**Supporting Statement for CMS Enterprise Identity Management System**

## A. Justification

In its administration of the Medicare Modernization Act, the Centers for Medicare & Medicaid Services (CMS) is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules. As a covered entity, CMS is required to verify at a high level of assurance all persons requesting access to CMS' computer systems. Under the Health Care Reform Bill HR 3590, known as the "Patient Protection and Affordable Care Act" (PPACA), there are many provisions that require the secure ingress and egress of data from CMS. CMS has created the horizontal enterprise services programs to address those provisions. One of these programs is the Enterprise Identity Management (EIDM) system. Identity management is an important part of protecting the security of CMS' data by ensuring that individuals are who they claim to be. The EIDM solution will provide an enterprise-wide solution that will also support CMS' senior management goal to improve the Provider and Health Information Exchange experience by providing an enterprise-wide set of credentials and single sign-on capability for multiple CMS applications.

The EIDM Shared Service will:

- Allow the assignment of a single electronic credential to an individual to enable their access to CMS systems while meeting the appropriate federal security requirements;
- Strengthen CMS security and reduce vulnerability to fraud through more robust identity proofing and requiring the use of multi-factor authentication before accessing CMS business applications;
- Employ an external third-party service that will verify the individual's claimed identity by examining the information provided by the individual requesting access. (e.g., identity history, credentials, documents, credit history);
- Reduce overall CMS costs by transitioning many of the existing identity management systems into the to the Shared Service;
- Provide the road-map, guidance and technology for individual CMS applications to connect to the EIDM Shared Service, allowing the application to control an individual's access and authorization to the application;
- Accept other federal agency credentials provided to CMS from the Federated Cloud Credential Exchange (FCCX);
- Adapt to dynamic changes in workload via an elastic cloud-based environment;
- Secure access to the CMS Enterprise Portal.

### 1. Need and Legal Basis

HIPAA regulations require covered entities to verify the identity of the person requesting Personal Health Information (PHI) and the person's authority to have access to that information Under the HIPAA Security Rule, covered entities, regardless of their size, are required under Section164.312(a)(2)(i) to "assign a unique name and/or number for identifying and tracking user identity." A 'user' is defined in Section 164.304 as a "person or entity with authorized access". Accordingly, the

Security Rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that receives, maintains or transmits electronic PHI, so that system access and activity can be identified and tracked by user. This pertains to workforce members within health plans, group health plans, small or large provider offices, clearinghouses and beneficiaries.

Federal law requires that CMS take precautions to minimize the security risk to the Federal information system. FIPS PUB 201 – 1 Para 1.2: "Homeland Security Presidential Directive 12 (HSPD 12), signed by the President on August 27, 2004 established the requirements for a common identification standard for identification credentials issued by Federal Departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. HSPD 12 directs the department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common identification credential."

OMB-04-04 updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 and implements section 203 of the E-Government Act, 44 U.S.C. ch. 36. After determining the assurance level appropriate for access to government systems or information "the agency should refer to the National Institute of Standards and Technology (NIST) e-authentication technical guidance to identify and implement the appropriate technical requirements. " NIST SP 800-63-1 is the authoritative document that provides information on the technical controls and approaches that an Agency must use for remote as well as in-person identity proofing requirements from Levels of Assurance (LOA) 1-4. Currently, FICAM does not have a certification process for a stand-alone identity proofing capability; current FICAM certification, via the Trust Framework Adoption Process, applies to a combined identity proofing-credential issuance solution. As such the requirements levied on an Identity Proofing service are based on the foundational requirements that all US Government Agencies must follow in complying with NIST Guidance. OMB-O4-04 requires that data collection must comply with the Privacy Act but also states:

*Most e-authentication processes capture the following information:*

- *Information regarding the individuals/ businesses/governments using the E-Gov service*
- *Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and Personal Identification Numbers)*
- *Transaction information associated with user authentication, including credential validation method*
- *Audit Log/Security information*

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. EIDM will:

- Support all currently approved Federal Identity, Credential, and Access Management (FICAM) Protocol Profiles, as found on IDManagement.gov, for

browser based Simplified Sign-On (SSO) [OpenID 2.0 and SAML 2.0 required; Identity Metasystem Interoperability version 1.0 (IMI 1.0) support is optional]
- Support newly approved FICAM Protocol profiles, as found on IDManagement.gov, within [90 days] of final approval by the ICAMSC
- Be capable of supporting all FICAM Adopted Trust Framework Provider Approved Credential Providers as found on IDManagement.gov
- Be capable of supporting PIV (for Government-to-Government use cases) and Personal Identity Verification Interoperable (PIV-I) Authentication which includes Trust Path Discovery and Trust Path Validation functionality
- Support the FICAM Security Assertion Markup Language version 2.0 (SAML 2.0) Identifier and Protocol Profiles for Backend Attribute Exchange version 2.0 (BAE v2.0) and the associated FICAM SAML 2.0 Metadata Profile for BAE v2.0 if the solution implements a SAML 2.0 Attribute Query/Response mechanism
- Support the following protocols and assertion formats for communication between itself and the relying party Agency application:
    - Protocols: Hypertext Transfer Protocol Secure (HTTPS), SAML 2.0
    - Assertion Formats: SAML 2.0, eXtensible Markup Language (XML), JavaScript Object Notation (JSON)

According to section 1321(c) of the PPACA, the Secretary has the authority to determine whether a State Exchange meets the requisite standards to operate. If the Exchange fails to meet these standards, the Secretary may establish and operate a Federally-facilitated Exchange (FFE) in that State. The FFE will be required to meet the same requirements as the state exchanges, including:

- Exchanges must be able to accept application information through secure electronic interfaces and determine eligibility promptly regardless of which agency received the application (CMS 9989-F Sec 155.345)
- Exchanges must establish privacy and security standards that protect PII data collected and stored by the Exchanges and States, while allowing applicants access to their data. This includes authenticating users, monitoring and mitigating security issues, developing secure interfaces with partners (CMS-9989-F Sec 155.260).
- Exchanges must submit name, date of birth and SSN of each enrollee to SSA to verify eligibility information. If an enrollee attests to being a legal alien or SSA records indicate inconsistencies, Exchanges will submit name, date of birth and any other information submitted to DHS. Information must also be submitted to the Dept. of Treasury to determine if applicant is eligible for a tax credit or cost-sharing reduction. If eligibility information cannot be verified or if inconsistencies exist, procedures are defined. (ACA 1411(a)(5)(c)(2) and CMS 9989-F Sec 155.315).

ARA/HITECH CFR 45 **§** 164.312 Technical Safeguards states:
*A covered entity must, in accordance with § 164.306:*
*(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).*
*(2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.*

In an effort to move from the role of a passive payer to an active purchaser of high-value health care, CMS is developing and implementing a number of value-based purchasing (VBP) initiatives in multiple settings of care. PPACA expands upon these efforts already underway by mandating new VBP programs and pilots as well as other efforts. The systems that will support these initiatives will house protected information, and an enterprise identity management system will be needed. These new programs include:

- Section 3001 establishes a hospital VBP program starting in FY2013. Under this program, a percentage of hospital payment would be tied to hospital performance on quality measures related to common and high-cost conditions, such as cardiac, surgical and pneumonia care. Quality measures included in the program (and in all other quality programs in this title) will be developed and chosen with input from external stakeholders.
- Section 10301 instructs the Secretary to develop a plan to implement a VBP program for payments under the Medicare program for ambulatory surgical centers. It also instructs the Secretary to develop methods for the public disclosure of information on the performance of ambulatory surgical centers.
- Section 10322 establishes guidelines for Quality Reporting for Psychiatric Hospitals. It instructs the Secretary to develop and implement a program for psychiatric hospitals and psychiatric units to submit data on specified quality measures and make that data available to the public.
- Physician resource use reporting has been at the forefront of CMS' VBP initiatives. As required under section 1848(n) of the Social Security Act, as amended by section 131(c) of the Medicare Improvements for Patients and Providers Act of 2008 (MIPPA), CMS established and implemented by January 1, 2009, a Physician Feedback Program using Medicare claims data and other data to provide confidential feedback reports to physicians (and as determined appropriate by the Secretary, to groups of physicians) that measure the resources involved in furnishing care to Medicare beneficiaries. ACA Section 3003 of the ACA greatly expands the Quality and Resource Use Measurement and Reporting (QRUR) reporting.
- Section 3007 requires CMS to develop and implement a budget-neutral payment modifier that provides for differential Medicare physician payments based on a combination of factors that indicate clinical quality and Medicare expenditures (cost) for care delivered to beneficiaries.
- In an effort to enhance Medicare and Medicaid program integrity efforts, Section 6402 requires CMS to include in the Integrated Data Repository (IDR) claims and payment data from the following programs: Medicare (A, B, C, & D), Medicaid, State Children's Health Insurance Program (CHIP), health-related programs administered by the VA and DOD, the SSA, and IHS.

