its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards—Access to the CDC Clifton Road facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. The hard copy records are kept in locked cabinets in locked rooms. The local fire department is located directly next door to the Clifton Road facility. The computer room is protected by an automatic sprinkler system, numerous automatic sensors (e.g., water, heat, smoke, etc.) are installed, and a proper mix of portable fire extinguishers is located throughout the computer room. The system is backed up on a nightly basis with copies of the files stored off site in a secure fireproof safe. Security guard service in buildings provides personnel screening of visitors. Computer work stations and automated records are located in secured areas.

Procedural Safeguards—Protection for computerized records both on the mainframe and the National Center Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, encryption, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures and secure off-site storage for backup tapes. When Privacy Act tapes are scratched, a special process is performed in which tapes are completely written over to avoid inadvertent data disclosure. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data.

CDC and contractor employees who maintain records are instructed to check with the system manager prior to making disclosures of data. When individually identified data are being used in a room, admittance at either CDC or contractor sites is restricted to specifically authorized personnel. Privacy Act provisions are included in contracts, and the CDC Project Director, contract officers and project officers oversee compliance with these requirements. Upon completion of the contract, all data will be either returned to CDC or destroyed, as specified by the contract.

Implementation Guidelines: The safeguards outlined above are in accordance with the HHS Information Security Program Policy and FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems." Data maintained on CDC's Mainframe and the National Center LAN are in compliance with OMB Circular A–130, Appendix III. Security is provided for information collection, processing, transmission, storage, and dissemination in general support systems and major applications.

The records in this System are retained and disposed of in the following way: Records are retained and disposed of in accordance with the CDC Records Control Schedule. Records are maintained in agency for two years. Source documents for computer disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records destroyed by paper recycling process when 20 years old, unless needed for further study.

VI. OMB Control Numbers, Expiration Dates, and Titles of Information Collection

A. *Full Title:* "Records of Subjects in Health Promotion and Education Studies, HHS/CDC/NCCDPHP."

OMB Control Number: 09–20–0160.

Expiration Date: TBD.

VII. Supporting Documentation

A. Preamble and Proposed Notice of System for publication in the **Federal Register**.

B. *Agency Rules:* None.

C. *Exemption Requested:* None.

D. *Computer Matching Report:* The new system does not require a matching report in accordance with the computer matching provisions of the Privacy Act.

[FR Doc. 2010–33025 Filed 1–24–11; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Privacy Act of 1974; Report of Modified or Altered System of Records

AGENCY: National Center for HIV, STD and TB Prevention (NCHSTP), Department of Health and Human Services (DHHS).

ACTION: Notification of proposed altered System of Records.

SUMMARY: The Department of Health and Human Services proposes to alter System of Records, 09–20–0161, "Records of Health Professionals in Disease Prevention and Control Training Programs, HHS/CDC/NCHSTP." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and responding to the Breach of Personally Identifiable Information:

To appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

These records will be maintained by the National Center for HIV, STD and TB Prevention (NCHSTP).

DATES: Comments must be received on or before February 24, 2011. The proposed altered System of Records will be effective 40 days from the date submitted to the OMB, unless NCHSTP receives comments that would result in a contrary determination.

ADDRESSES: You may submit comments, identified by the Privacy Act System of Record Number 09–20–0161:

- *Federal eRulemaking Portal: http://regulations.gov*. Follow the instructions for submitting comments.
- *E-mail:* Include PA SOR number 09–20–0161 in the subject line of the message.
- *Phone:* 770/488–8660 (not a toll-free number).
- *Fax:* 770/488–8659.
- *Mail:* HHS/CDC Senior Official for Privacy (SOP), Office of the Chief Information Security Officer (OCISO), 4770 Buford Highway—M/S: F–35, Chamblee, GA 30341.
- *Hand Delivery/Courier:* HHS/CDC Senior Official for Privacy (SOP), Office of the Chief Information Security Officer (OCISO), 4770 Buford Highway—M/S: F–35, Chamblee, GA 30341.

