Billing Code: 4163-18-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

CENTERS FOR DISEASE CONTROL AND PREVENTION

Privacy Act of 1974; New System of Records

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

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the requirements of the Privacy Act, the Centers for Disease Control and Prevention (CDC) is modifying the name of the system of records (SOR), 09-20-0170 for the "National Select Agent Registry (NSAR)/ Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER." The information system is being modified from "NSAR" to "Electronic Federal Select Agent Program portal (eFSAP)/Electronic Import Permit Program portal (eIPP)." The purpose of the system is to limit access to those biological select agents and toxins (BSAT) listed in provisions of Part 73, of Title 42 of the Code of Federal Regulations (42 C.F.R. Part 73), Part 121 of Title 9 of the Code of Federal Regulations (9 C.F.R. Part 121), and Part 331 of Title 7 of the Code of Federal Regulations (7 C.F.R. Part 331), to those individuals who have a legitimate need to handle or use such BSAT, and who are not identified as restricted persons by the U.S. Attorney General and to protect the public's health by regulating the importation of infectious biological agents, infectious substances, and vectors of human disease as listed in provision 42 CFR §71.54. The eFSAP/eIPP system is a single web-based information management system shared by CDC and the U.S. Department of Agriculture (USDA)/Animal and Plant Health Inspection Service (APHIS) that tracks the possession, use and transfer of BSAT. In addition, eFSAP/eIPP system is a single web-based information management system that tracks CDC permits issued for the importation of infectious biological agents, infectious substances, and vectors of human disease into the United States under the provisions of 42 CFR §71.54.

DATES: Comments will be accepted until [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. This modified system will be effective in September 2017.

ADDRESS: You may submit comments, identified by the Privacy Act System of Record Notice (SORN) Number 09–20–0170:

- Federal eRulemaking Portal: http://regulations.gov. Follow the instructions for submitting comments.

- E-mail: Include PA SORN number 09–20–0170 in the subject line of the message.
- Phone: 770/488–8660 (not a tollfree 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.

FOR FURTHER INFORMATION CONTACT: Beverly Walker, Chief Privacy Officer, Office of the Chief Information, Centers for Disease Control and Prevention, 4770 Buford Highway, Building 101, Room 1112, Mailstop F-35, Chamblee, GA 30341, (770) 488-8524.

SUPPLEMENTARY INFORMATION: This notice serves to modify the name of the SOR from "NSAR" to "Electronic Federal Select Agent Program portal (eFSAP)/Electronic Import Permit Program portal (eIPP)." There is no changes in the data that will be maintained in eFSAP/eIPP system. The system will still contain records about the select agents or toxins at each facility, the individuals approved for access to these agents and toxins, laboratory biosafety and security information for these agents and toxins, observations from the inspections of each registered entity, and permit information issued for the importation infectious biological agents, infectious substances, and vectors of human disease into the United States. The eFSAP/eIPP system allows the regulated community to report information or make requests electronically via a single web portal. This process allows the regulated community to interact with the Program more efficiently, allow for better and faster reporting of potential losses, and reduce the program burden and reliance on labor-intensive and paper-based processes. The new system utilizes a secured database environment to provide regulatory responses faster, provide guidance more quickly, and respond rapidly to public health emergencies.

SYSTEM NAME AND NUMBER: Electronic Federal Select Agent Program portal (eFSAP)/Electronic Import Permit Program portal (eIPP), 09-20-0170.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Division of Select Agents and Toxins (DSAT), Office of Public Health Preparedness and Response (OPHPR), Bldg. 20, Centers for Disease Control and Prevention (CDC), 1600 Clifton Road, NE, Atlanta, GA 30329.

SYSTEM MANAGERS: Director, DSAT, OPHPR, Bldg. 20, Rm. 4100, MS A46, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30329 and Director, AgSAS,

Animal and Plant Health Inspection Service, 4700 River Road, Unit 2, Mailstop 22, Riverdale, MD 20737.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Public Health Security and Bioterrorism Preparedness and Response Act of 2002, the Agricultural Bioterrorism Protection Act of 2002, and Public Health Service Act, Section 361, "Regulations to Control Communicable Diseases" (42 U.S.C. 264).

PURPOSE(S) OF THE SYSTEM: The eFSAP/eIPP system allows the regulated community to report information or make requests electronically via a single web portal and is made up of two separate databases, eFSAP and eIPP. eFSAP portal is a joint information management system that is used by the Federal Select Agent Program. The Federal Select Agent Program is jointly comprised of DSAT and the Animal and Plant Health Inspection Service/Agriculture Select Agent Services. The Federal Select Agent Program oversees the possession, use and transfer of biological select agents and toxins, which have the potential to pose a severe threat to public, animal or plant health or to animal or plant products as outlined in the select agent regulations (42 C.F.R. Part 73, 9 C.F.R. Part 121, and 7 C.F.R. Part 331). eFSAP maintains records associated with information regarding an entity's registration which includes the list of select agents or toxins, list of individuals who will have access to select agents and toxins, laboratory information, the transfers of select agents and toxins, and the identification and final disposition of any select agent or toxin contained in a specimen presented for diagnosis, verification, and proficiency testing, inspections of registered entities and reports of any theft, loss or release of select agent or toxin. This system is a single shared web-based system developed by the Federal Select Agent Program, which allows the regulated community to submit information electronically using the select agent forms approved by the Official of Management and Budget via a single web portal. eIPP is an information management system that is used by the CDC Import Permit Program. The CDC Import Permit Program oversees the importation of infectious biological agents, infectious substances, and vectors of human disease as outlined in the Import Permit regulations (42 CFR 71.54). eIPP maintains records associated with import permit application and inspections of importers of infectious biological agents, infectious substances, and vectors of human disease into the United States, which allows the regulated community to submit information electronically using the import permit forms approved by the Official of Management and Budget via a single web portal.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: For eFSAP portal, the following information in identifiable form (IIF) is collected for individuals: name, date of birth, department of justice identification number and job title. The Application for Registration (APHIS/CDC Form 1) requires the Responsible Official or Alternate Responsible Official (individual designated by an entity with the authority and control to ensure compliance with the select agent regulations) provide the name, date of birth, department of justice identification number and job title of each individual that has access to select agents and toxins. The information is shared with the Federal Bureau of Investigation (FBI)/ Criminal Justice Information Services Division (CJIS). The FSAP approves the individual or entity to possess, use and transfer select agents and toxins based on the security risk assessment performed by CJIS. For eIPP portal, the following information is collected from the applicant to receive an import permit as required under 42 CFR 71.54. 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.

