information that is necessary for inclusion with another record. In that case, the email or message should be copied from the messaging system to that record file. Because emails or messages of this type are included with another record as supporting documentation, they will follow the record schedule of the associated records and be dispositioned along with the record file.

Traditional records management refers to the removal of records from an EIS to be filed in one of the CSB's records systems. This can be to allow easier retrieval of the records, to allow colleagues to access the records for reference, or to ensure the records are maintained for as long as required by the records schedule that grants disposition authority for those records.

- (4) Personal or Multiple Accounts. 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 system must be used and a federal record is created or received on a non-CSB 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 e-mail system, staff must determine whether the record is a transitory record or must be captured in a CSB records 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.

Use of personal social media tools outside of official CSB accounts administered by the office of public affairs (for example, but not limited to: YouTube, Twitter, LinkedIn, Facebook) is prohibited for conducting CSB business. However, this does not prohibit CSB employees from using personal social media tools to disseminate publicly available information about the CSB, such as a publicly announced CSB job opening or a new investigation report or safety video that the CSB has publicly released.

- f. **Access and Protection of Records.** CSB records must be maintained, captured, identified on a file plan, 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 applicable statutory requirements.

All CSB employees are responsible for preventing the unauthorized transfer, removal, possession, damage, or destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of the CSB or destroyed except for in accordance with the assigned records schedule and with approval from the Agency Records Officer (ARO). Willful and unlawful destruction, damage, transfer, removal, or possession of federal records may include disciplinary actions and/or fines, imprisonment, or a combination of these penalties, imposed by 18 U.S.C. 2701. Any unlawful or accidental removal, defacing, alteration, or destruction of records must be promptly reported to NARA in accordance with 36 C.F.R. 1230.

- g. **Procedures for Reporting Unlawful or Accidental Destruction or Loss of Records.**

- (1) The Records Liaison must report, in writing, any unlawful or accidental removal, defacing, alteration, or destruction of records to the ARO via the office's director within 24 hours of discovery. The report should be as complete as can be determined and include a description of the records, volume and dates (if known), office of origin, and an explanation of the exact circumstances surrounding the unauthorized action.
- (2) The ARO will work with staff to attempt to salvage, retrieve, or reconstruct the records, and establish safeguards to prevent further losses. The ARO will include those actions in the report and provide it to the CSB's assigned NARA Archivist within 5 days of discovery of the violation.

- h. **Records Disposal Process.** The following procedures will be used by the CSB to request authorization for the disposal of temporary records per assigned record schedules. This process includes an inventory that collects volumes of the disposed and remaining records. Completed forms will be maintained by the ARO.

- (1) With assistance from office staff, the Records Liaison will prepare the records disposition and inventory form for both the disposition of eligible records and the inventory of active records. The Records Liaison will forward the form to the office director for approval/disapproval and signature. Upon completion, the office director will forward the completed form to the ARO.
- (2) Upon concurrence of the office director, the ARO will authorize or deny disposition by signing the form and notifying the Records Liaison.
- (3) Once approved for disposition the Records Liaison will dispose of the records. The Records Liaison will then certify destruction of temporary records by signing the form, then forwarding the form to the ARO.
- (4) If there are records that are eligible for destruction but are disapproved for

destruction, the office director must fill out and sign a memorandum to the record to provide justification for the continued retention of those records.

i. Information/Record Sensitivity Categorization and Marking Requirements.

- (1) General principles. The selection and use of information technology security controls, records management retention, 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.
- (2) Sensitivity Labelling policy. The sensitivity of 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. The CSB has implemented sensitivity labels through the Microsoft Purview system. The sensitivity label program allows the CSB to require that documents made or received through the Microsoft 365 platform (Word, Excel, Outlook, etc.) are labelled by the end-user. This allows for a greater understanding of how information is accumulated at the agency and how to manage that information. Below are the sensitivity label categories that end-users must choose from to apply to the documents that they generate or receive:
 - (a) Personal Non-Business. To be applied to non-business, personal data. Compromise of this non-sensitive information would have no negative consequences.
 - (b) Public. To be applied to business information that is specifically prepared for and releasable to the public.
 - (c) Non-Public. To be applied to business information that is not intended for public consumption. This category will cover the majority of documents at the agency, this includes administrative, financial, and operational documents. Compromise could cause significant financial loss or operational disruption, or require legal action for correction. The CSB works with outside entities and agencies and has therefore implemented access controls with the below sub-categories:
 1. Unrestricted – Can be shared externally.
 2. Employees Only – Can be shared internally with CSB employees and contractors.
 3. Government Only – Can only be shared internally with government employees.

(d) Confidential. To be applied to sensitive business data. Compromise of this category of information would cause extremely grave injury to government interests. Confidential information includes trade secrets, processes, and investigatory materials. Compromise could cause major financial loss or operational disruption, or require legal action for correction. The CSB works with outside entities and agencies and has therefore implemented access controls with the below sub-categories:

1. Unrestricted – Can be shared with externally if deemed appropriate by data owner.
2. NDA Restricted – Can be shared with externally under the restrictions of a non-disclosure agreement (NDA).
3. Employees Only – Can be shared internally with CSB employees and contractors.
4. Government Only – Can only be shared internally with government employees.

10. **WAIVERS**.

- a. **Waiver Process.** In consultation with the Chairperson, the ARO 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; and (3) an assessment of impacts results from non-compliance.
- c. **Notification.** The ARO 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.

11. **RECORDKEEPING**. Records created as a result of this Order, regardless of media and format, shall be managed in accordance with pertinent federal recordkeeping requirements.

12. **REVIEW AND UPDATE**. The ARO and General Counsel will review this Order at least every two years and make recommendations to the Chairperson and the Board for appropriate revisions, if any. The ARO is responsible for coordinating the review.

U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

Adopted May 20, 2003; Amended, April 16, 2016; Amended, August 12, 2026.