## 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:** Division of Select Agents and Toxins (DSAT), Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER), 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, 09–20–0170, National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER". 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 Office for Terrorism Preparedness and Emergency Response (COTPER), Division of Select Agents and Toxins (DSAT).

**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 COTPER/DSAT receives comments that would result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by the Privacy Act System of Record Number 09–20–0170:

- *Federal eRulemaking Portal: http://regulations.gov*. Follow the instructions for submitting comments.
- *E-mail:* Include PA SOR number 09–20–0170 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:** COTPER/DSAT proposes to alter System of Records, No. 09–20–0170, "National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER". Records maintained in the National Select Agent Registry (NSAR)—a joint DSAT and U.S. Department of Agriculture/Animal and Plant Health Inspection Service (APHIS) information management system—are accessed by DSAT through the Select Agent Transfer and Entity Registration Information System (SATERIS) which is an user interface for data entry, data query, and routine reporting activities. The purpose of this system of records is to limit access to those select agents listed in 42 CFR Part 73, 9 CFR Part 121, and 7 CFR Part 331 to those individuals who have a legitimate need to handle or use such select agents, and who are not identified as a restricted person by the U.S. Attorney General. The NSAR is also used to track the possession, use, and transfer of select agents and is a single Web-based system shared by DSAT and APHIS.

DSAT conducts regulatory oversight of individuals and entities that possess, use, or transfer select agents. This includes the review of registration applications, conducting inspections of registered facilities or facilities requesting registration, processing requests to import select agents, processing all reports and requests received from individuals or entities regarding a select agent, and maintaining this information pertaining to individuals and entities that possess, use, and/or transfer select agents.

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)*

Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER)

**National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS)**

*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. 09–20–0170," National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER". 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*

Records maintained in the National Select Agent Registry (NSAR)—a joint DSAT and U.S. Department of Agriculture/Animal and Plant Health Inspection Service (APHIS) information management system—are accessed by DSAT through the Select Agent Transfer and Entity Registration Information System (SATERIS) which is an user interface for data entry, data query, and routine reporting activities. The purpose of this system of records is to limit access to those select agents listed in 42 CFR Part 73, 9 CFR Part 121, and 7 CFR Part 331 to those individuals who have a legitimate need to handle or use such select agents, and who are not identified

as a restricted person by the U.S. Attorney General. The NSAR is also used to track the possession, use, and transfer of select agents and is a single Web-based system shared by DSAT and APHIS.

DSAT conducts regulatory oversight of individuals and entities that possess, use, or transfer select agents. This includes the review of registration applications, conducting inspections of registered facilities or facilities requesting registration, processing requests to import select agents, processing all reports and requests received from individuals or entities regarding a select agent, and maintaining this information pertaining to individuals and entities that possess, use, and/or transfer select agents.

**II. Authority for Maintenance of the System**

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and the Agricultural Bioterrorism Protection Act of 2002 (Pub. L. 107–188).

**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:

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.

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.

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.

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.

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.

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**

The routine uses proposed for this System are compatible with the stated purpose of the System:

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.

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 by file folders, computer tapes and disks, CD–ROMs. The records are retrieved by name or DOJ identifier number.

The following special safeguards are provided to protect the records from inadvertent disclosure:

*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 Select Agent Program staff (DSAT FTEs and contractors) who have responsibility for conducting regulatory oversight of individuals and entities that possess, use, or transfer select agents.

*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 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.

*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. When possible, 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.

The USDA/APHIS maintains similarly stringent safeguards that are discussed within that agency's Select Agent system of records notice.

*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.

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 and Sensitive But Unclassified (SBU) information designated for local disposition will be placed in a locked container or designated secure storage area while awaiting destruction. All SBU data 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.

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

A. *Full Title:* "National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER."

*OMB Control Number:* 09–20–0170.

*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. 2010–33028 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:** Division of Global Migration and Quarantine, National Center for the Preparedness, Detection, and Control of Infectious Disease (NCPDCID), Coordinating Center for Infectious Diseases (CCID), 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, 09–20–0171, "Quarantine and Traveler Related Activities, including Records for Contract Tracing Investigation and Notification under 42 CFR Parts 70 and 71, HHS/CDC/CCID." 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 Infectious Diseases (CCID), Division of Global Migration and Quarantine, National Center for the Preparedness, Detection, and Control of Infectious Disease (NCPDCID).

**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 CCID receives comments that would result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by the Privacy Act System of Record Number 09–20–0171:

- *Federal eRulemaking Portal: http://regulations.gov.* Follow the instructions for submitting comments.
- *E-mail:* Include PA SOR number 09–20–0171 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:** CCID proposes to alter System of Records, No. 09–20–0171, "Quarantine and Traveler Related Activities, including Records for Contract Tracing Investigation and Notification under 42 CFR Parts 70 and 71, HHS/CDC/CCID". This system maintains records on the conduct of activities (*e.g.,* quarantine, isolation) that fulfill HHS's and CDC's statutory authority under sections 311, 361–368 of the Public Health Service Act to prevent the introduction, transmission and spread of communicable diseases.

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