which . . . . is privileged or confidential''—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at *www.regulations.gov,* we cannot redact or remove your comment unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before December 28, 2020. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy.*

Josephine Liu,

Assistant General Counsel for Legal Counsel.

[FR Doc. 2020–23764 Filed 10–26–20; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[Docket No. CDC–2020–0089]

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 modified 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 modifying a system of records maintained by the Centers for Disease Control and Prevention (CDC), 09–20–0170, National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER. SATERIS is a national database registry containing the name of and location information about individuals possessing, using, or transferring select agents and toxins and characterization information about the agents and toxins, as required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. HHS/CDC is changing the name of the system of records to ''Electronic Federal Select Agent Program Portal (eFSAP Portal)'' and making other updates, some of which result from an information technology (IT) system upgrade.

DATES: The modified system of records is applicable October 27, 2020, subject to a 30-day period in which to comment on the routine uses. Written comments must be received on or before November 27, 2020.

ADDRESSES: You may submit comments, identified by Docket No. CDC–2020–0089 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: General questions about the modified system of records may be submitted to 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, (770) 488–8524.

SUPPLEMENTARY INFORMATION:

I. Background on the Federal Select Agent Program and eFSAP Portal IT System

HHS/CDC and the U.S. Department of Agriculture, Animal and Plant Health Inspection Service (USDA/APHIS) jointly manage the Federal Select Agent Program (FSAP). FSAP oversees the possession, use, and transfer of biological select agents and toxins (BSAT), as outlined in the select agent regulations (42 CFR part 73, 9 CFR part 121, and 7 CFR part 331). BSAT have the potential to pose a severe threat to public, animal or plant health or to animal or plant products.

BSAT are divided into four categories based on whether an agent causes disease in humans, animals, plants, or a combination of humans and animals. HHS/CDC regulates the possession, use, and transfer of BSAT that have the potential to pose a severe threat to public health and safety. USDA/APHIS regulates the possession, use, and transfer of BSAT that pose a severe threat to animal or plant health or products. HHS/CDC and USDA/APHIS regulate overlapping BSAT that have the potential to pose a severe threat to both public health and safety and to animal health or products.

The information that FSAP collects in order to track possession, use, and transfer of BSAT includes: Registration records about a registered entity or individual, identifying BSAT at each of the registrant's locations or facilities and the individuals approved for access to BSAT at each location or facility; laboratory biosafety and security information for BSAT; information about transfers of BSAT; identification and final disposition of any BSAT contained in a specimen presented for diagnosis, verification, or proficiency testing; observations from the inspections of each registered individual or entity; and reports of any theft, loss, or release of BSAT.

The IT system used by FSAP to track possession, use, and transfer of BSAT has been upgraded to allow the regulated community to report required information or make requests to FSAP electronically, via a single web portal known as the eFSAP portal. The eFSAP portal is a single web-based information management system shared by HHS/CDC and USDA/APHIS.

As upgraded, the IT system will continue to utilize a secure database environment and to contain the same information that was included in SATERIS. Allowing electronic submissions from the regulated community will enable the regulated community to interact with FSAP more

efficiently, allow for better and faster reporting of potential losses, reduce program burdens and reliance on labor-intensive and paper-based processes, and enable HHS/CDC and USDA/APHIS to more rapidly provide regulatory responses and guidance and respond to emergency events involving BSAT that may impact public health and safety.

II. Modifications Made to System of Records 09–20–0170

HHS/CDC has made the following modifications to the system of records:

- Changed the name of the system of records to Electronic Federal Select Agent Program Portal (eFSAP Portal).
- Updated the System Location and System Manager information.
- Updated the Authority section to add ''Subtitle A, Title II'' and ''42 U.S.C. 262a'' before and after ''Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Pub. L. 107–188),'' and to remove ''The Agricultural Bioterrorism Protection Act of 2002'' which authorizes maintenance of related USDA/APHIS records but not the HHS/CDC records covered in this system of records.
- Shortened and simplified the Purpose description.
- Revised the Categories of Individuals section by adding individual or sole proprietor applicants/registrants.
- Reorganized and expanded the Categories of Records section to list each category of record with a description or list of data elements specific to that category.
- Expanded the Record Source Categories section to include all applicable sources.
- Added five new routine uses.

○ New routine use 1 authorizes disclosures to USDA to provide comprehensive and effective oversight of BSAT, compliance with select agent regulations, and administration of FSAP.

○ New routine use 4 authorizes disclosures to agricultural authorities for the purpose of dealing more effectively with outbreaks of animal and plant diseases or other conditions of agricultural significance.