2. Information Use

In order to prove the identity of an individual requesting electronic access to CMS protected information or services, CMS will collect a core set of attributes about that individual. These core attributes will be used to:

1. Provide the identity proofing service sufficient data to establish that the individual's identity is provable to a NIST assurance level;
2. Store the approval information returned by the identity proofing service;
3. Provide CMS with additional data for multi-factor identification (personal questions and answers);
4. Provide the user a single sign-on, federated CMS EIDM ID and Password;
5. Authenticate the user;
6. Authorize the user for application access.

Data collection and verification will occur in phases.

- Phase 1 is the initial form data collected from the end user requesting a CMS IT credential. This information is transmitted to the Remote Identity Proofing (RIDP) vendor and is used to initially identify the user for ID proofing. This information is also used to generate questions to increase/decrease the Level of Assurance score. Phase 1 required attributes include name, current or most recent personal address, primary phone number, email address, full SSN, and date of birth. Alternate phone number and text messaging device are optional attributes.
- Phase 2 is the additional information provided to CMS after the end users request and identity is confirmed by the RIDP vendor and includes transaction reference ID, unique cross-reference ID, date, proofing score, pass/fail code.
- Phase 3 is the successful creation of the end users credential to the CMS identity system(s). Phase 3 attributes include the user ID, user password, NIST assurance level and Authentication (Secret) Questions and Answers. The user will be required to select and answer 4 of 16 questions which EIDM will collect and use for additional security for self-service activities and password resets. For security reasons, CMS will not list actual questions being used but the questions are similar to "What is your maternal grandfather's first name?" The user is required to answer all 4 questions correctly to reset a password and perform other self-service functionality.
- Phase 4 is used to ask the new user to add to their user profile any additional mandatory or optional attributes that enable CMS to better serve the individual user and includes alternate email address. The user will also complete multi-factor criteria if necessary.

3. Use of Information Technology

In October 2011, the Federal CIO stated, "We must focus on maximizing the return on American taxpayers' investment in government IT by driving efficiency throughout the federal enterprise. President Obama is committed to rooting out misspent tax dollars and making government more efficient and effective for the American people… That's why we're launching an initiative aimed at rooting out waste and duplication across the federal IT portfolio. Through this 'Shared First' initiative, we're looking for opportunities to shift to commodity IT, leverage technology, procurement, and best practices across the whole of government, and build on existing investments rather than re-inventing the wheel." In the 30-day sprint analysis, CMS identified 20 potential shared services that could save up to $2.3 billion in development and operational costs over a 5-year period. EIDM was identified as one of the initial shared services to be implemented by CMS.

EIDM will save money and reduce burden by creating one centralized identity and access management system that will be used by the entire agency and:

1. Reduce infrastructure costs;
2. Reduce future development costs;
3. Reduce maintenance costs;
4. Increase security by eliminating existing systems with security findings;
5. Enhance user experience with single sign-on and federated credential support;
6. Reduce cost by becoming a relying party of FICAM certified credential providers.

4. Duplication of Efforts

Similar systems in CMS were examined in an effort to determine whether information already collected could be used for EIDM. These other systems did not identity proof users to NIST standards and did not collect sufficient information that would support identity proofing to NIST standards. Information from other I&A systems will be migrated into EIDM as appropriate.

The collection of this additional information will enable EIDM to create a single identity credential to replace multiple credentials (and user names and passwords), be interoperable with digital identity credentials used by other organizations, including FDA, NIH, DEA, etc., be linked to an actual, vetted individual identity, be legally-binding and non-reputable, and allow for scalability that will reduce the need for duplicate identity and access management efforts to support PPACA.

5. Small Business Impact

There will be minimal impact on small businesses as the length of time to read, complete, and submit the on-line form is expected to be less than fifteen minutes.

6. Non/Less Frequent Collection

The data will be collected one time during the initial identity proofing. If this information is not collected, EIDM will be unable to identity proof individuals to NIST standards and not realize the cost and burden reductions, not qualify for federation, and not meet federally mandated security requirements.

7. Special Circumstances

No special circumstances have been identified.

8. Federal Register / Outside Consultation

The 60-day Federal Register notice for this information collection request published on November 26, 2012.

CMS has consulted with SSA, VA, and IRS on their experiences with data collection for identity proofing users. CMS also used data from 2 state (MA and AL) health insurance exchange pilot identity proofing programs. Plus Experian has conducted demographics analysis to determine reliability of proofing results based on the information collected. CMS also participates in the Office of the National Coordinator's (ONC) National Strategy for Trusted Identities in Cyberspace (NSTIC) forums and the Federal Cloud Credential Exchange (FCCX) initiative that includes other government agencies such as NIST and DHS.

9. Payments / Gifts to Respondents

There are no payments or gifts to respondents.

10. Confidentiality

EIDM is covered under the System of Records Notice titled Individuals Authorized Access to Centers for Medicare & Medicaid Services Computer Services (IACS) #09-70-0538 Publication Date 11/13/2007.

The information collected will be gathered and used solely by CMS and approved contractor(s) and state health insurance exchanges. Information confidentiality will conform to HIPAA and FISMA requirements. Respondents may also access CMS Terms of Service and CMS Privacy Statement on the Web.

11. Sensitive Questions

There are no questions regarding sexual preference, religion, or medical history.

EIDM will collect the full 9 digit SSN. Per ACA 1411(a)(4)(1), CMS-2349-F, and CMS-9989-F Sec 155.310 (3), the full SSN is required by health insurance exchanges. Additionally, per ACA 1413(a), ACA 1413(b)(1)(B), and ACA 1413(b)(10(A), exchanges "develop a streamlined enrollment process that includes one application form that is developed by HHS or by the State (if it meets the standards) and used by all State health insurance programs. If the Exchange determines that the applicants are not eligible for Exchange programs, the application is automatically routed to Medicaid, CHIP, etc." Collecting the full SSN during identity proofing will eliminate the need to collect some subset of the SSN (e.g. last 4 digits) and then ask the user for the full SSN if they apply for health insurance. Executive Order 9397, as amended by Executive Order 13478, permits Federal agencies to utilize individuals' SSNs when necessary even if CMS doesn't have specific program authority to collect SSNs. The Executive Order (with amended text bolded and struck) is listed below.

***Policy.*** **It is the policy of the United States that Federal agencies should conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use.**

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and
WHEREAS some seventy million persons have heretofore been assigned account numbers pursuant to the Social Security Act; and
WHEREAS a large percentage of Federal employees have already been assigned account numbers pursuant to the Social Security Act; and
WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems:
NOW, THEREFORE, by virtue of the authority vested in me as President of the United States, it is hereby ordered as follows:
1. Hereafter any Federal department, establishment, or agency **may,** whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to **title 20, section 422.103** of the Code of Federal Regulations and pursuant to paragraph 2 of this order.
2. The Social Security-**Administration** shall provide for the assignment of an account number to each person who is required by any Federal agency to have such a number but who has not previously been assigned such number by the **Administration**. The **Administration** may accomplish this purpose by (a) assigning such numbers to individual persons, (b) assigning blocks of numbers to Federal agencies for reassignment to individual persons, or (c) making such other arrangements for the assignment of numbers as it may deem appropriate.
3. The Social Security **Administration** shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an

account or the name and other identifying data pertaining to any account number of any such person.
4. The Social Security **Administration** and each Federal agency shall maintain the confidential character of information relating to individual persons obtained pursuant to the provisions of this order.
5. There shall be transferred to the Social Security **Administration**, from time to time, such amounts as the Director of the **Office of Management and Budget** shall determine to be required for reimbursement by any Federal agency for the services rendered by the **Administration** pursuant to the provisions of this order.
6. This order shall be implemented in accordance with applicable law and subject to the availability of appropriations.
7. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person;
8. This order shall be published in the FEDERAL REGISTER.

To achieve NIST assurance level 3 (AL-3), which is required for access to most CMS systems, financially-based questions must be used. During the identity proofing process, the individual will be asked to answer financially-based multiple choice questions that are generated using the information entered by the user. Per the Fair Credit Reporting Act, the user will see a disclaimer that explains the access of credit report data. The user will need to check the box to continue the process. This type of query does not affect their credit score and no financial data is stored by EIDM.

SSN (and all PII data) is protected as described below:

- Data Collection and In-Transit:
    - All communications will be via Hypertext Transfer Protocol Secure (HTTPS) connection, port 443 and 2048 certificates with 256-bit encryption for the tunnel. Screens will have input masking ability for SSN. Users will have to provide the last 4 digits of their SSN and other attributes to establish identity for Help Desk calls and Help Desk agents will have to login to EIDM with multi-factor authentication (MFA) to access user information. CMS web-service calls made to Experian's Precise ID℠ use/support TLS V1.0 (or SSL V3.1) are in line with FIPS 140-2 compliance using hardware / software solutions (Datapower XG45 with HSM). EIDM data will be sent to LDAPS and JDBC over SSL.
- Data Storage:
    - Experian Precise ID℠ inquiry data is stored in a DB2 mainframe database and is appropriately protected using layers of network, application, physical, and administrative controls rather than encryption (due to the volume of data processed / performance reasons). Experian's compensating controls in lieu of data at rest encryption are accepted by Qualified Security Assessor (QSA) for the Payment Card Industry Data Security Standard (PCI DSS) compliance process. CMS inquiry data resides only on Experian's internal network (DB2 on a mainframe) segregated from other client data, behind three layers of firewalls and network intrusion detection equipment that is monitored constantly by a Global Security Operations Center (GSOC).

Network equipment and servers housing the solution must pass a vulnerability assessment before being put into production and periodic scans/assessments thereafter. Precise ID℠ is part of Experian's Application Certification Program and is housed only in Experian's secure data center. Experian enforces full disk encryption on all workstations and removable media using FIPS 140-2 certified products. Because Experian has redundant data centers, there is no need to back up CMS information. EIDM will store the full SSN in Oracle Identity Manager (OIM) and Oracle Universal Directory (OUD), using FIPS 140-2-compliant encryption algorithm and key management.

- Archive:
  - Experian Precise ID℠ data is kept for a minimum of seven (7) years and is archived to tapes stored onsite at the data center which is Tier Level 4 security facility (Maximum security). These tapes never leave the facility and are accessed using an automated robotic system which enforces user authentication and authorization.
  - CMS will retain archived information pursuant to the Records Management Schedule developed for EIDM. The disposition authority for EIDM Master Files are identified below:
    1. Registration files - Disposition Authority, GRS 24, item 13a1
    2. Authorization files - Disposition Authority, GRS 24, item 13a1
    3. ID Management files - Disposition Authority: GRS 20, Item 1
    4. Access Management files - Disposition Authority: GRS 20, Item 1
- Enterprise Cloud Infrastructure for EIDM:
  - EIDM will run on Terremark's "Infrastructure as a Service" (IaaS) available from two geographically diverse and secure Tier III+ datacenters that provide assured availability of compute resources. The Enterprise Cloud services allow Federal customers to control a resource pool of processing, storage and networking and allow deployment of server capacity on demand.
  - CMS has accredited the General Support System as compliant with the Federal Information Security Management Act of 2002 (FISMA).

12. Burden Estimates

The user community that is expected to request access to the EIDM is estimated to be at a 65,000,000 (6M providers, 40M Exchange participants, and 14M employees, contractors, and beneficiaries) with all of the respondents to reply electronically. The estimated time to read, execute and submit this form is approximately 20 minutes.

1. Initial Access: The total burden is estimated to be 21,666,667 hours over 3 years or 7,222,222 hours per year for 3 years. This is a one-time collection of information for each user.
2. Re-Certification or Information Update: Providers, employees, and contractors will be required to recertify yearly and all users may have periodic updates to their information (e.g. address change). It is estimated that 20% of the users will need to re-certify or update their profile information each year. The burden is estimated to be 4,333,333 hours per year over 3 years.

The total burden for initial access and re-certification and information updates is 26,000,000 hours over 3 years or 8,666,667 hours per year over 3 years.

This burden is necessary to comply with security requirements dictated by FISMA and NIST.

13. Capital Costs

There are no capital costs to the respondents.

14. Cost to Federal Government

The yearly average cost to the Federal Government is estimated at $15.7M for remote identity proofing and multi-factor authentication services and $21.8M for the Enterprise Identity Management core services design, development, hosting, operations and maintenance, software licensing, end user support, and ongoing professional services by the enterprise services development/maintenance contractor. The yearly average cost is based on 5 year (base plus 4 option years) contracts.

15. Changes to Burden

This is a new information collection system.

16. Publication / Tabulation Dates

N/A

17. Expiration Date

This collection does not lend itself to the displaying of an expiration date.

18. Certification Statement

The use of Survey Methodology is not applicable to this collection.

19. Collections of Information Employing Statistical Methods

No statistical methods were employed.