1**Centers for Disease Control and Prevention**

Report of a New Privacy Act System of Records

System name: Etiological Agent Import Permit Program (EAIPP) 2.0, HHS/CDC/OPHPR

Security classification: None

System location: Division of Select Agents and Toxins (DSAT), Office of Public Health Preparedness and Emergency Response (OPHPR), Bldg. 20, Centers for Disease Control and Prevention (CDC), 1600 Clifton Road, NE, Atlanta, GA 30333

and

Federal Records Center, 4712 Southpark Blvd., Ellenwood, GA 30294.

Categories of individuals covered by the system: Any individual who submits an application to receive a permit to import infectious biological agents, infectious substances, and vectors of human disease under 42 CFR 71.54 this would include individuals from academic institutions and biomedical centers, commercial manufacturing facilities, federal, state, and local laboratories, including clinical and diagnostic laboratories, research facilities, exhibition facilities, and educational facilities.

Categories of records in the system: The information being collected to receive a permit as required under 42 CFR 71.54 includes the applicant's name, mailing address, phone numbers, and email address. The information available on the permit includes the applicant's name, mailing address, phone numbers, and email address.

Authority for maintenance of the system: Public Health Service Act, Section 361, "Regulations to control communicable diseases"(42 U.S.C. 264).

Purpose(s): Records maintained in EAIPP 2.0 which is used for data entry, data query, and routine reporting activities. The purpose of this system of records is to protect the public's health by regulating the importation of infectious biological agents, infectious substances, and vectors of human disease.

DSAT regulates the importation of infectious biological agents, infectious substances, and vectors of human disease into the United States. Prior to issuing an import permit, EAIPP reviews all applications to ensure that entities have appropriate safety measures in place for working safely with imported infectious agents. DSAT may inspect applicants to ensure that the facilities have implemented the appropriate biosafety measures for the infectious agent or vector to be imported.

Routine Uses of Records Maintained In the System, Including Categories of Users and the Purposes of Such Uses:

1. Records may be disclosed to State and/or local health departments and other public health or cooperating medical authorities to deal more effectively with outbreaks and conditions of public health significance.

2. Disclosure of records or portions of records may be made to a Member of Congress or a Congressional staff member submitting a verified request involving an individual who is entitled to the information and has requested assistance from the Member or staff member. The Member of Congress or Congressional staff member must provide a copy of the individual's written request for assistance.

3. In the event of litigation where the defendant is: (a) The Department, any component of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the Department or any of its components; or (c) any Department employee in his or her individual capacity where the Justice Department has agreed to represent such employee, disclosure may be made to the Department of Justice to enable that Department to present an effective defense, provided that such disclosure is compatible with the purpose for which the records were collected.

4. Records may be disclosed to the Department of Justice when (1) HHS, or any component thereof; or (2) any employee of HHS in his or her official capacity; or (3) any employee of HHS in his or her individual capacity where the Department of Justice or HHS has agreed to represent the employee; or (4) the United States, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by HHS to be relevant and necessary to the litigation; provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected

5. Records may be disclosed to the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto.

6. Records may be disclosed to a contractor performing or working on a contract for HHS and/or CDC and who has a need to have access to the information in the performance of its duties or activities for HHS and/or CDC in accordance with law and with the contract. The contractor is required to comply with the applicable provisions of the Privacy Act.

7. Records subject to the Privacy Act may be disclosed to private firms for data entry, computer systems analysis and computer programming services. The contractors promptly return data entry records after the contracted work is completed. The contractors are required to maintain Privacy Act safeguards.

8. Disclosure to the Office of Inspector General, Department of Health and Human Services, any other Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States that administers, or that has the authority to investigate potential fraud, waste, or abuse.

9. Disclosure 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 as it is relevant and necessary for that assistance.

Policies and Practices For Storing, Retrieving, Accessing, Retaining, and Disposing of Records In the System

Storage: Records are stored in file folders, as well as on computer tapes and disks, and CD-ROMs. The system is backed up on a nightly basis with copies of the files stored off site in a secure location.

Retrievability: Records are retrieved by the applicant's name or assigned permit number.

Safeguards: 1. **Authorized Users:** Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Individuals who have daily access to these records are limited to DSAT staff (FTEs and contractors) who have responsibility for conducting regulatory oversight of the importation of infectious biological agents, infectious substances, and vectors of human disease into the United States.

2. **Physical Safeguards:** Paper records are maintained in locked cabinets in locked rooms in a restricted access location that is controlled by a cardkey system, and security guard service provides personnel screening of visitors. Electronic data files are password protected and stored in a restricted access location. The computer room is protected by an automatic sprinkler system, numerous automatic sensors (e.g., water, heat, smoke, etc.) are installed, and the appropriate portable fire extinguishers are located throughout the computer room. Computer workstations, lockable personal computers, and automated records are located in secured areas.

3. **Procedural Safeguards:** Protection for computerized records 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 secure off-site storage is available for backup files.

Knowledge of individual tape passwords is required to access tapes, and access to the system is limited to users obtaining prior supervisory approval. To avoid inadvertent data disclosure, a special additional procedure is performed to ensure that all Privacy Act data are removed from computer tapes and/or other magnetic media. A backup copy of data is stored at an offsite location and a log kept of all changes to each file and all persons reviewing the file. Additional safeguards may also be built into the program by the system analyst as warranted by the sensitivity of the data set.

The DSAT and contractor employees who maintain records are instructed in specific procedures to protect the security of records, and are to check with the system manager prior to making disclosure 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.

Appropriate 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.

4. **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 COTPER 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.

Retention and Disposal: The DSAT records and associated information are retained and dispositioned in accordance with DSAT records retention schedule, N1-442-06-1, pending approval by the National Archives and Records Administration. The DSAT records will be retained for 10 years in compliance with the records retention schedule requirements or until such time as no longer needed for litigation or other records purposes. Records will be transferred to a Federal Records Center for storage when no longer in active use. Final disposition of records stored offsite at the Federal Records Center will be accomplished by a controlled process requesting final disposition approval from the record owner prior to any destruction to ensure records are not needed for litigation or other records purposes. Hard copy records will be placed in a locked container or designated secure storage area while awaiting destruction. Dara will be destroyed in a manner that precludes its reconstruction, such as shredding.

Electronic information will be deleted or overwritten using overwriting software that wipes the entire physical disk and not just the virtual disk. Overwriting is required for the destruction of all electronic SBU information.

System Manager(s) and contact information: Director, Division of Select Agents and Toxins, Office of Public Health Preparedness and Emergency Response, Bldg. 20, MS A46, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Notification Procedure: An individual may learn if a record exists about himself or herself by contacting the system manager at the above address. Requesters in person must provide driver's license or other positive identification. Individuals who do not appear in person must submit a notarized request on institutional letterhead to verify their identity. 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 and/or imprisonment.

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

Contesting Record Procedures: Contact the system manager at the address specified above, reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Record Source Categories: Any applicant seeking to import infectious biological agents, infectious substances, and vectors of human disease into the United States.

Systems exempted from certain provisions of the act: None.