○ New routine use 8 authorizes disclosures of records that indicate a violation, or possible violation, of law to relevant law enforcement authorities. This routine use is necessary to cover instances in which the law enforcement agency is unaware of the violation or potential violation, so is unable to initiate a request for the records under subsection (b)(7) of the Privacy Act (5 U.S.C. 552a(b)(7)).

○ New routine use 9 authorizes disclosures to relevant government agencies and jurisdictions for the purpose of investigating potential fraud, waste, and abuse.

○ New routine use 10 authorizes disclosures to the National Archives and Records Administration (NARA) for records management inspections.

- Revised four routine uses.

○ Routine use 2, which authorizes disclosures to FSAP contractors, no longer mentions certain duties a contractor would perform but describes them as ''the functions listed in the Purpose section.''

○ Routine use 3 now authorizes disclosures to ''federal law enforcement authorities'' (in addition to public health and cooperating medical authorities, previously the only authorities identified) for the purpose of dealing more effectively with ''emergency events involving BSAT that may impact public health and safety'' (rather than ''outbreaks and conditions of public health significance'').

○ Routine use 5, which authorizes disclosures to assist federal agencies in determining an individual's trustworthiness to access biological select agents and toxins (BSAT), now uses the broader term ''BSAT'' instead of ''select agents'' and omits, as unnecessary, the word ''recipient'' before ''federal agencies.''

○ Routine use 6 now permits disclosures not only to the Department of Justice but also to ''a court or other adjudicative body,'' for use not only in litigation but also in ''other proceedings,'' when relevant and necessary to the proceedings.

- Changed the description in the Storage section to state that the oldest inactive records are in paper form and that all other records are stored electronically, instead of describing particular storage media (''file folders, computer tapes and disks, CD–ROMs'').
- Updated the Retention section to identify the current disposition schedule, DAA–0442–2019–001, instead of the previous schedule cited, N1–442–06–01; and to move descriptions of secure destruction methods to the Safeguards section.
- Updated the Safeguards section to refer to current governing statutes, policies and guidelines, including the description of secure destruction methods, and to include additional safeguards (*e.g.,* encryption, firewalls, and intrusion detection systems, and reviewing security controls on an ongoing basis).
- Updated the Access, Amendment, and Notification Procedures sections to allow a requester to provide a written certification to verify the requester's identity, and to state that an accounting of disclosures may also be requested.

Because some of these changes are significant, HHS provided advance notice of the modified system of records to the Office of Management and Budget and Congress as required by 5 U.S.C. 552a(r) and OMB Circular A–108.

Dated: October 22, 2020.

Suzi Connor,

Chief Information Officer, Centers for Disease Control and Prevention.

SYSTEM NAME AND NUMBER:

Electronic Federal Select Agent Program Portal (eFSAP Portal), 09–20–0170.

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, CDC, 1600 Clifton Rd. NE, Atlanta, GA 30329, (404) 718–2000, *lrsat@cdc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Subtitle A, Title II, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law 107–188 (42 U.S.C. 262a).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to cover records about individuals, retrieved by personal identifier, that HHS/CDC uses in managing the Federal Select Agent Program (FSAP) to track the possession, use, and transfer of biological select agents and toxins (BSAT), in order to ensure that BSAT are managed appropriately to prevent potential threats to public health.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records are about these categories of individuals:

- Individuals who in an individual (*i.e.,* sole proprietorship) capacity have applied for or received a certificate of registration from FSAP.
- Individuals designated as an entity applicant's Responsible Official and Alternate Responsible Official.
- Other individuals identified in an application as requesting or needing

access to BSAT under 42 CFR part 73, otherwise known as the HHS select agent regulations. The FSAP approves, or disapproves, these individuals to possess, use, and transfer BSAT based on the security risk assessments performed by the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division (CJIS), Bioterrorism Risk Assessment Group (BRAG).

CATEGORIES OF RECORDS IN THE SYSTEM:

The system of records includes these categories of records, some of which are forms approved by the Office of Management and Budget (OMB):

