tasks involved in gathering and producing the responsive information, and has applied an average hourly wage of $460/hour for their labor. Thus, the labor costs per applicant for expedited review should range from approximately $13,800 to $23,000.

Estimated Annual Capital or Other Non-Labor Costs

The capital or other non-labor costs associated with the information requests will be minimal. Industry members should already have in place the means to store information of the volume requested. In addition, respondents may have to purchase office supplies such as file folders, computer CDs or DVDs, photocopier toner, or paper in order to comply with the Commission's requests. The FTC estimates that such costs will be minimal.

For the Antitrust Division of the Department of Justice.

Sharis A. Pozen,

Chief of Staff and Deputy Assistant Attorney General.

For the Federal Trade Commission.

By direction of the Commission, Commissioner Rosch dissenting.

Donald S. Clark,

Secretary.

[FR Doc. 2011–9466 Filed 4–18–11; 8:45 am]

BILLING CODE 6750–01–P

DEPARMENT OF HEALTH AND HUMAN SERVICES

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

AGENCY: Office of Grants and Acquisition Policy and Accountability (OGAPA), Assistant Secretary for Financial Resources (ASFR), Department of Health and Human Services (HHS).

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

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, the HHS OGAPA is proposing to establish a new system titled, "HHS Consolidated Acquisition Solution (HCAS), System No. 09–90–0411." As an IT investment, HCAS is monitored by the HHS IT Investment Review Board (ITIRB). In addition to the ITIRB oversight, HCAS is monitored by the HHS/ASFR Office of Grants and Acquisition Policy and Accountability (OGAPA).

At HHS, there were seven different systems in place to support the people who make buying—procurement—possible. The HHS Consolidated Acquisition System (HCAS) is an initiative to reduce the number of duplicative acquisition systems, thereby streamlining and standardizing our procurement processes and systems across the Department. The use of disparate systems complicates all interfaces to financial, inventory, and other systems that HHS has or will employ.

HCAS replaced varying Procurement Request Information System (PRISM) configurations that existed across HHS, and replaced legacy acquisition systems and manual processes necessary for capturing HHS acquisition transactions for integration with the Unified Financial Management System (UFMS). We are also proposing routine uses for this system of records.

DATES: *Effective Dates:* The HHS ASFR/OGAPA 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 April 8, 2011. 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 HHS/ASFR/OGAPA receives comments that require alterations to this notice. Although the Privacy Act requires only that the HHS/ASFR/OGAPA provide an opportunity for interested persons to comment on the proposed routine uses, the HHS/ASFR/OGAPA invites comments on all portions of this notice.

FOR FURTHER INFORMATION OR COMMENTS CONTACT: The public should address comments to Kowanna Parran at HHS Office of the Secretary, Assistant Secretary for Financial Resources, Office of Grants and Acquisition Policy and Accountability, Hubert H. Humphrey Building, 200 Independence Avenue, Washington, DC 20201. Ms. Parran can be reached by telephone at (202) 205–0722 or via e-mail at *kowanna.parran@hhs.gov.* 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.

SUPPLEMENTARY INFORMATION: The HCAS system itself collects information necessary to support a procurement relationship between HHS and the vendor community. Information is collected on HHS Contracting Officers, and HHS vendors. There are limited instances where an individual's information in identifiable form (IIF) will be collected in order to facilitate a transaction in HCAS. HCAS collects and maintains IIF for service fellows and sole proprietorships that provide vendor services as individuals. Acquisition processes supported by HCAS include acquisition planning, solicitation, contract creation and approval, contract award and award closeout, and contract performance and management. To support these business processes, IIF contained in HCAS may include the following: vendor and contracting officer names, vendor mailing addresses, phone numbers, vendor financial account information, legal documents, Web URLs, e-mail addresses, vendor education records, and vendor tax ID numbers (TIN) or Social Security numbers.

The Privacy Act allows information disclosure 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 Government will only release HCAS information that can be associated with an individual as provided for under "Section III. Proposed Routine Use Disclosures of Data in the System." Both identifiable and non-identifiable data may be disclosed under a routine use. We will only collect the minimum personal data necessary to achieve the purpose of HCAS. We are proposing to establish the following routine use disclosures of information maintained in the system:

(1) To agency contractors or consultants who have been engaged by the agency to assist in the accomplishment of the HCAS Operations and Maintenance (O&M) function relating to the purposes for this system and who need to have access to the records in order to assist the OGAPA and HCAS O&M Federal leadership.

We contemplate disclosing information under this routine use only in situations in which OGAPA and HCAS O&M Federal leadership enters into a contractual or similar agreement with a third party to assist in accomplishing a HCAS function relating to purposes for this system.

The HHS Program Support Center (PSC) Financial Enterprise Systems Management (FESM) Operations and Maintenance (O&M) must be able to give a contractor or consultant whatever information is necessary for the contractor or consultant to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting

the contractor or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant to return or destroy all information at the completion of the contract.

(2) To the Department of Justice (DOJ), court or adjudicatory body when: the agency or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or the United States Government is a party to litigation or has an interest in such litigation, and by careful review, OGAPA determines that the records are relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

Whenever HHS OGAPA is involved in litigation, and occasionally when another party is involved in litigation and OGAPA policies or operations could be affected by the outcome of the litigation, OGAPA would be able to disclose information to the DOJ, court or adjudicatory body involved.

The HHS OGAPA will utilize a combination of administrative, technical, and physical controls to balance privacy and confidentiality with the system's goals. These controls include providing read-only access to HCAS users; authenticating users prior to granting access; controlling access levels and permissions based on user, role, and organizational unit; configuring all servers to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data; and physically restricting server access at the Department of Health and Human Services, National Institutes of Health, Center for Information Technology (CIT) Computer Room.

This system will conform to all applicable Federal laws and regulations, and HHS/Office of the Secretary 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; and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal and HHS/Office of the Secretary policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications and the HHS–OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook.

The OGAPA 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.

The OGAPA 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 patients whose data are maintained in this system. HCAS will collect only that information necessary to perform the system's functions. In addition, the OGAPA will make disclosure from the proposed 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. The OGAPA, therefore, does not anticipate an unfavorable effect on individual privacy as a result of information relating to individuals.

Dated: April 7, 2011.

Nancy J. Gunderson,

Deputy Assistant Secretary, Office of Grants and Acquisition Policy and Accountability, HHS/ASFR.

SYSTEM NO: 09–90–0411

SYSTEM NAME:

"HHS Consolidated Acquisition Solution (HCAS)," HHS/ASFR.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

NIH Center for Information Technology, 10401 Fernwood Road, Bethesda, MD 20817.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Information is collected on HHS Contracting Officers and HHS vendors who are service fellows or sole proprietorships that provide vendor services as individuals.

CATEGORIES OF RECORDS IN THE SYSTEM:

HCAS records include HHS statements of work, purchase requests, requests for proposals (RFPs), bids, proposals, vendor invoices, requisitions, contract awards, contract modifications, progress reports, financial status reports, audit reports, and contract deliverables.

Individual Information in Identifiable Form (IIF) contained in these records includes names of HHS contracting officers, vendor names, mailing addresses, phone numbers, financial account information, legal documents, Web URLs, and e-mail addresses and may include Social Security numbers when a vendor Tax Information Number (TIN) is not available.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

As an IT investment, HCAS is governed by the HHS IT Investment Review Board (ITIRB), as part of the HHS Capital Planning and Investment Control (CPIC) process, as managed by the HHS Office of the Chief Information Officer (OCIO). CPIC is mandated by the Clinger-Cohen Act which requires agencies to use a disciplined process to acquire, use, maintain and dispose of information technology. The OCIO exercises authorities delegated by the Secretary to the Deputy Assistant Secretary for Information Technology, as the CIO for HHS. These authorities derive from the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, the Computer Matching and Privacy Act of 1988, the Computer Security Act of 1987, the Federal Information Security Management Act (FISMA), the National Archives and Records Administration Act of 1984, the Competition in Contracting Act of 1984, the Federal Records Act of 1950, OMB Circulars A–130 and A–11, Government Printing and Binding Regulations issued by the Joint Committee on Printing, and Presidential Decision Directive 63.

In addition to the ITIRB oversight, HCAS falls within the governance of the HHS Office of Grants and Acquisition Policy and Accountability (OGAPA).

PURPOSE(S):

HHS has acquisition offices across 10 Operating/Staff Divisions, which conduct and process thousands of procurement transactions annually. The HHS acquisition community requires a transaction-based, integrated procurement system that is consistent across the entire HHS. Except for the Centers for Disease Control and Prevention (CDC), HHS utilizes the acquisition processing and management functionality of Purchase Request Information System (PRISM), a commercial off-the-shelf (COTS) application from Compusearch Software Systems. Except for CDC and Centers for Medicare and Medicaid Services (CMS), HHS utilizes the requisitioning functionality in Oracle i-Procurement, a package available within Oracle Federal Financials, the software utilized by the Unified Financial Management System

(UFMS), the HHS enterprise financial management system.

The HHS Consolidated Acquisition System delivers a standardized global PRISM for all operational contracting components within HHS (except CDC) that utilize UFMS (referred to as HCAS clients). HHS deployed HCAS to the following seven HCAS client contracting offices: Agency for Healthcare Research and Quality (AHRQ), Assistant Secretary for Preparedness and Response (ASPR), Food and Drug Administration (FDA), Program Support Center (PSC), Health Resources and Services Administration (HRSA), Indian Health Service (IHS) and Substance Abuse and Mental Health Services Administration (SAMHSA). (CMS and National Institutes of Health (NIH), which use other distinct Oracle Federal Financial instances for financial management that are not UFMS, are not considered HCAS clients and are outside the scope of this system.) CDC, while using UFMS, does not use the HCAS PRISM environment but uses their own procurement system Integrated Contracts Expert (ICE). HCAS PRISM was fully implemented across its HHS clients on February 8, 2009.

The enterprise PRISM configuration via HCAS allows HHS to standardize acquisition business processes across the department. A consolidated PRISM facilitates and enables a single solution for integrating acquisition with financial management (one interface between HCAS and UFMS) and other mixed financial management systems.

The HCAS system itself collects information necessary to support a procurement relationship between HHS and the vendor community. There are limited instances where an individual's information in identifiable form (IIF) will be collected in order to facilitate a transaction in HCAS. HCAS collects and maintains IIF for service fellows and sole proprietorships that provide vendor services as individuals.

Acquisition processes supported by HCAS include acquisition planning, solicitation, contract creation and approval, contract award and award closeout. To support these business processes, IIF contained in HCAS may include the following: Vendor and contracting officer names, vendor mailing addresses, phone numbers, vendor financial account information, legal documents, Web URLs, e-mail addresses, vendor education records, and vendor tax ID numbers (TIN) or Social Security numbers. HCAS users will be able to retrieve data records by vendor or contracting officer name, among other identifiers. For example, names of contracting officer who act as buyers for HHS may be used to retrieve request for proposals or other HHS solicitation materials or purchase requests. Users may also use a contracting officer's name to retrieve associated contact information such as business e-mail or phone number when creating a solicitation or contract. Similarly, users may retrieve solicitation and contract materials, such as proposals, progress reports, and contract modifications by vendor name.

Social Security numbers of vendors may be captured within HCAS under certain circumstances where a Tax Identification Number (TIN) is not available. The HCAS system will comply with all provisions of section 7 of the Privacy Act, including compliance with the following paragraph:

Any Federal, State or local government agency which requests an individual to disclose his Social Security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

When vendor SSN information is collected by HCAS, it is required for vendors to obtain the benefit of contracting with HHS. Provision of this information by the vendor is elective and again, is only used when a vendor TIN is not available.

HCAS is integrated with UFMS and information is exchanged in both directions between the two systems. Information retrieved from HCAS may be shared/disclosed within and across the HHS contracting and financial management communities to: (1) Specify the Contracting Officer conducting an HHS solicitation or purchase request; (2) to specify vendor information in contract documentation, including award, modifications, and task progress reports; and (3) to validate and approve payments to HHS vendors. Information on vendors pertaining to specific HHS contract transactions captured in HCAS is not shared or disclosed to agencies outside of HHS. Names of contracting officers who act as buyers for HHS are contained in solicitation materials that are released to the public for competitive procurements.

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

The Privacy Act allows information disclosure 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 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:

(1) To agency contractors or consultants who have been engaged by the agency to assist in the accomplishment of the HCAS/FESM Operations and Maintenance function (O&M) relating to the purposes for this system and who need to have access to the records in order to assist the OGAPA and HCAS/FESM O&M Federal leadership.

(2) To the Department of Justice (DOJ), court or adjudicatory body when the agency or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the HHS OGAPA determines that the records are relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

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

STORAGE:

All records are stored on electronic media.

RETRIEVABILITY:

Identifiers used to retrieve records may include names of contracting officers and vendors. Names of contracting officers who act as buyers for HHS may be used to retrieve RFPs, statements of work, purchase requests, contract awards or contract modifications. Vendor names may be used to retrieve proposals, contract awards, contract modifications, progress reports, financial status reports, invoices, and contract deliverables. In the limited instance that a vendor is a service fellow or a sole proprietorship that provides services to HHS as an individual, HCAS will allow users to use the individual's name to retrieve vendor related procurement records.

SAFEGUARDS:

ADMINISTRATIVE CONTROLS:

The following Administrative Controls have been in place for HCAS:

ACCOUNT MANAGEMENT/USER IDENTIFICATION AND AUTHENTICATION:

Users must have a UFMS account prior to creation of the PRISM account. User's supervisor or another UFMS user submits a request for access on behalf of the prospective user through the User Provisioning Automated (UPA) process. The UPA process is the on-line UFMS user provisioning module. The UPA process is a workflow process that requires supervisor approval, responsibility approval, SOD approval, and security verification of background investigation. Reports can be generated detailing the approvals for user provisioning. Inactive accounts are locked after 60 days of inactivity. The use of temporary and emergency accounts is prohibited.

AUTHENTICATOR MANAGEMENT:

Users are required to change their password upon initial login. If users do not log in and change their passwords within 30 days of account generation, then the account is made inactive. Users are responsible for understanding and complying with all password use requirements including the need for adequate (difficult to decipher) passwords. Users are required to use passwords of a mix of eight (8) alpha, numeric and special characters, with at least one uppercase letter, one lower case letter, and one number. Users are automatically required to change their passwords every 90 days. Users are instructed to keep their passwords confidential and not share them with anyone. Upon notification that a password has been forgotten or compromised, the password is immediately reset to a unique (non-default) password and the user is notified. Upon login, after a password reset, the user is required to change their password within 2 days to prevent the account from being deactivated.

ACCESS ENFORCEMENT:

User access to the application functions are granted through the UPA process based upon the role that has been assigned to the user and approved through the workflow. Privileges assigned to users of the system/application are granted based upon the role that has been assigned to the user. This includes administrative privileges that can be performed within the system.

INFORMATION FLOW ENFORCEMENT—NIH/CIT SECURITY MECHANISMS:

Carbon Copy (CC): The UFMS application resides on hardware located within the National Institutes of Health, Center for Information Technology (NIH/CIT) general support system (GSS). The flow of information within the system and between interconnected systems is controlled by various NIH/CIT network firewalls, and authentication mechanisms HHS–Net Certification and Accreditation (C&A)—The flow of information within the system traverses the HHS–Net network which includes routers, switches, network firewalls, and authentication mechanisms.

LEAST PRIVILEGE:

Privileges assigned to users of the system/application are granted based upon the role that has been assigned to the user.

UNSUCCESSFUL LOGIN ATTEMPTS:

The system contains functionality that prevents user access when the maximum number of unsuccessful login attempts is exceeded.

The HCAS system automatically locks an account until released by an administrator when three (3) unsuccessful login attempts occur.

TECHNICAL CONTROLS:

Access to the system is controlled by HCAS Systems Security Officer, which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

PHYSICAL CONTROLS:

The servers will reside in the NIH CIT Computer Room where policies and procedures are in place to restrict access to the machines.

This system will conform to all applicable Federal laws and regulations and HHS/Office of the Secretary 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; and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal and HHS/Office of the Secretary 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.

RETENTION AND DISPOSAL:

HCAS is governed by the HHS Records Management and Disposition guidelines for the retention and destruction of IIF. The guidelines reference the National Archive and Records Administration Act of 1984 (Pub. L. 98–497, 44 U.S.C. Chapter 21). The HCAS FESM/O&M will retain identifiable information maintained in the HCAS system of records in accordance with the National Archives and Records Administration General Records Schedules and Federal Acquisition Regulation (FAR 4.805).

SYSTEM MANAGER(S) AND ADDRESS:

Director, Information and Systems Management Services (ISMS), U.S. Department of Health and Human Services, Parklawn Building, 5600 Fishers Lane, Rockville, Maryland 20857.

NOTIFICATION PROCEDURE:

Inquiries should be made in writing to the System Owner, Deputy Assistant Secretary, Office of Grants and Acquisition Policy and Accountability, Assistant Secretary for Financial Resources, U.S. Department of Health and Human Services, 200 Independence Avenue, SW., Washington, DC 20201. The individual making the inquiry must show proof of identity before information is released and give name and social security number, purpose of inquiry, and if possible, the document number.

RECORD ACCESS PROCEDURES:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system owner named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulations 45 CFR 5b.7).

RECORD SOURCE CATEGORIES:

Information in HCAS will be collected, in part, from the data transmitted from i-Procurement which includes: Requisition number; date of

request; object class, appropriation code and Central Accounting Number (CAN) of the item requested; HHS requesting organization name; and location, HHS point of contact name and business contact phone number within the requesting organization; a description of the item requested and corresponding quantity and cost required. Other information collected includes; proposal, solicitation, market research, and contract award documentation.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2011–9467 Filed 4–18–11; 8:45 am]

BILLING CODE 4150–24–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Notice of Intent To Award Affordable Care Act Funding to Approved Applications Formerly Received in Response to the Centers for Disease Control and Prevention Funding Opportunity IP11–010, "Enhanced Surveillance for New Vaccine Preventable Disease"

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

ACTION: Notice.

SUMMARY: This notice provides public announcement of CDC's intent to fund Approved cooperative agreement applications previously received and competed in response to CDC Funding Opportunity, CDC–RFA–IP11–010, "*Enhanced Surveillance for New Vaccine Preventable Disease*." It is the intent of CDC to fund the applications with Patient Protection Affordable Care Act (ACA), Section 4002, appropriations.

CFDA Number 93.533 is the ACA-specific CFDA number for this initiative.

Award Information

Approximate Current Fiscal Year Funding: $2,750,000.

Approximate Number of Awards: 3–5.

Approximate Average Award: $500,000.

Fiscal Year Funds: Patient Protection and Affordable Health Care Act of 2011.

Anticipated Award Date: 31 May 2011.

Budget Period: 12 months.

Project Period: 5 years.

Application Selection Process: CDC will apply the same selection methodology published in the FOA, CDC–RFA–IP11–010.

The following will be considered in making funding decisions:

- Scientific and technical merit of the proposed project as determined by scientific peer review.
- Availability of funds.
- Relevance of the proposed project to program priorities.
- Funding decision criteria will include a priority score, programmatic importance/value relative to program priorities, past and current surveillance performance and capabilities, research portfolio, geographic locations, and study population consideration (ethnicity, etc.)
- Preference may be given to a medical institution catchment area having a total population of greater than 500,000 persons.
- Applicants must have a letter of support with a research laboratory for rotavirus analyses or they will not be funded.

CDC will add the following Authority to that which is reflected in the published Funding Opportunity:

—Section 4002 of the Patient Protection and Affordable Care Act (Public Law 111–148.)

DATES: The effective date for this action is April 19, 2011 and remains in effect until the expiration of the project period of the ACA funded applications..

FOR FURTHER INFORMATION CONTACT: Elmira Benson, Deputy Director, Centers for Disease Control and Prevention, 2920 Brandywine Road, Atlanta, GA 30341, telephone (770) 488–2802, e-mail *Elmira.Benson@cdc.gov.*

SUPPLEMENTARY INFORMATION: On March 23, 2010, the President signed into law the Patient Protection and Affordable Care Act (ACA). ACA is designed to improve and expand the scope of health care coverage for Americans. Cost savings through disease prevention is an important element of this legislation and ACA has established a Prevention and Public Health Fund (PPHF) for this purpose. Specifically, the legislation states in Section 4002 that the PPHF is to "provide for expanded and sustained national investment in prevention and public health programs to improve health and help restrain the rate of growth in private and public sector health care costs. ACA and the Prevention and Public Health Fund make improving public health a priority with investments to improve public health.

The PPHF states that the Secretary shall transfer amounts in the Fund to accounts within the Department of Health and Human Services to increase funding, over the fiscal year 2008 level, for programs authorized by the Public Health Services Act, for prevention, wellness and public health activities including prevention research and health screenings, such as the Community Transformation Grant Program, the Education and Outreach Campaign for Preventative Benefits, and Immunization Programs.

ACA legislation affords an important opportunity to advance public health across the lifespan and to reduce health disparities by supporting an intensive community approach to chronic disease prevention and control.

Therefore, the FOA program activities CDC proposes to fund with ACA appropriations are authorized by the amendment to the Public Health Services Act which authorized the Prevention and Wellness Program.

Dated: April 8, 2011.

John Murphy,

Business Operation Manager, Centers for Disease Control and Prevention.

[FR Doc. 2011–9417 Filed 4–18–11; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[60-Day–11–11EF]

Proposed Data Collections Submitted for Public Comment and Recommendations

In compliance with the requirement of Section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995 for opportunity for public comment on proposed data collection projects, the Centers for Disease Control and Prevention (CDC) will publish periodic summaries of proposed projects. To request more information on the proposed projects or to obtain a copy of the data collection plans and instruments, call 404–639–5960 and send comments to Daniel Holcomb, CDC Reports Clearance Officer, 1600 Clifton Road, MS–D74, Atlanta, GA 30333 or send an e-mail to *omb@cdc.gov.*

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the