U.S. Chemical Safety and Hazard Investigation Board

SUBJECT: Protection of Personally Identifiable Information and Privacy Act Records

CONTENTS

1. Purpose 2
2. Effective Date 2
3. Scope 2
4. References 2
5. Policy 2
6. Definition of Personally Identifiable Information (PII) 2
7. Other Definitions 4
8. Responsibilities 5
9. Rules of Behavior 6
10. Consequences and Corrective Actions 7
11. Protection of PII 9
12. Use of Social Security Numbers 11
13. Review of PII Holdings 12
14. Privacy Act Reviews 12
15. Training 13
16. Review and Update 13

1. **PURPOSE.** This Order establishes policies, rules, and procedures for the Chemical Safety and Hazard Investigation Board (CSB) for the protection and safe handling of Personally Identifiable Information and Privacy Act records.

2. **EFFECTIVE DATE.** This Order is effective as of the date of Board approval.

3. **SCOPE.** This Order applies to all CSB employees and information systems. The provisions of this Order also apply to the personnel and information systems of CSB contractors, to the extent that such contractor personnel and systems are used to handle, maintain, and/or process CSB records.

4. **REFERENCES.** The following statutes, regulations, and other authorities provide the basis for the provisions of this Order:

   - Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 et seq.
   - The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
   - 5 C.F.R. Part 293, Personnel Records.
   - Executive Order 13402 (May 10, 2006), Strengthening Federal Efforts to Protect Against Identity Theft, as amended by Executive Order 13414 (Nov. 3, 2006).
   - Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources.
   - OMB Memoranda: M-07-16 (May 22, 2007), Safeguarding Against and Responding to the Breach of Personally Identifiable Information; M-06-19 (July 12, 2006), Reporting Incidents Involving Personally Identifiable Information; M-06-16 (June 23, 2006), Protection of Sensitive Agency Information.
   - Office of Personnel Management Memorandum (June 18, 2007), Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft.

5. **POLICY.** It is the policy of the Board that records containing personally identifiable information shall be maintained with appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of such records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained.

6. **DEFINITION OF PERSONALLY IDENTIFIABLE INFORMATION (PII).**

   a. **OMB Definition.** OMB, in Memorandum M-06-19 (July 12, 2006), defines the term personally identifiable information (PII) to mean:

      Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to

distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

b. **Identification of PII.** To determine whether any particular item of information maintained by the CSB is covered by the definition of PII, the following analytical framework shall be used:

(1) Information may be identified as PII regardless of the format in which it is maintained (e.g., hard copy or electronic) or the media on which it is stored (e.g., disk-based storage, removable storage, back-up media).

(2) Social Security Numbers in any form, including by themselves, are always PII.

(3) One or more items from Set A, below, in combination with one or more items from Set B, below, OR multiple items from Set A alone, also constitute PII.

(a) Set A:

- Name
- Driver's License number
- Place of birth associated with an individual
- Date of birth associated with an individual
- Mother's maiden name associated with an individual
- Biometric record associated with an individual (e.g., fingerprint, iris scan, DNA)

(b) Set B:

- Medical history information associated with an individual
  - Medical conditions, including history of disease
  - Metric information (e.g., weight, height, blood pressure)
  - Medical research information that has not been de-identified
- Criminal history associated with an individual
- Employment history and other employment information associated with an individual
  - Performance ratings
  - Disciplinary actions
  - Performance elements and standards (or work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal
  - Leave types or balances
- Financial information associated with an individual
  - Credit card numbers
  - Bank account numbers
  - Banking activity

- Security clearance history or related information (not including actual clearances held)

c. **Exclusions.** The following types of information are not considered PII, unless they are located in a Privacy Act System of Records:

- Agency phone numbers
- Agency street addresses
- Agency e-mail addresses
- Digital pictures
- Information pertaining to employee work status (e.g., John Doe is on leave today)
- Medical information included in a safety report
- Employment information that is not PII even when associated with a name:
  - Resumes, unless they include an SSN
  - Present and past position titles and occupational series
  - Present and past grades
  - Present and past salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials)
  - Present and past duty stations and organization of assignment (including room and phone numbers; organization designations; work e-mail address; or other identifying information regarding buildings, room numbers, or places of employment)
  - Position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) the release of which would not interfere with law enforcement programs or severely inhibit agency effectiveness
  - Security clearances held
  - Written biographies
  - Academic credentials – degrees held (e.g., Ph.D., MS, BS, AA); schools attended; major or area of study
- Personal information stored by individuals about themselves on their assigned workstation or laptop (unless it contains an SSN)

7. **<u>OTHER DEFINITIONS</u>.**

a. **Breach** – the loss of control, compromise, unauthorized acquisition, unauthorized access, unauthorized disclosure, or any similar situation in which persons or entities other than authorized users and/or for an other than authorized purpose gain access or potential access to PII and/or Privacy Act records, whether physically or electronically.

b. **Information system** – a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

c. **Privacy Act record** – an item or grouping of information that specifically identifies (e.g., by name or by Social Security Number), and describes something about, a particular individual, and which is maintained by the CSB in a Privacy Act System of Records. By definition, Privacy Act records will always contain PII. However, PII also may be found in records not covered by the Privacy Act.

d. **Privacy Act System of Records** – a group of records under the control of the CSB, from which records about particular individuals are actually and systematically retrieved by reference to some personal identifier. CSB-specific Systems of Records, as well as government-wide Systems of Records used by the CSB, are described in the CSB Notice of Systems of Records, which is posted on the agency's web site.

e. **Security controls** – the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

f. **User** – any person or entity with authorized access to CSB information systems.

8. **RESPONSIBILITIES.**

a. **Chairperson** – The Chairperson, acting on behalf of the Board, is responsible for overseeing and ensuring the effectiveness of all CSB efforts to ensure the proper handling and protection of PII. Among other responsibilities, this includes approving the issuance and use of a supplemental user agreement regarding PII and Privacy Act records.

b. **Senior Agency Official for Privacy** – The Senior Agency Official for Privacy is responsible for supervising the implementation of this Order. In consultation with the IT Security Officer and the General Counsel, develops and proposes to the Chairperson for approval a supplemental user agreement regarding PII and Privacy Act records.

c. **Information Technology (IT) Security Officer** – The IT Security Officer is responsible for implementing, as described in this Order, necessary security controls that ensure the proper handling and protection of PII.

d. **Managers and supervisors** – Managers and supervisors are responsible for supporting and cooperating with the implementation of the policies, rules, and procedures set forth in this Order, within the units for which they are responsible. Managers and supervisors must clearly inform subordinates that the proper handling and protection of PII is a high priority and that there are serious consequences for mishandling of PII.

e. **Users** – Users are responsible for familiarizing themselves with, and complying with, the policies, rules, and procedures set forth in this Order. As directed, users must participate in training on the proper handling and protection of PII.

9. **RULES OF BEHAVIOR.**

a. Every CSB employee, and all agency contractor personnel, must be aware of the nature of PII and Privacy Act records; and of the restrictions on access to, requirements for protection of, and consequences for mishandling PII and Privacy Act records. As a condition of access to CSB information systems, every CSB employee, and all agency contractor personnel, must complete annual training on, and sign a supplemental user agreement regarding, PII and Privacy Act records.

b. CSB employees and contractor personnel whose duties require the handling of PII and/or Privacy Act records shall take care to protect the integrity, security, and confidentiality of such information/records. Such employees and contractor personnel shall access PII and/or Privacy Act records only when they have a need to know in order to discharge their official duties, and shall not exceed their level of authorized access to such information/records.

c. Any CSB employee or contractor personnel who become aware of a suspected or known breach of PII and/or Privacy Act records must immediately report such breach to the Senior Agency Official for Privacy and to the IT Security Officer, in accordance with section 8 of the *Information Security Incident Reporting Policy* (Board Order 034, Appendix F) and section 8 of the *Breach Notification Policy* (Board Order 034, Appendix J).

d. Managers and supervisors must instruct, train, and supervise their subordinates on safeguarding PII. Contracting Officer's Technical Representatives (COTR) must ensure that the contracts for which they are responsible include provisions requiring the contractor to instruct, train, and supervise its personnel on safeguarding PII; and must monitor contractor performance to ensure compliance.

e. Managers and supervisors whose subordinates are responsible for implementing and maintaining security controls for PII shall ensure that the performance plans for such subordinates include elements and standards for the evaluation of their performance in carrying out those security responsibilities.

f. CSB employees and contractor personnel shall not disclose PII or Privacy Act records unless: (1) a disclosure is authorized or required by law, (2) the intended recipient of the disclosure is authorized by law to receive the information/records, and (3) the employee/contractor personnel is authorized to release CSB records. In any case where there is doubt about the propriety of a proposed disclosure, it should be reviewed by the Management Official responsible for the information/records in question, and by the Office of General Counsel.

g. CSB employees shall not alter or destroy records containing PII, unless such action is authorized or required by law, and is part of the employee's official duties. In any case where there is doubt about the propriety of a proposed action, it should be reviewed by the Management Official responsible for the record(s) in question, and by the Office of General Counsel.

h. **Rule for personal digital devices.** CSB employees are not permitted to download, handle, or store PII or Privacy Act records on non-agency-issued personal digital devices (e.g., personal digital assistants, smartphones, etc.). Personal digital devices issued by the CSB (i.e., BlackBerries) must be protected with a security time-out, access password, and encryption, if technically feasible. Devices for which such protection is not technically feasible may not be used to store PII or Privacy Act records, and messages containing PII or Privacy Act records should be deleted from such devices as soon as possible. Employees must immediately report to the IT Security Officer the loss or theft of a CSB-issued personal digital device, so that appropriate security responses can be initiated.

i. **Rule for personal identity verification cards.** In accordance with Homeland Security Presidential Directive 12 (HSPD-12), the CSB anticipates that it will begin issuing personal identity verification (PIV) cards to employees. PIV cards include a chip containing several items of PII about the cardholder. To prevent surreptitious access to the chip, employees are required to carry their PIV cards in a protective sleeve provided by the agency. To further ensure the security of this information, employees and contractor personnel are not permitted to possess within the CSB offices any non-agency-issued device capable of reading or scanning a PIV card chip. For the protection of their own personal information and the integrity of the PIV system, CSB employees are required to immediately report to the Chief Personnel Security Officer the loss or theft of a PIV card.

10. **CONSEQUENCES AND CORRECTIVE ACTIONS.**

a. **Consequences.**

(1) In addition to the specific situations listed below, failure to comply with any Rule of Behavior set forth in section 9 of this Order – or any other requirement established by statute, regulation, or Board Order for the handling and protection of PII and Privacy Act records – may be considered misconduct (in the case of CSB or other U.S. Government employees) or a default (in the case of contractors and their personnel).

(2) Exceeding one's level of authorized access to, or making an unauthorized disclosure of, PII or Privacy Act records may be considered misconduct (in the case of CSB or other U.S. Government employees) or a default (in the case of contractors and their personnel). Depending on the facts and circumstances, an act of unauthorized access or disclosure may also be a violation of civil and/or criminal law.

(3) Failure to immediately report a suspected or known breach of PII and/or Privacy Act records of which an individual has become aware may be considered misconduct (in the case of CSB or other U.S. Government employees) or a default (in the case of contractors and their personnel).

(4) Failure by a manager, supervisor, or COTR to take appropriate action upon discovering a breach of PII or Privacy Act records involving employees/contractor personnel for whom they are responsible, or to take required steps to prevent such a breach, may be considered misconduct.

(5) Failure by a manager or supervisor to adequately instruct, train, and supervise his or her subordinates on their responsibilities with respect to PII and Privacy Act records may result in a negative performance evaluation, consistent with Board Order 010, *Performance Appraisal Program*. Failure by a COTR to ensure that the contracts for which he or she is responsible include provisions requiring the contractor to instruct, train, and supervise its personnel on safeguarding PII – or failure to monitor contractor performance to ensure compliance – may result in a negative performance evaluation.

(6) Employees who are responsible for implementing and maintaining security controls for PII and Privacy Act records, and who fail to do so, may receive negative performance evaluations, consistent with Board Order 010, *Performance Appraisal Program*. As indicated by the facts and circumstances, a particular failure may also be considered misconduct. Affected employees may be subject to these consequences regardless of whether the failure results in the loss of control or unauthorized disclosure of PII or Privacy Act records.

b. **Corrective actions.** In individual cases of a breach or other failure to comply with rules/requirements, corrective actions should be commensurate with the level of responsibility of the person(s) involved and the type of PII or Privacy Act records involved. The particular facts and circumstances of each situation, including whether the breach/failure was intentional and the consequences of the breach/failure, will be considered in determining the appropriate corrective action. Any corrective action must be determined and implemented in a manner consistent with applicable statutes, regulations, and CSB policy.

(1) Minimum action. In any case in which an employee or contractor personnel demonstrates egregious disregard or a pattern of error in safeguarding PII or Privacy Act records, or other behavior that indicates he or she presents a continuing security risk, the CSB will promptly remove the individual's authority to access CSB information and information systems.

(2) Poor performance. Corrective actions resulting from negative performance evaluations may include, but are not limited to, informal counseling; denial of a within-grade increase, pursuant to 5 U.S.C. § 5335; placement on a Performance Improvement Plan; and performance-based actions, in accordance with 5 U.S.C. § 4303 and 5 C.F.R. Chapter 432.

(3) Misconduct. Corrective actions for misconduct may include the full range of disciplinary actions, including but not limited to, reprimand; suspension;

removal; other adverse actions, in accordance with 5 U.S.C. Chapter 75; and other actions permitted by applicable statutes, regulations, or CSB policy.

(4) Default. Instances of default by contractors or their personnel will be referred to the responsible Contracting Officer for evaluation of appropriate corrective actions. Such actions may include the full range of measures permitted by the Federal Acquisition Regulation or other applicable authorities, including but not limited to, negative past performance evaluations, termination for default, and debarment. At a minimum, the CSB may require a contractor to immediately reassign any personnel who appear to be involved in a breach or other compliance failure related to CSB PII or Privacy Act records.

(5) Legal violations. The CSB will refer suspected violations of civil or criminal laws to the appropriate investigative or law enforcement authority for further action.

11. **PROTECTION OF PII.**

a. **Protection of non-electronic records on-site.** When maintained in non-electronic (i.e., paper) form on-site at the CSB offices, records containing PII shall be protected with the following minimum safeguards:

(1) Records containing PII may be used only in areas of the CSB offices in which access is limited to CSB employees whose duties require use of such records and controlled to prevent casual observation of the records while they are in use.

(2) When not in use, records containing PII shall be stored in locked file cabinets. Cabinets secured only by a key lock must also be located within a locked room.

(3) Records containing PII must never be left unattended in open or unlocked work spaces or file cabinets.

b. **Protection of electronic records on-site.** When maintained in electronic form on-site at the CSB offices, records containing PII shall be protected in accordance with the provisions of Board Order 034, Information Technology Security Program.

c. **Physical removal.**

(1) Policy. PII may be physically removed from the CSB offices, provided that removal is necessary for a legitimate agency business purpose and the protections described in paragraph c.(2) of this section are applied to the removed PII.

(2) Required protections.

(a) Any PII that is physically removed from the CSB in electronic form must be encrypted. The device or media containing the PII must have an external label that identifies it as U.S. Government Property; lists a name, telephone number, and address for a CSB point-of-contact; and directs anyone who finds the device/media to contact the CSB to arrange for its return at the CSB's expense. CSB employees who carry a device or media containing electronic PII must at all times either keep it in their possession or secure it in a locked area to which only the employee has access. Such devices/media must not be placed in checked baggage or otherwise left unattended in an unsecured area.

(b) The IT Security Officer shall implement NIST SP 800-53 (or any required superseding equivalent) security controls to ensure the encryption of PII, including back-up media, that is physically removed from the CSB in electronic form for transportation to and/or storage at a remote site.

(c) The IT Security Officer shall develop and implement appropriate procedures and accountability measures to ensure that off-site use of physically removed PII in electronic form does not result in bypassing of encryption. Such procedures and accountability measures will be mandatory and must be applied in every instance that PII is physically removed in electronic form.

(d) Any PII that is physically removed from the CSB in paper form must be carried in a locked document security bag. Such bags, which can be placed within a typical briefcase, will be provided by the CSB. The bag must have an external label that identifies it as U.S. Government Property; lists a name, telephone number, and address for a CSB point-of-contact; and directs anyone who finds the bag to contact the CSB to arrange for its return at the CSB's expense. CSB employees who carry such a bag must at all times either keep it in their possession or secure it in a locked area to which only the employee has access. Document security bags must not be checked as baggage or otherwise left unattended in an unsecured area.

(3) Identification of back-up media. For security planning and awareness purposes, the IT Security Officer shall identify in writing all instances of offsite transportation and/or storage of backup media. This list will be reviewed and, if needed, updated annually and after any significant change in back-up practices.

d. **Remote access.**

(1) Policy. PII in electronic form may be accessed remotely, provided that such access is necessary for a legitimate agency business purpose; is in accordance with the requirements of section 19 of Board Order 034, Information

Technology Security Program; and is accomplished with the protections described in paragraph d.(2) of this section.

(2) Required protections.

(a) Remote access to PII must always be accomplished only through a secure connection. For direct access to information resources on the CSB network, the required secure connection is a virtual private network (VPN) connection established using CSB-issued authentication certificate(s) or hardware tokens. For access to information resources through a web interface (e.g., Outlook Web Access), the required secure connection is one protected by 128-bit secure socket layer (SSL) encryption.

(b) The IT Security Officer shall implement NIST SP 800-53 (or any required superseding equivalent) security controls to ensure that an authenticated, VPN connection is required for remote access.

(c) The IT Security Officer shall implement NIST SP 800-53 (or any required superseding equivalent) security controls enforcing allowed downloading of PII.

(d) The IT Security Officer shall implement NIST SP 800-53 (or any required superseding equivalent) security controls enforcing encrypted remote storage of PII.

(3) Download and remote storage. When necessary for a legitimate agency business purpose, PII may be downloaded to and/or remotely stored on an encrypted CSB-issued device or media only. Once PII has been downloaded to/stored on such a device/media, the PII must be treated as having been physically removed and is subject to the requirements of section 11.c. of this Order.

12. **USE OF SOCIAL SECURITY NUMBERS.**

a. **Policy.** The CSB will not directly collect or use social security numbers from employees or members of the public, except in circumstances where there is a legal requirement to do so or where use of an alternative identifier is not possible. As appropriate, the CSB will participate in government-wide efforts to explore alternatives to agency use of social security numbers as a personal identifier for both federal employees and federal programs.

b. **Implementation Plan.** The Senior Agency Official for Privacy shall develop a plan to identify and eliminate instances of the unnecessary collection and use of social security numbers in the systems and programs of the CSB. The actions identified in the plan are to be completed within the timeframe specified in OMB Memorandum M-07-16 (May 22, 2007), Attachment 1, paragraph B.2.a.

13. **REVIEW OF PII HOLDINGS.**

a. **Initial review.** The Senior Agency Official for Privacy shall develop an implementation plan providing for the Responsible Management Official for each CSB information system and system component to conduct a baseline review of current holdings of PII in the systems and system components for which they are responsible to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, complete, and reduced to the minimum necessary for the proper performance of a documented agency function. The scope of this review will include both electronic and non-electronic information systems.

b. **Periodic updated review.** Following the initial review described in paragraph a. of this section, the Responsible Management Official for each CSB information system and system component shall, once each fiscal year, review the holdings of PII in the systems and system components for which they are responsible. The purpose of the review is to ensure, to the maximum extent practicable, that PII holdings continue to be accurate, relevant, timely, complete, and reduced to the minimum necessary for the proper performance of a documented agency function. The scope of this review will include both electronic and non-electronic information systems. The reviews are to be conducted during the second quarter of each fiscal year and the results shall be submitted to the Senior Agency Official for Privacy no later than March 31 of each year. The Senior Agency Official for Privacy shall ensure that this review schedule is made known to the public.

14. **PRIVACY ACT REVIEWS.** In accordance with the Privacy Act and OMB Circular A-130 (Appendix I, Section 3), the Senior Agency Official for Privacy shall ensure that the reviews listed in this section are conducted and shall be prepared to report to the Director of OMB on the results of such reviews and the corrective actions taken to resolve any issues identified in the reviews. Each of the reviews listed in this section shall be conducted during Fiscal Year 2009, and then repeated thereafter according to the review cycles specified below.

a. **Section (m) contracts.** Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Privacy Act binding on the contractor and its employees.

b. **Recordkeeping practices.** Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Privacy Act, paying particular attention to the maintenance of automated records.

c. **Routine use disclosures.** Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.

d. **Exemption of systems of records.** Review every four years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Privacy Act in order to determine whether such exemption is still needed.

e. **Matching programs.** Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Privacy Act; the OMB guidance; and any agency regulations, operating instructions, or guidelines have been met.

f. **Privacy Act training.** Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Privacy Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.

g. **Violations.** Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Privacy Act, or an employee being found criminally liable under the provisions of Section (i) of the Privacy Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.

h. **Systems of records notices.** Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register.

15. **TRAINING.** The Senior Agency Official for Privacy and the IT Security Officer shall jointly develop and deliver comprehensive training on the handling and protection of PII. In addition to other topics they deem appropriate, such training must include instruction on the rules of conduct established by this Order, and on ensuring that off-site use of physically removed PII in electronic form does not result in bypassing of encryption. This training must be completed annually by every CSB employee and by any contractor personnel whose work requires them to handle PII. The Senior Agency Official for Privacy shall maintain records documenting the completion of this training.

16. **REVIEW AND UPDATE.** The Senior Agency Official for Privacy, in consultation with the IT Security Officer, shall review this Order annually. As necessary based upon the results of such review, the Senior Agency Official for Privacy shall submit proposed amendments to this Order to the Board by March 31 of each year.

CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

May 5, 2008.