- *Request for Exclusion:* This type of request is submitted to the FSAP by an individual or entity applicant or registrant to seek a determination by the HHS Secretary that an attenuated strain or modified toxin does not pose a severe threat to public health and safety (see 42 CFR 73.3(e) and 73.4(e)).
- *Report of Identification of Select Agent or Toxin (APHIS/CDC Form 4).* This form is used by a clinical or diagnostic laboratory to notify the FSAP that BSAT has been identified as the result of diagnosis, verification, or proficiency testing or has been disposed of or transferred in accordance with regulatory requirements (see 42 CFR 5(a)–(b) and 6(a)–(b)).
- *Request for Exemption (APHIS/CDC Form 5).* This form is used by an individual or entity registrant or applicant seeking an exemption on the basis that it is using an investigational product that is, bears, or contains BSAT (see 42 CFR 5(d) and 6(d)).
- *Application for Registration (APHIS/CDC Form 1).* This form is used by an individual or entity to apply for a certificate of registration from the FSAP. The applicant completes the form by providing location or facility information; a list of BSAT in use, possession, or for transfer by the applicant; characterization of each BSAT the applicant will possess; the name, date of birth, and job title of each individual who needs access to BSAT; and laboratory information such as biosafety level, building and room location (see 42 CFR 7(d)). FSAP assigns a DOJ identification number for each individual associated with application so that individuals can submit information to BRAG for security risk assessment. This form is also used by an applicant or registrant to amend the registration if any changes occur in the information submitted (see 42 CFR 7(h)(1)).
- *Security Risk Assessment.* BRAG uses the information the applicant provides in the Application for Registration about each individual needing access to BSAT to perform a security risk assessment of each individual and provides the assessments to the FSAP. FSAP uses the information to approve individuals to access BSAT following a security risk assessment (see 42 CFR 10(a)).
- *Documentation of Inspection:* Prior to issuance of a certificate of registration, the FSAP will inspect the applicant's locations or facilities to ensure compliance with the select agent regulations and will document the inspection, including the applicant's responses to any written requests from the FSAP (see 42 CFR 18).
- *Request for Expedited Review:* An individual or entity applicant or registrant may apply to the HHS Secretary or APHIS Administrator for an expedited review (*i.e.,* an expedited security risk assessment) by the Attorney General of an individual identified as needing access to BSAT. The request is made by submitting a request in writing to the HHS Secretary establishing the need for such action (see 42 CFR 10(e)).
- *Security Plan:* An individual or entity required to register with the FSAP must develop and implement a written security plan, which must be sufficient to safeguard BSAT against unauthorized access, theft, loss, or release (see 42 CFR 11(a)). As a condition of registration, an individual or entity is required to provide a copy of the plan to the FSAP.
- *Biosafety Plan:* An individual or entity required to register with the FSAP must develop and implement a written biosafety plan that is commensurate with the risk of BSAT, given its intended use. The biosafety plan must contain sufficient information and documentation to describe the biosafety and containment procedures for each BSAT the individual or entity will possess, including any animals (including arthropods) or plants intentionally or accidentally exposed to or infected with a select agent (see 42 CFR 12(a)). As a condition of registration, an individual or entity is required to provide a copy of the plan to the FSAP.
- *Request Regarding a Restricted Experiment:* An individual or entity may not conduct, or possess products resulting from certain experiments unless approved by and conducted in accordance with the conditions prescribed by the HHS Secretary; these requests to seek such approval to conduct restricted experiments are maintained by FSAP (see 42 CFR 13(a)).
- *Incident Response Plan:* An individual or entity required to register under this part must develop and implement a written incident response plan based upon a site-specific risk assessment. The incident response plan must be coordinated with any entity-wide plans, be kept in the workplace, and be available to employees for review (see 42 CFR 14(a)). As a condition of registration, an individual or entity is required to provide a copy of the plan to the FSAP.
- *Training Record:* A registered individual, or a registered entity's Responsible Official, must ensure training is provided to each individual with access to BSAT and each escorted individual (*e.g.,* laboratory workers, visitors, etc.) and that a record of the training is maintained. The record must include the name of each such individual, the date of the training, a description of the training provided, and the means used to verify that the individual understood the training (see 42 CFR 15(d)), and a copy of the training record may be requested by FSAP.
- *Request to Transfer Select Agent or Toxin (APHIS/CDC Form 2).* This form is used by a registered individual or entity to request pre-authorization from FSAP to receive or send a specific BSAT (see 42 CFR 16).
- *Other Records:* An individual or entity required to register with the FSAP must maintain complete records relating to the activities covered by the select agent regulations, any of which may be requested by FSAP (see 42 CFR 17(a)).
- *Report of Potential Theft, Loss, or Release of Select Agent or Toxin form (APHIS/CDC Form 3).* This form is completed by a registered individual or entity to report any theft, loss, or release of BSAT to FSAP (see 42 CFR 19(a)–(b)).

RECORD SOURCE CATEGORIES:

The records in the system of records are obtained from the individuals and entities applying for or receiving a certificate of registration from FSAP to possess, use, and transfer BSAT or permit individuals to access BSAT; or from FSAP, or from BRAG.