• Comments received will be available for inspection and copying at this same address from 9 a.m. to 3 p.m., Monday through Friday, Federal holidays excepted.

SUPPLEMENTARY INFORMATION: NCHSTP proposes to alter System of Records, No. 09–20–0161, "Records of Health Professionals in Disease Prevention and Control Training Programs, HHS/CDC/NCHSTP." This record system enables the CDC officials to maintain training records and access the impact of the agency's training programs on the knowledge, attitudes and practices of clinicians and other health care personnel, in order to develop improved training curricula and programs for disease prevention and control for such health care personnel.

This System of Record Notice is being altered to add the Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) memorandum dated May 22, 2007.

The following notice is written in the present tense, rather than the future tense, in order to avoid the unnecessary expenditure of public funds to republish the notice after the System has become effective.

Dated: December 11, 2009.

James D. Seligman,

Chief Information Officer, Centers for Disease Control and Prevention.

Editorial Note: This document was received at the Office of the Federal Register on December 27, 2010.

Department of Health and Human Services (HHS)

Centers for Disease Control and Prevention (CDC)

National Center for HIV, STD and TB Prevention (NCHSTP)

Records of Health Professionals in Disease Prevention and Control Training Programs

Report of Modified or Altered System of Records

Narrative Statement

I. Background and Purpose of the System

A. Background

The Department of Health and Human Services proposes to alter System of Records, No. 09–20–0161, "Records of Health Professionals in Disease Prevention and Control Training Programs, HHS/CDC/NCHSTP." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and responding to the Breach of Personally Identifiable Information:

To appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

B. Purpose

This record system enables the CDC officials to maintain training records and access the impact of the agency's training programs on the knowledge, attitudes and practices of clinicians and other health care personnel, in order to develop improved training curricula and programs for disease prevention and control for such health care personnel.

II. Authority for Maintenance of the System

Public Health Service Act, Section 301, "Research and Investigation" (42 U.S.C. 241).

III. Proposed Routine Use Disclosures of Data in the System

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a "routine use." The routine uses proposed for this System are compatible with the stated purpose of the System:

Disclosure may be made to CDC contractors in the conduct of training surveys and studies covered by this system notice and in the preparation of scientific reports, in order to accomplish the stated purposes of the system. The recipients will be required to maintain Privacy Act safeguards with respect to such records.

CDC is under contract with private firms for the purpose of collating, analyzing, aggregating or otherwise refining records in this system. Relevant records are disclosed to such contractors. The contractors are required to maintain Privacy Act safeguards with respect to such records.

Disclosure may be made to a congressional office from the record of an individual in response to a verified inquiry from the congressional office made at the written request of that individual.

The Department of Health and Human Services (HHS) may disclose information from this system of records to the Department of Justice, or to a court or other tribunal, when: (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

Records may be disclosed to appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

IV. Effects of the Proposed System of Records on Individual Rights

An individual may learn if a record exists about himself or herself by contacting the system manager at the address above. Requesters in person must provide driver's license or other positive identification. Individuals who do not appear in person must either: (1) Submit a notarized request to verify their identity; or (2) certify that they are the individuals they claim to be and that they understand that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act subject to a $5,000 fine.

The following information must be provided when requesting notification: (1) Full name; (2) name of the clinic organization in which requester was employed at time of training or survey participation; and (3) nature of the training or survey questionnaire in which the requester participated.

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. An accounting of disclosures that have been made of the record, if any, may be requested.

V. Safeguards

The records in this System are stored in computer/disks, printouts and file folders. The records are retrieved by the name of individual respondent, identification number, and type of training received are some of the indices used to retrieve records from this system.

The records in this System have the following safeguards in place to maintain and protect the information as it relates to Authorized users, physical and procedural safeguards:

Authorized Users—Access is granted to only a limited number of personnel, i.e., CDC Project Officer, interviewers and designated support staff of CDC or its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards—Locked cabinets in locked rooms, 24-hour guard service in buildings, personnel screening of visitors, electronic anti-intrusion devices in operation at the Federal Records Center, fire extinguishers, overhead sprinkler system and card-access control equipment in the computer room, computer terminals and automated records located in secured areas.

Procedural Safeguards—Protection for computerized records both on the mainframe and the CIO Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures and Vault Management System for secure off-site storage is available for backup tapes. To avoid inadvertent data disclosure, "degaussing" is performed to ensure that all data are removed from Privacy Act computer tapes and/or other magnetic media. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data.

CDC and contractor employee who maintain records are instructed to check with the system manager prior to making disclosures of data. When individually identified data are being used in a room, admittance at either CDC or contractor sites is restricted to specifically authorized personnel. Privacy Act provisions are included in contracts, and the CDC Project Director, contract officers and project officers oversee compliance with these requirements. Upon completion of the contract, all data will be either returned to CDC or destroyed, as specified by the contract.

The safeguards outlined above are developed in accordance with Chapter 45–13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual; and Part 6, "Automated Information System Security," of the HHS Information Resources Management Manual. FRC safeguards are in compliance with GSA Federal Property Management Regulations, Subchapter B—Archives and Records. Data maintained in CDC's Processing Center are in compliance with OMB Circular A–130, Appendix III. Security is provided for information collection, processing, transmission, storage, and dissemination in general support systems and major applications. CIO LANs currently operate under Novell Netware v. 4.11 and are in compliance with "CDC & ATSDR Security Standards for Novell File Servers."

The records in this System are retained and disposed of in the following way: Records are maintained in agency for two years. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records destroyed by paper recycling process after 12 years, unless needed for further study.

VI. OMB Control Numbers, Expiration Dates, and Titles of Information Collection

A. *Full Title:* "Records of Health Professionals in Disease Prevention and Control Training Programs, HHS/CDC/NCHSTP."

B. *OMB Control Number:* 09–20–0161.

C. *Expiration Date:* TBD.

VII. Supporting Documentation

A. Preamble and Proposed Notice of System for publication in the **Federal Register**.

B. *Agency Rules:* None.

C. *Exemption Requested:* None.

D. *Computer Matching Report:* The new system does not require a matching report in accordance with the computer matching provisions of the Privacy Act.

[FR Doc. 2010–33026 Filed 1–24–11; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Privacy Act of 1974; Report of Modified or Altered System of Records

AGENCY: National Center for Environmental Health (NCEH), Coordinating Center for Environmental Health and Injury Prevention (CCEHIP), Department of Health and Human Services (DHHS).

ACTION: Notification of proposed altered System of Records.

SUMMARY: The Department of Health and Human Services proposes to alter System of Records, 09–20–0162, "Records of Subjects in Agent Orange, Vietnam Experience, and Selected Cancers Studies, HHS/CDC/CCEHIP/NCEH." HHS is proposing to add the following Breach Response Routine Use Language to comply with the Office of Management and Budget (OMB) Memoranda (M) 07–16, Safeguarding Against and responding to the Breach of Personally Identifiable Information:

To appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

These records will be maintained by the Coordinating Center for Environmental Health and Injury Prevention (CCEHIP), National Center for Environmental Health (NCEH).

DATES: Comments must be received on or before February 24, 2011. The proposed altered System of Records will be effective 40 days from the date submitted to the OMB, unless CCEHIP/NCEH receives comments that would result in a contrary determination.

ADDRESSES: You may submit comments, identified by the Privacy Act System of Record Number 09–20–0162:

- *Federal eRulemaking Portal: http://regulations.gov.* Follow the instructions for submitting comments.
- *E-mail:* Include PA SOR number 09–20–0162 in the subject line of the message.
- *Phone:* 770/488–8660 (not a toll-free number).
- *Fax:* 770/488–8659.
- *Mail:* HHS/CDC Senior Official for Privacy (SOP), Office of the Chief Information Security Officer (OCISO), 4770 Buford Highway—M/S: F–35, Chamblee, GA 30341.
- *Hand Delivery/Courier:* HHS/CDC Senior Official for Privacy (SOP), Office