Billing Code: 4163-18-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[Docket No. CDC-2020-0088]

Privacy Act of 1974; System of Records

AGENCY: Centers for Disease Control and Prevention (CDC), Department of Health and Human Services (HHS).

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS) is establishing a new system of records to be maintained by the Centers for Disease Control and Prevention, 09-20-0180, "Electronic Import Permit Program Portal (eIPP Portal)." The system of records will be used by CDC to monitor the importation of infectious biological agents, infectious substances, and vectors of human disease.

DATES: The modified system of records is applicable [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], subject to a 30-day period in which to comment on the routine uses.

Written comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION DATE IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by Docket No. CDC-2020-0088 by any of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Beverly Walker, Chief Privacy Officer, CDC Privacy Unit, CyberSecurity Program Office (CSPO), Centers for Disease Control and Prevention, 4770 Buford Hwy, Mailstop S101, Atlanta, GA 30341.

Instructions: All submissions received must include the agency name and Docket Number. All relevant comments received will be posted without change to https://regulations.gov, including any personal information provided. Therefore, do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure. For access to the docket to read background documents or comments received, go to https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Beverly Walker, Chief Privacy Officer, CDC Privacy Unit, CyberSecurity Program

Office (CSPO), Centers for Disease Control and Prevention, 4770 Buford Hwy, Mailstop S101, Atlanta, GA 30341. Telephone: 770-488-8524.

SUPPLEMENTARY INFORMATION:

I. Background on the CDC Import Permit Program

Under the authority of Section 361 of the Public Health Service Act (PHS Act) (42 U.S.C. 264), the HHS Secretary makes and enforces such regulations as in his/her judgment are necessary to prevent the introduction, transmission, or spread of communicable diseases from foreign countries into the U.S. states or territories. For purposes of carrying out and enforcing such regulations, the HHS Secretary may authorize a variety of public health measures, including inspection, fumigation, disinfection, sanitation, pest extermination, destruction of animals or articles found to be sources of dangerous infection to human beings, and other measures. The Foreign Quarantine regulations (42 CFR Part 71) set forth provisions to prevent the introduction, transmission, and spread of communicable disease from foreign countries into the United States. Part 71, Subpart F (Importations) contains provisions governing the importation of infectious biological agents, infectious substances, and vectors (42

CFR 71.54), including requiring persons to obtain a permit issued by the CDC before importing, or distributing after import, any of these materials. The purpose of the import permit requirement and permitting process is to prevent the introduction, transmission, or spread of communicable diseases from foreign countries into the U.S. states or territories. Before issuing an import permit, the CDC Division of Select Agents and Toxins, Import Permit Program (CDC/IPP) reviews the application to ensure the applicant has appropriate safety measures in place for importing and working safely with the applicable infectious biological agent(s), substance(s), and/or vector(s). Regulations of the U.S. Department of Transportation apply to such materials while in transit in the U.S. states and territories.

II. New System of Records 09-20-0180

The proposed new system of records, "Electronic Import Permit Program Portal (eIPP Portal)," will cover records about individual applicants, which the CDC/IPP maintains in the new eIPP Portal information technology (IT) system for the purpose of overseeing—and issuing permits allowing—the importation of infectious biological agents, infectious substances, and vectors of human disease

as outlined in the import permit regulations at 42 CFR 71.54. The eIPP Portal IT system is a single web-based information management system that will track permit applications submitted to and permits issued by CDC/IPP. It will allow the regulated community to submit the applications and engage in related information exchanges with CDC/IPP electronically via a single web portal. This will enable the regulated community to interact with CDC/IPP more efficiently, allow for faster processing of permit applications, and reduce program burdens and reliance on labor-intensive and paper-based processes.

A report on the new system of records was sent to Congress and OMB in accordance with 5 U.S.C. 552a(r).

Dated: August 21, 2020.

Suzi Connor,

Chief Information Officer,

Centers for Disease Control and Prevention.

SYSTEM NAME AND NUMBER:

Electronic Import Permit Program Portal (eIPP Portal), 09-20-0180.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the HHS component responsible for this system of records is: Division of Select Agents and Toxins (DSAT), Center for Preparedness and Response, Centers for Disease Control and Prevention (CDC), 1600 Clifton Rd. NE, Atlanta, GA 30329.

SYSTEM MANAGER(S):

The System Manager is: Director, Division of Select Agents and Toxins (DSAT), Center for Preparedness and Response, MS A-46, CDC, 1600 Clifton Rd. NE, Atlanta, GA 30329, (404) 718-2000, lrsat@cdc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Public Health Service Act, Section 361, "Regulations to Control Communicable Diseases" (42 U.S.C. 264).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to support CDC/IPP's oversight of, and permitting process for, the importation and any subsequent distribution of infectious biological agents, infectious substances, and vectors of human disease into the United States, the purpose of which is to prevent the introduction, transmission, or spread of communicable diseases from foreign countries into the states or possessions.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records in the system will cover those individuals who apply for an import permit from CDC/IPP under 42 CFR 71.54.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system of records will include the following categories of records. The three applications are forms approved by the Office of Management and Budget (OMB).

- Application for Permit to Import Biological Agents and Vectors of Human Disease into the United States. An applicant submits this application to CDC/IPP to request a permit for the importation, and any subsequent distribution after importation, of infectious biological agents, infectious substances, or vectors of human disease.
- Application for Permit to Import or Transfer Live Bats. An applicant submits this application to CDC/IPP to request a permit for the importation, and any subsequent distribution after importation, of live bats.
- Application for Permit to Import Infectious Human Remains into the United States. An applicant submits this application to CDC/IPP to request a permit for the importation of human remains or body parts that

contain biological agents, infectious substances, or vectors of human disease.

- Import Permit. CDC/IPP issues a permit on an approved application, allowing the applicant to import biological agents and vectors of human disease human remains or body parts that contain biological agents, infectious substances, or vectors of human disease or live bats.
- Documentation of Inspection. CDC/IPP may inspect an applicant's or importer's premises to ensure compliance with the import permit regulations. As part of the inspection process, the applicant may need to respond to written requests from DSAT. DSAT has not developed standardized forms for this documentation.

RECORD SOURCE CATEGORIES:

The applicant will be the source of most information in the records. CDC/IPP will be the source of certain information in the permits, tracking records, and inspection records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to other disclosures authorized directly in the Privacy Act at 5 U.S.C. 552a(b)(1) and (2) and (4) through (11), HHS may disclose records about a subject individual

from this system of records to parties outside HHS as described in these routine uses, without the individual's prior written consent.

1. Records may be disclosed to contractors engaged to assist CDC/IPP with performing the functions listed in the Purpose section above. Contractors are required to maintain Privacy Act safeguards with respect to such records.
2. Records may be disclosed to state health departments, other public health agencies, cooperating medical authorities, or federal law enforcement agencies to effectively manage outbreaks and conditions of public health significance.
3. Information may be disclosed to the Department of Justice (DOJ) or to a court or other adjudicative body in litigation or other proceedings when:
    a. HHS or any of its component thereof, or
    b. any employee of HHS acting in the employee's official capacity, or
    c. any employee of HHS acting in the employee's individual capacity where the DOJ or HHS has agreed to represent the employee, or
    d. the United States Government,

is a party to the proceeding or has an interest in such proceeding and, by careful review, HHS determines that the records are both relevant and necessary to the proceeding.

4. 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.
5. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to agency concerned, whether federal, state, Tribal, local, territorial, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.
6. For the purpose of combatting fraud, waste, and abuse, records may be disclosed to a relevant federal agency or instrumentality of any governmental jurisdiction

within or under the control of the United States for the purpose of investigating potential fraud, waste, or abuse.

7. Records may be disclosed to representatives of the National Archives and Records Administration (NARA) in records management inspections conducted pursuant to 44 U.S.C. 2904 and 2906.
8. Records may be disclosed to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records, (2) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the federal government, or national security, and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
9. Records may be disclosed to another federal agency or federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1)

responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The records will be maintained electronically, but paper printouts may be generated.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records will be retrieved by the applicant's name or assigned permit number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records will be retained for 10 years in compliance with the records retention schedule requirements, or until such time as the records are no longer needed for litigation or other records purposes, in accordance with CDC/IPP disposition schedule DAA-0441-2019-0001. 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 HHS record owner prior to any destruction to ensure the records are not needed for litigation or other records purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Safeguards will conform to the HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html, the HHS Information Security and Privacy Policy (IS2P), and applicable federal laws, rules and policies, including: the E-Government Act of 2002, which includes the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3541-3549, as amended by the Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551-3558; all pertinent National Institutes of Standards and Technology (NIST) publications; and OMB Circular A-130, Managing Information as a Strategic Resource.