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 (b)(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 USDA to provide comprehensive and effective oversight of BSAT, compliance with select agent regulations, and administration of FSAP.

2. Records may be disclosed to contractors engaged to assist FSAP with performing the functions listed in the Purpose section above. Contractors are required to maintain Privacy Act safeguards with respect to such records.

3. Records may be disclosed to state health departments and other public health, cooperating medical or federal law enforcement authorities to deal more effectively with emergency events involving BSAT that may impact public health and safety.

4. Records may be disclosed to state agriculture departments and other agriculture cooperating authorities to deal more effectively with outbreaks of animal and plant diseases or other conditions of agriculture significance.

5. Personal information from this system of records may be disclosed as a routine use, to assist in making a determination concerning an individual's trustworthiness to access BSAT, to any federal or state agency where the purpose in making the disclosure is to prevent access to BSAT for use in domestic or international terrorism or for any criminal purpose; or to any federal or state agency to protect the public, animal, and plant health and public safety with regard to the possession, use, or transfer of BSAT.

6. 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 components 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.

7. 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.

8. 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 the 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.

9. 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.

10. 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.

11. 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.

12. 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 oldest inactive records are in paper form; all other records are stored electronically.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by the subject individual's name or DOJ identification number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained for 10 years, or until such time as the records are no longer needed for litigation or other records purposes and are then disposed of in accordance with FSAP disposition schedule DAA–0442–2019–0001. Records are 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 is 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 conform to the HHS Information Security and Privacy Program, *http://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 are implemented on government computers to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed by FSAP on a regular basis. Individuals who have routine access to these records are 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 includes programmed verification of valid user identification code and password prior to logging on to the system; mandatory password changes, limited number of log-in attempts, virus protection, encryption, firewalls, and intrusion detection systems, and user rights/file attribute restrictions. Password protection imposes username and password log-in requirements to prevent unauthorized access. Each username is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures, and backup files are securely stored off-site.

Security controls are reviewed on an ongoing basis.

• 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.

• FTEs 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 identifiable data are used in a room, admittance at either federal or contractor sites is restricted to specifically authorized personnel.

• Appropriate Privacy Act provisions and breach notification provisions are included in applicable 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 federal government or destroyed, as specified by the contract that includes breach notifications.

• Records that are eligible for destruction are disposed of using destruction methods prescribed by NIST SP 800–88. Hard copy records are placed in a locked container or designated secure storage area while awaiting destruction. Records are 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 is obtained by using a National Security Agency/Central Security Service (NSA/CSS) approved degaussing device.

PHYSICAL SAFEGUARDS:

• Paper records are maintained in locked cabinets in restricted areas to which access is controlled by an electronic cardkey system and is limited to staff who have responsibility for conducting regulatory oversight.

• Electronic data files are stored in a restricted access location. The computer room is protected by an automatic sprinkler system and numerous automatic sensors (*e.g.,* water, heat, smoke, etc.) which are monitored, and a proper mix of portable fire extinguishers is located throughout the computer room. Computer workstations, lockable personal computers, and automated records are 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 DOJ identification 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 records, 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:

72 FR 35993 (July 2, 2007); 76 FR 4483 (Jan. 25, 2011), 83 FR 6591 (Feb. 14, 2018).

[FR Doc. 2020–23770 Filed 10–26–20; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2015–N–0030]

Memorandum of Understanding Addressing Certain Distributions of Compounded Human Drug Products Between the State Board of Pharmacy or Other Appropriate State Agency and the Food and Drug Administration; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of availability; withdrawal.

SUMMARY: The Food and Drug Administration (FDA or the Agency) is announcing the availability of a final standard memorandum of understanding (MOU) entitled ''Memorandum of Understanding Addressing Certain Distributions of Compounded Human Drug Products Between the [insert State Board of Pharmacy or Other Appropriate State Agency] and the U.S. Food and Drug Administration'' (final standard MOU). The final standard MOU describes the responsibilities of a State Board of Pharmacy or other appropriate State agency that chooses to sign the MOU in investigating and responding to complaints related to drug products compounded in such State and distributed outside such State and in addressing the interstate distribution of inordinate amounts of compounded human drug products.

DATES: The announcement of the MOU is published in the **Federal Register** on October 27, 2020. FDA is withdrawing its revised draft standard MOU that published on September 10, 2018 (83 FR 45631), as of October 27, 2020.

ADDRESSES: Submit electronic comments on the final standard MOU to Docket No. FDA–2015–N–0030. Submit written comments on the final standard MOU to the Dockets Management Staff (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm.