Supporting Statement – Part A

CMS Enterprise Identity Management System

A. Background

In support of the American Recovery and Reinvestment Act (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Patient Protection and Affordable Care Act (PPACA) of 2010, also known as Affordable Care Act (ACA), and the Medicare Access & CHIP Reauthorization Act (MACRA) of 2015, Centers for Medicare & Medicaid Services (CMS) has implemented an Enterprise Identity Management (EIDM) system. EIDM is an identity management system that provides the means for users needing access to CMS applications to identify themselves, apply for and receive credentials in the form of a user identifier (User ID) and password, and apply for and receive approval to access the required application/system(s). EIDM manages the life cycle of user ID's, passwords and the supporting data collected from the user, from issuance to archive. Currently, EIDM supports at least fifty-eight (58) CMS business applications.

EIDM service provides the following functions:

1. Registration Service – This function allows new users to create an account credential in order to obtain a single digital identity that can be used across CMS applications that are integrated with EIDM.
2. Authentication Service – This function confirms the user's identity attributes and access privileges. It is available only to users that have completed the registration process and have a valid credential. The Authentication Service validates that users have a valid credential issued to them by providing something they know (e.g., a password), something they have (e.g., a security token), or a combination of those factors. As part of the authentication process, EIDM invokes Multi-Factor Authentication (MFA) using a 3rd party service currently provided by Symantec, by which EIDM requires (when appropriate) that the user of a CMS Application provide more than one form of credential in order to verify their identity and allow access to the system.
3. Authorization Service – This function provides a user the ability to receive approval to access a CMS business application by requesting a role and going through an approval workflow process before being granted access. It also provides integrated applications an automated capability to have user provided attributes cross-referenced against an authoritative data source during the approval/routing workflow. As part of the authorization process EIDM invokes Remote Identity Proofing (RIDP) using a 3rd party solution currently provided by Experian to ensure authenticity of the claimed identity.
4. Lifecycle Management Service – This function includes self-service management, which allows user information to change over time in a controlled and auditable manner within EIDM. User information can be managed by the user through self-service or by an Authorized Help Desk user (e.g., reset password, update user profile, etc.).

The information collected will be gathered and used solely by CMS, approved contractor(s), and state health insurance exchanges. Information confidentiality will conform to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Federal Information Security Management Act (FISMA) requirements. Respondents may also access CMS's Terms of Service and Privacy Statement on the CMS.gov website.

B. Justification

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. Per 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 the identification of 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 800-63-2 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 through 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.*

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 (Personally Identifiable Information) 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 (Social Security Number) 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.

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 web service 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), REST, SOAP

2. Information Users

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

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

Data collection and verification will occur in phases:

• **Phase 1:** During this phase the initial form data is collected from the end user requesting a CMS digital account credential. Phase 1 required attributes include full legal name, current or most recent personal address, primary phone number, email address, full SSN, user ID/name, password, and date of birth. The user will also be required to select three (3) knowledge based authentication questions and provide a corresponding answer to the questions, which EIDM will collect and use for additional security as part of self-service activities and

password resets. For security reasons, CMS will not list actual questions being used, however, the questions are unique to the user (e.g., "What is your maternal grandfather's first name?"). The user is required to answer all 3 questions correctly in order to reset a password and perform other self-service end user account functionality.

- **Phase 2:** In this phase the user logs into the CMS portal/application website by entering their CMS EIDM credential and password created in Phase 1. The user then proceeds to the CMS business application catalogue to select an application and then to request a role(s) in order to obtain access to that CMS application. Each business application role has a NIST Level of Assurance (LOA) associated with it. As part of the business application access approval workflow, the user may be required to enter additional attributes (e.g., business organization/contact information, contract number, reason for request, etc.).