Administrative and Technical Safeguards:

- Security measures will be implemented on government computers to control unauthorized access to the system. Attempts to gain access by unauthorized individuals will be automatically recorded and reviewed by IPP on a regular basis. The individuals permitted to access these

records will be limited to staff (FTEs and contractors having security clearances at T3 (Non-Critical Sensitive positions requiring Secret clearance) or T4 (Non-Sensitive High Risk (Public Trust)) levels) who have responsibility for conducting regulatory oversight.

- Protection for computerized records will include programmed verification of valid user identification code and password prior to logging on to the system; mandatory password changes, limited log-ins, virus protection, encryption, firewalls, and intrusion detection systems, and user rights/file attribute restrictions. The password protection will impose username and password log-in requirements to prevent unauthorized access. Each user name will be assigned limited access rights to files and directories at varying levels to control file sharing. There will be routine daily backup procedures, and backup files will be securely stored off-site. Security controls will be reviewed on an ongoing basis.
- Knowledge of individual tape passwords will be required to access backups, and access to the system will be limited to users obtaining prior supervisory approval. To avoid inadvertent data disclosure, a special additional procedure will be performed to ensure that

all Privacy Act data are removed from computer hard drives. Additional safeguards may also be built into the program by the system analyst as warranted by the sensitivity of the data set.

- FTEs and contractor employees who maintain records will be instructed in specific procedures to protect the security of records, and will be required to check with the system manager prior to making disclosure of data. When individually identifiable data are being used in a room, admittance at either federal or contractor sites will be restricted to specifically authorized personnel.
- Appropriate Privacy Act provisions and breach notification provisions will be included in applicable contracts, and the CDC Project Director, contract officers, and project officers will oversee compliance with these requirements. Upon completion of a contract, all data will be either returned to federal government or destroyed, as specified by the contract.
- Records that are eligible for destruction will be disposed of using destruction methods prescribed by NIST SP 800-88. Hard copy records will be placed in a locked container or designated secure storage area while awaiting destruction. Records will be destroyed in a manner that precludes its reconstruction, such as

secured cross shredding. Utilizing the HHS Security Rule Guidance Material found at https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html, electronic information will be deleted or overwritten using Department of Defense National Institute of Standards and Technology/ General Services Administration (NIST/GSA) approved overwriting software that wipes the entire physical disk and not just the virtual disk. In addition, the physical destruction will be obtained by using a National Security Agency/Central Security Service (NSA/CSS) approved degaussing device.

Physical Safeguards:

- Paper records (i.e., hard copy printouts) will be maintained in locked cabinets in secured rooms through electronic access in a restricted access location that is controlled by an electronic cardkey system that is limited to staff who have responsibility for conducting regulatory oversight. Electronic data files will be encrypted using Federal Information Processing Standards Publication (FIPS) 140-2, and will be stored in a restricted access location. The computer room will be protected by an automatic sprinkler system and numerous

automatic sensors (e.g., water, heat, smoke, etc.) which will be monitored, and a proper mix of portable fire extinguishers will be located throughout the computer room. Computer workstations, lockable personal computers, and automated records will be located in secured areas.

RECORD ACCESS PROCEDURES:

An individual seeking access to records about that individual in this system of records must submit a written access request to the System Manager, identified in the "System Manager" section of this SORN. The request must contain the requester's full name, address, and signature, and permit number if known. To verify the requester's identity, the signature must be notarized or the request must include the requester's written certification that the requester is the individual who the requester claims to be and that the requester understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000. An accounting of disclosures that have been made of the record, if any, may also be requested.

CONTESTING RECORD PROCEDURES:

An individual seeking to amend a record about that individual in this system of records must submit an amendment request to the System Manager identified in the "System Manager" section of this SORN, containing the same information required for an access request. The request must include verification of the requester's identity in the same manner required for an access request; must reasonably identify the record and specify the information contested, the corrective action sought, and the reasons for requesting the correction; and should include supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

NOTIFICATION PROCEDURES:

An individual who wishes to know if this system of records contains records about that individual should submit a notification request to the System Manager identified in the "System Manager" section of this SORN. The request must contain the same information required for an access request, and must include verification of the requester's identity in the same manner required for an access request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2020-18805 Filed: 8/26/2020 8:45 am; Publication Date: 8/27/2020]