CATEGORIES OF RECORDS IN THE SYSTEM: The DSAT maintains records which include the names of the Responsible Official, alternate Responsible Official, owners of non-governmental entities, and individuals who have access, or who have applied to have access to select agents (defined as a virus, bacteria, fungus or toxin that could pose a severe threat to public health and safety, to animal or plant health; or animal or plant products), and the list of select agents to which they have access. The Responsible Official, alternate Responsible Official, owners of non-governmental entities, and individuals requesting access to select agents are required to provide their name, date of birth, and job title and the name of the institution that would be housing the select agent(s). Other information collected under the select agent regulations include records associated with information regarding an entity's registration such as the list of select agents or toxins, list of individuals who will have access to select agents and toxins, laboratory information, the transfers of select agents and toxins, and the identification and final disposition of any select agent or toxin contained in a specimen presented for diagnosis, verification, and proficiency testing, inspections of registered entities and reports of any theft, loss or release of select agent or toxin. 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. In addition, information for import permits include records associated with import permit application and inspections of importers of infectious biological agents, infectious substances, and vectors of human disease into the United States.

RECORD SOURCE CATEGORIES: For eFSAP portal, applicants registering for possession, use, and transfer of select agents and the U.S. Attorney General. For eIPP portal, applicants seeking to import infectious biological agents, infectious substances, and vectors of human disease into the United States.

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

1. Records may be disclosed to contractors to handle program work overflow duties, performing many of the same functions (listed in the Purpose section above) as DSAT employees. Contractors are required to maintain Privacy Act safeguards with respect to such records.

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

3. Personal information from this system may be disclosed as a routine use to assist the recipient Federal agency in making a determination concerning an individual's trustworthiness to access select agents; to any Federal or State agency where the purpose in making the disclosure is to prevent access to select agents for use in domestic or international terrorism or for any criminal purpose; or to any Federal or State agency to protect the public health and safety with regard to the possession, use, or transfer of select agents.

5. 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.

6. Records or portions of records may be disclosed 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.

7. 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.

8. Records may be disclosed to the Office of Inspector General, Department of Health and Human Services, and 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. Records may be disclosed to appropriate agencies, entities, and persons when HHS/CDC (1) suspects or has confirmed that there has been a breach of the system of records, (2) has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS/CDC (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/CDC efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

10. Records may be disclosed to appropriate agencies, entities, and persons when HHS/CDC 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: 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 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 location. Computer workstations, lockable personal computers, and automated records are located in secured areas.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:
To retrieve the IFF, name of individual or department of justice identification number is used.
POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The DSAT records and associated information are retained and dispositioned in accordance with DSAT records retention schedule, N1-442-06-1. 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. Data will be destroyed in a manner that precludes its reconstruction, such as secured cross shredding.

Electronic information will be deleted or overwritten using Department of Defense strength NIST/GSA approved overwriting software that wipes the entire physical disk and not just the virtual disk. Physical destruction is obtained by using a NSA approved degaussing device.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. **Authorized Users**: A database security package is implemented on CDC computers to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Individuals who have routine access to these records are limited to staff (FTEs and contractors having security clearances at T3 or T4 levels) who have responsibility for conducting regulatory oversight.

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 that is limited to staff who responsibility for conducting regulatory oversight. Electronic data files are encrypted using FIPS 140-2 certified AES-256 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 a proper mix of portable fire extinguishers is located throughout the computer room. The system is backed up on a nightly basis. 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 backups, 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 hard drives. 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 that includes breach notifications.

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 OPHPR 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.

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.

NOTIFICATION PROCEDURE: An individual may learn if a record exists about himself or herself by contacting the system manager at: Director, DSAT, OPHPR, Bldg. 20, Rm. 4100, MS A46, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30329 and Director, AgSAS, Animal and Plant Health Inspection Service, 4700 River Road, Unit 2, Mailstop 22, Riverdale, MD 20737. 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.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT: None.

HISTORY:

- Federal Register notice Vol. 72, No. 126, Tuesday, July 2, 2007, pages 35993-35997, was published to add the System of Records, 09-20-0170, National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER.
- Federal Register notice Vol. 76, No. 16, January 25, 2011, pages 4483-4485, was published to alter the System of Records, 09-20-0170, National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER.