Federal Communications Commission
Marlene H. Dortch,
Secretary.
[FR Doc. 07–3234 Filed 6–28–07; 2:56 pm]
BILLING CODE 6712–01–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 New System of Records.

SUMMARY: In accordance with the requirements of the Privacy Act, the Centers for Disease Control and Prevention (CDC) is proposing to establish a new system of records (SOR), 09–20–0170, "National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER." The purpose of the system is to limit access to those biological agents and toxins 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 agents or toxins, and who are not identified as restricted persons by the U.S. Attorney General. NSAR 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 select agents and toxins that could pose a severe threat to public health and safety, to the health and safety of animals, and to the safety of plants or animal and plant products. We have provided background information about the new system in the **SUPPLEMENTARY INFORMATION** section below.

DATES: *Effective Date:* CDC filed a new SOR report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Homeland Security & Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on June 25, 2007. CDC invites interested parties to submit comments on the proposed routine uses. To ensure that all parties have adequate time in which to comment, the new system will be effective 30 days from the publication of this notice, or 40 days from the date it was submitted to OMB and the Congress, whichever is later, unless CDC receives comments that persuade us to defer implementation.

ADDRESSES: Comments should be addressed to the CDC Privacy Act Officer at the address listed below. Comments received will be available for review at this location by appointment during regular business hours from 8 a.m. to 4:30 p.m., Monday through Friday in the CDC Roybal Facility, Building 21, Room 8125, Atlanta, Georgia.

FOR FURTHER INFORMATION CONTACT: Betsey S. Dunaway, Privacy Act Officer, Office of the Chief Science Officer, Centers for Disease Control and Prevention, 1600 Clifton Road, NE., Building 21, Room 8125, Mailstop D–74, Atlanta, Georgia 30333, (404) 639–4642.

SUPPLEMENTARY INFORMATION: CDC proposes to establish a new system of records within its Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER): 09–20–0170, "National Select Agent Registry (NSAR)/ Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER." An important component of the nation's overall terrorism deterrence policy, the Division of Select Agents and Toxins (DSAT) in the Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER) within the CDC regulates the possession, use, and transfer of biological agents and toxins (select agents) that could pose a severe threat to public health and safety. A select agent is 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.

I. Description of the Proposed System of Records

A. Statutory and Regulatory Basis for SOR. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires entities to register with the U.S. Department of Health and Human Services (HHS) if they possess, use, or transfer select agents that could pose a severe threat to public health and safety. The Agricultural Bioterrorism Protection Act of 2002 requires that facilities handling select agents that could pose a severe threat to animal or plant health; or animal or plant products register with the USDA. Within HHS, the DSAT is responsible for registering entities and personnel who either possess or are applying for approval to possess, use or transfer select agents that could pose a severe threat to public health and safety. Within the USDA, APHIS has a similar responsibility for registering entities and personnel handling agents that pose a severe threat to animal or plant health; or animal or plant products.

The Acts require safeguards and security measures that will adequately protect these agents. This includes controlling access and screening of entities and personnel through security risk assessments conducted by the U.S. Attorney General. The Acts also require the establishment of a national database of registered entities. While some entities register for select agents regulated only by HHS, others for select agents regulated only by USDA, there are a number of entities registering for select agents that can pose a severe threat to public health and safety, to animal health, or to animal products ("overlap" select agents). Since DSAT and APHIS coordinate regulatory activities for those overlap select agents that would be regulated by both agencies, the Acts require that a single national database be established. This new Privacy Act system of records notice (SORN) describes the records and processes that enable DSAT to fulfill HHS' requirements; APHIS will be publishing a similar SORN to address how USDA will fulfill theirs.

B. Collection and Maintenance of Data in the System

CDC will only collect the minimum amount of personal data necessary to achieve the purpose of this system, which is to limit access to the 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 agents, and who are not identified as a restricted person by the U.S. Attorney General. The data elements required are: name, address, date of birth, job title, and the name of the institution that would be housing the select agent(s).

Entities handling select agents must appoint a Responsible Official within their organization who certifies that the entity meets federal requirements for handling select agents such as having security measures in place to protect the select agents they possess from theft, loss and unauthorized access, and safety measures to prevent the release of agents. DSAT's SOR includes personal information on those individuals who have access or who have applied to have access to select agents, and the list of select agents to which they have access or would have access.

II. Agency Policies, Procedures, and Restrictions on the Routine Use

The Privacy Act permits 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 disclosure of data is known as a "routine use." The government will only release select agent information that can be associated with an individual as provided for under "Section III. Proposed Routine Use Disclosures of Data in the System." We will only collect the minimum personal data necessary to achieve the purpose of this system.

CDC has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure and only after CDC:

A. Determines that the use or disclosure is consistent with the reason that the data are being collected, e.g., to limit access to select agents to those individuals who have a legitimate need to handle or use select agents and who are not identified as a restricted person by the U.S. Attorney General.

B. DETERMINES THAT:

1. The purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

2. The purpose for which the disclosure is to be made is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and

3. There is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

C. Requires the information recipient to:

1. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

2. Remove or destroy at the earliest time all identifiable information; and

3. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

D. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

The Privacy Act permits 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 disclosure of data is known as a "routine use." The proposed routine uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

A. Records may be disclosed to contractors to handle program work overflow duties, performing many of the same functions as DSAT employees. Contractors are required to maintain Privacy Act safeguards with respect to such records. These functions include conducting regulatory oversight of individuals and entities that possess, use, or transfer select agents, including the review of registration applications, conducting inspections of registered facilities or facilities requesting registration, and maintaining this information pertaining to individuals and entities that possess, use, and/or transfer select agents. DSAT contracts out certain functions when doing so would contribute to efficient and effective operations of the agency. DSAT must be able to give a contractor the information necessary for the contractor to fulfill its duties. Safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the Statement of Work and requires the contractor to return or destroy all information at the contract's completion.

B. 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. When outbreaks or other conditions of public health significance that might have been caused by exposure to select agents (either accidental or otherwise) occur, CDC's sharing of information on those individuals and organizations registered to possess select agents could prove beneficial to the health department's investigation.

C. 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.

Based on the provisions of the Acts, the Attorney General has the authority and responsibility to conduct electronic database checks (i.e., the security risk assessments) on the Responsible Official, alternate Responsible Official, owners of non-governmental entities, and individuals requesting access to select agents. The Federal Bureau of Investigation, Criminal Justice Information Services Division (CJIS), has been delegated authority for conducting these security risk assessments. Therefore, the information must be shared with the CJIS for them to conduct a security risk assessment to ensure that individuals requesting access to select agents are not identified as a restricted person based on criteria established in the U.S.A. Patriot Act. This is compatible with the overall purpose of the system—that only trustworthy individuals are granted access.

Other Federal or State agencies may require the information DSAT possesses on individuals with access to select agents and the institutions at which those agents are housed to aid in their investigations of domestic or international terrorism or for any other criminal purpose. The purpose of the system is to be certain that only individuals who have a legitimate need to handle or use such select agents have access to them; this routine use is compatible in that this disclosure is done to prevent access to select agents for terrorism or other criminal purposes. State emergency planners may need this identifiable information to fulfill their responsibilities.

The overall purpose of this SOR is to protect the public health and safety. Federal and State agency emergency responders may require DSAT's identifiable information if select agents are accidentally released or otherwise used inappropriately with the ultimate goal of protecting the public's health and safety. Records may also be shared with the Department of Transportation to ensure that the transfer of select agents is done safely and in compliance with their regulations—a use in line with CDC's purpose of safely transferring select agents for which it has responsibility.

D. 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. When a constituent requests a congressional office to facilitate obtaining information from this CDC system, it is compatible to provide such information, since this is in line with the overall purpose of the Privacy Act

which is to provide access to the subject individual of the records the government has on him or her.

E. 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.

Whenever CDC is involved in litigation dealing with the DSAT, and CDC policies or operations could be affected by the outcome of the litigation, CDC must be able to disclose identifiable information to the Department of Justice so that an effective defense could be presented.

IV. Safeguards

The CDC/DSAT has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel with access to the system have been trained in Privacy Act and information security requirements. Employees maintaining records are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal and HHS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the E-Government Act of 2002; the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS and CDC policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications and the HHS Information Systems Program Handbook.

V. Effects of the Proposed System of Records on Individual Rights

CDC proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CDC will take precautionary measures to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of individuals whose data are maintained in the system. CDC will collect only that information necessary to perform the system's purpose. In addition, CDC will make disclosures from the system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act. CDC, therefore, does not anticipate an unfavorable effect on individual privacy as a result of information relating to individuals.

Dated: June 22, 2007.

James D. Seligman,

Chief Information Officer, Office of the Director, Centers for Disease Control and Prevention.

Privacy Act System

NO. 09–20–0170

SYSTEM NAME:

National Select Agent Registry (NSAR)/Select Agent Transfer and Entity Registration Information System (SATERIS), HHS/CDC/COTPER.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Division of Select Agents and Toxins (DSAT), Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER), Bldg. 20, Centers for Disease Control and Prevention (CDC), 1600 Clifton Road, NE., Atlanta, GA 30333 and Federal Records Center, 4712 Southpark Blvd., Ellenwood, GA 30294.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The Responsible Official, alternate Responsible Official, owners of non-governmental entities, and individuals requesting access to select agents under the provisions of Part 73, of Title 42 of the Code of Federal Regulations (42 CFR part 73), Part 121 of Title 9 of the Code of Federal Regulations (9 CFR Part 121), and Part 331 of Title 7 of the Code of Federal Regulations (7 CFR part 331).

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, address, date of birth, and job title and the name of the institution that would be housing the select agent(s).

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).

PURPOSE(S):

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.

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.

4. Disclosure may be made to a congressional office from the record of an individual in response to a verified inquiry from the congressional office made at the written request of that individual.

5. 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.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM

STORAGE:

File folders, computer tapes and disks, CD–ROMs.

RETRIEVABILITY:

By name or DOJ identifier number.

SAFEGUARDS:

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

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 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.

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, 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.

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 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.

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 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.

RETENTION AND DISPOSAL:

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.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Select Agents and Toxins, Coordinating Office for Terrorism Preparedness and Emergency Response, Bldg. 20, Rm. 4100, MS A46, Centers for Disease Control and Prevention, 1600 Clifton Road, NE., Atlanta, GA 30333.

NOTIFICATION PROCEDURE:

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.

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.

RECORD SOURCE CATEGORIES:

Applicants registering for possession, use, and transfer of select agents and the U.S. Attorney General.

[FR Doc. E7–12682 Filed 6–29–07; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of a New System of Records

AGENCY: Department of Health and Human Services (HHS), Center for Medicare & Medicaid Services (CMS).

ACTION: Notice of a New System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system titled, "Medicare Master Death Records File (MMDRF), System No. 09–70–0597." Under the provisions of Sections 1106 (42 U.S.C. 1306 and 205(r) (42 U.S.C. 405(r) of the Social Security Act (the Act), the Social Security Administration (SSA) will provide to CMS the SSA Death Master File including unrestricted State death data. CMS will use this death data to: (1) Ensure that no future payments are made to any physician or individually enrolled practitioner and other individuals for whom CMS has a record of death, and (2) investigate and initiate an appropriate response where a deceased physician's billing number has been found to have been used as the basis for a request for payment for services allegedly rendered after the physician's date of death. Upon independent verification of the facts with respect to specific individuals, the results will be used to update CMS databases and may also be used to support payment recovery operations and or the work of law enforcement. We have provided additional background information about the new system in the "Supplementary Information" section below.

The primary purpose of this system is to collect and maintain Social Security Administration death records for physicians, non-physician practitioners and individuals associated with organizational providers and suppliers to ensure payments are not made for services rendered after confirmed date of death and to prevent and/or detect any fraud, waste and abuse. Information retrieved from this system may be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant, CMS grantee; (2) assist another Federal or State agency with information to contribute to the accuracy of CMS's proper payment of Medicare benefits, enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; (3) support litigation involving the agency; and (4) combat fraud, waste, and abuse in certain Federally-funded health benefits programs.

EFFECTIVE DATES: CMS filed a new system report with the Chair of the House Committee on Oversight and Government Reform, the Chair of the Senate Committee on Homeland Security and Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on *June 25, 2007.* To ensure that all parties have adequate time in which to comment, the new SOR, including routine uses, will become effective 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later, unless CMS receives comments that require alterations to this notice. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice.

ADDRESSES: The public should address comments to: CMS Privacy Officer, Division of Privacy Compliance, Enterprise Architecture and Strategy Group, Office of Information Services, CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.—3 p.m., Eastern Time zone.

FOR FURTHER INFORMATION CONTACT: Allen Gillespie, Technical Advisor, Division of Provider/Supplier Enrollment, Program Integrity Group, Office of Financial Management, Mail Stop C3–24–01, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244–1849. He can be reached by telephone at 410–786–5996, or via e-mail at *allen.gillespie@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION: CMS staff will develop a program to compare data on the monthly MMDRF with individuals in the Provider Enrollment Chain Ownership System (PECOS). A report of potential matches from the MMDRF and PECOS will be distributed monthly to the Parts A and B MACs and affiliated contractors. CMS will issue manual instructions with procedures contractors should follow to determine if the individual name on the monthly report is a match to the individual in the