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

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 Center for Infectious Diseases (CCID)

Quarantine and Traveler Related Activities, Including Records for Contract Tracing Investigation and Notification Under 42 CFR Parts 70 and 71

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. 09–20–0171 "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.

B. Purpose

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.

Records are collected when individual known or suspected to have been exposed to serious communicable diseases arrives into the United States from foreign countries or is engaged in interstate or international movement These records are used to (1) document reports of illness that may pose a public health risk occurring while on board airplanes, maritime vessels, and at land-border crossings of persons arriving from foreign countries or traveling between States; (2) perform contact tracing investigations and notifications of passengers and crew when known or suspected exposures to serious communicable diseases occur on board a conveyance arriving in the United States from a foreign country or traveling from one State or possession to another; (3) inform international, Federal, State or local public health authorities so that these authorities may act to protect public health or safety; and (4) take such actions (*e.g.,* quarantine or isolation) as necessary to prevent the introduction, transmission, and spread of serious communicable diseases from persons arriving into the United States from foreign countries or persons engaged in interstate or international movement.

II. Authority for Maintenance of the System

Sections 311, 361–368 of the Public Health Service Act.

III. Proposed Routine Use Disclosures of Data in the System

This System of Records contains information on Individuals subject to quarantine or isolation orders, ill travelers (*i.e.,* passengers and crew), contacts of ill travelers, and/or individuals exposed or suspected of being exposed to serious communicable diseases.

Passenger and crew manifests from conveyances carrying individuals subject to 42 CFR parts 70 and 71, case reports, illness response forms, medical assessments, medical records (including but not limited to clinical, hospital and laboratory data and data from other relevant tests), name, address, date of birth, and related information and documents collected for the purpose of carrying out agency responsibilities under sections 311 and 361–368 of the Public Health Services Act.

Records may be disclosed to contractors to handle program work duties, performing many of the same functions as FTEs within DGMQ in situations where additional staff is required. Contractors are required to maintain Privacy Act safeguards with respect to such records.

Records may be disclosed to State and local health departments and other cooperating medical and public health authorities and their counsel to more effectively deal with outbreaks and other significant public health conditions.

Personal information from this system may be disclosed as a routine use to appropriate conveyance personnel, Federal agencies, State and local health departments, Department of State and embassy personnel (U.S. and foreign), and health authorities in foreign countries for contact tracing investigations and notifications of possible exposures to serious communicable diseases in connection with travel.

Records may be disclosed to the Department of Homeland Security to restrict travel of persons who pose a public health risk and in the instance of suspected domestic or international terrorism.

Disclosure may be made to medical personnel providing evaluation and care for ill or exposed persons, including travelers.

Records may be disclosed to the World Health Organization in accordance with U.S. responsibilities as a signatory to the International Health Regulations or other international agreements.

Personal information may be disclosed to Federal, State, and local authorities for taking necessary actions to place someone under quarantine or isolation, for enforcement of other quarantine regulations, or to protect the public's health and safety. Records may be disclosed to cooperating State and local legal departments enforcing concurrent legal authority related to quarantine or isolation activities.

In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program 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 appropriate agency, whether Federal, foreign, State or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

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.

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 address listed above. Requesters in person must provide driver's license or other positive identification. Individuals who do not appear in person must either: (1) Submit a notarized request to verify their identity; or (2) certify that they are the individuals they claim to be and that they understand that 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.

An individual who requests notification of or access to medical records shall, at the time the request is made, designate in writing a responsible representative who is willing to review the record and inform the subject individual of its contents.

A parent or guardian who requests notification of, or access to, a child's medical record shall designate a family physician or other health professional (other than a family member) to whom the record, if any, will be sent. The parent or guardian must verify relationship to the child by means of a birth certificate or court order, as well as verify that he or she is who he or she claims to be.

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 in Electronic media and file folders for hard-copy records. The records are retrieved by name of the individual or other identifying particulars.

The records in this System have the following safeguards in place to maintain and protect the information as it relates to Authorized users, physical and procedural safeguards:

Authorized Users: A database security package is implemented on CDC's computer systems to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control and Prevention (CDC), or its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards: Access to the CDC Clifton Road facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. Access to the data entry area is also controlled by a cardkey system. Guard service in buildings provides personnel screening of visitors. Local fire department is located directly next door to the Clifton Road facility. 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. Computer files are backed up on a routine basis. Hard-copy records are stored in locked cabinets at CDC headquarters and CDC Quarantine stations which are located in a secure area of the airport.

Procedural Safeguards: Protection for computerized records, both on the mainframe and the National Center Local Area Network (LAN), 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 back-up procedures, and secure off-site storage is available. To avoid inadvertent data disclosure, measures are taken to ensure that all data are removed from electronic media containing Privacy Act information. Additional safeguards may be built into the program by the system analyst, as warranted by the sensitivity of the data.

CDC and contractor employees who maintain records are instructed to check with the system manager prior to making disclosures 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. 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.

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 National Centers' LANs 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 records in this System are retained and disposed of in the following way: The records in this System are retained and disposed of in the following way: Contact tracing records will be maintained in the agency until the contact investigation is complete or no longer than twelve months, in accordance with proposed retention schedules; remaining quarantine records would be maintained 10 or 20 years, based on the applicable CDC records control schedule. Disposal methods include wiping electronic media and macerating paper materials.

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

A. *Full Title:* "Quarantine and Traveler Related Activities, including Records for Contract Tracing Investigation and Notification under 42 CFR Parts 70 and 71, HHS/CDC/CCID".

OMB Control Number: 09–20–0171.

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. 2010–33029 Filed 1–24–11; 8:45 am]

BILLING CODE 4163–18–P