- **Phase 3:** Once the user has filled in the required application specific information required in Phase 2, the user's core attributes provided in Phase 1 (legal name, address, phone, date of birth) will be transmitted to the Remote Identity Proofing (RIDP) service provider to uniquely identify the user and ensure they are who they claim to be. Based on the LOA associated with business application role being requested, the user will be presented with a list of 4-6 Out-of-Wallet Questions (OOW), provided by the RIDP service provider, to answer. The questions and the answers provided by the user are managed by the RIDP service provider and are not retained by the CMS EIDM system. The RIDP service provider only returns to EIDM the results of the online proofing transaction (i.e., reference ID, a unique cross-reference ID, date, proofing score, and a pass/fail code). Once the end users' identity is confirmed by the RIDP service provider, the user can proceed to Phase 4 to setup additional security for their account.

- **Phase 4:** In this phase, depending on the LOA associated with the business application role, the user may be required (or can voluntarily select) to complete the multi-factor authentication (MFA) registration process. MFA provides an extra layer of security to a user's account, such as a one-time use security code, when logging in with a User ID and Password. The CMS EIDM system will prompt the user to register an MFA device type from the list provided (e.g., phone, computer, email, SMS) and then the user will need to input the Credential ID they receive in order to complete MFA device registration.

3. Use of Information Technology

CMS identified twenty (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 is a suite of web-based services that supports organizational and non-organizational users. The user identification and authentication process requires the electronic submission of responses, and the data collected resides in a protected environment to mitigate or avoid the risk of data leakage in the event of a security breach.

In compliance with the Government Paperwork Elimination Act (GPEA), which requires Federal agencies, by October 21, 2003, "to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically

when practicable" and "specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form," EIDM has mandated that all data collection efforts are conducted electronically 100% of the time. EIDM does not require a signature from respondents for this collection.

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

1. Reduce infrastructure costs;
2. Reduce future development costs;
3. Reduce maintenance costs;
4. Ensure interoperability;
5. Increase security by eliminating existing systems with security findings;
6. Enhance user experience with single sign-on and federated credential support;
7. Reduce cost by becoming a relying party of FICAM certified credential providers;
8. Reduce authentication system development & acquisition costs; and,
9. Facilitate more cost effective solutions for providing credentials to business partners or, through trust relationships, leverage credentials issued by external entities.

4. Duplication of Efforts

Similar systems in CMS were examined in effort to determine whether information already being collected could be used for EIDM. These other systems did not identity proof users to meet National Institute of Standards and Technology (NIST) standards and did not collect sufficient information that would support identity proofing to those standards. Information from other Identity and Access Management (I&AM) 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 (i.e., usernames and passwords). This credential will be:

- Interoperable with digital identity credentials used by other organizations;
- Linked to an actual, vetted individual identity;
- Legally-binding and non-reputable;
- Scalable and will reduce the need for duplicate identity and access management efforts to support current/future legislatively mandated programs.

5. Small Businesses

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

6. Less Frequent Collection

If this information is not collected, EIDM will be unable to register an individual, issue credentials, identity proof, or authorize access to CMS business applications/systems to the 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 target publication date for 60-day Federal Register Notice (FRN) for this information collection request is March 21, 2017 (82FR14514) and the 30-day FRN published on July 26, 2017 (82FR3675) with no comments received.

CMS has consulted with the Social Security Administration (SSA), the Veterans Affairs (VA) administration, and the Internal Revenue Service (IRS) on their experiences with data collection for identity proofing users. CMS also used data from 2 state (Massachusetts and Alabama) health insurance exchange pilot identity proofing programs. Additionally, 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 Connect.gov (formerly the Federal Cloud Credential Exchange) 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). Information confidentiality will conform to HIPAA and FISMA requirements.

Respondents may also access CMS Terms of Service and CMS Privacy Statement on the CMS.gov website.

11. Sensitive Questions

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

EIDM will collect the full 9-digit SSN. Collecting the full SSN during identity proofing is necessary in order to verify that the *asserted* identity corresponds to a *real* individual and to comply with NIST 800-63 guidance. 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.

Section 1. 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 ~~shall~~ **may,** whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize ~~exclusively~~ the Social Security Act account numbers assigned pursuant to ~~Title 26, section 402.502~~ **title 20, section 422.103** of ~~the 1940 Supplement to~~ the Code of Federal Regulations and pursuant to paragraph 2 of this order.
2. The Social Security ~~Board~~ **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 ~~Board~~ **Administration**. The ~~Board~~ **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 ~~Board~~ **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 ~~Board~~ **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 ~~Board~~ **Administration**, from time to time, such amounts as the Director of the ~~Bureau of the Budget~~ **Office of Management and Budget** shall determine to be required for reimbursement by any Federal agency for the services rendered by the ~~Board~~ **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;
~~6.~~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 IDSM use/support TLS V1.0 or higher 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 Internet Directory (OID), 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 Infrastructure for EIDM:
  - EIDM is hosted at the HP Enterprise Services Data Center, which is a combination of virtual machines and physical servers. The HPE datacenter satisfies all of the essential characteristics of an Infrastructure as a Service (IaaS), including broad network access and resource pooling. The EIDM solution is designed to be a loosely coupled service-based secure system that supports the high level of availability, scalability, and performance with implementation of Oracle Real Application Clusters (RAC) database. High availability for EIDM application components is provided by Weblogic clustering.
  - CMS has accredited the General Support System as compliant with FISMA.

12. Burden Estimates (Hours & Wages)

The average response time is estimated to be 20 minutes, with all respondents to reply electronically. Due to the individual differences of each case—particularly, any online activity that may involve initial end-user account registration, recertification, or profile updates—the range of time for an end-user to complete data entry on the website form(s) may vary between 5 to 25 minutes. Responses should certainly not require over 30 minutes from respondents. It is estimated that 750,000 users per year respond to the information collection requirement. We also estimate that the total burden for end-user account registration to be 300,000 hours

annually (750,000 respondents x 24 min. per response / 60 min.). The time estimate for preparation and completion of the EIDM data entry activities (i.e., end-user account registration, recertification, or profile updates) on the CMS Portal website is based upon the professional judgment of staff members at the Centers for Medicare and Medicaid Services.

We believe that roughly 90% of users who will be responding to the information collection requirements can be categorized as office and administrative support, while the remaining 10% of users are physicians. Based on the most recent Bureau of Labor and Statistics Occupational and Employment Data May 2015 for Category 43-0000 (Office and Administrative Support Occupations), the mean hourly wage for an administrative staff is $18.83, and for Category 29-0000 (Healthcare Practitioners and Technical Occupations), the mean hourly wage for a healthcare practitioner is $40.18. We have added 100% of the mean hourly wage to account for fringe and overhead benefits, which calculates to $80.36 ($40.18 + $40.18) for healthcare practitioners and $37.66 ($18.83 + $18.83) for administrative staff. The total weighted average is $41.93 ($80.36. x .10 + 37.66 x .90). We estimate the total annual cost to be $12,579,000 (300,000 hours x $41.93/ hour).

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 $12M for RIDP and MFA services and $20M for the Enterprise Identity Management core services design, development, 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

As of March 1, 2015, the Scalable Login System (SLS)—a separate CMS identity management system—has the responsibility of creating and managing the issuance of credentials for Marketplace consumers, who were migrated from EIDM to SLS, using Healthcare.gov. While the SLS is not explicitly referenced by name in the OMB approved information collection request approved under 0938-1191, the ICR does contain all of the burden associated with individuals applying for coverage in the Marketplace. Included in that burden estimate is the time associated with applying via electronic media and identity management processes. We will work to clearly identify SLS in the next submission of 0938-1191. EIDM services will continue to support identity proofing of Marketplace consumers and business support applications. Due to this change, the overall number of consumer accounts managed by EIDM decreased substantially and, as a result, new burden estimates were made. Additionally, the overall volume decreased (even though remote identity proofing is part of the EIDM suite of services and currently used by SLS), due to EIDM's registration page(s) not collecting information from consumers. The user community that is expected to request access to EIDM is estimated at 750,000, consisting primarily of health care professionals (i.e.,

providers, suppliers, and representatives, insurance agents and brokers, CMS contractors, and CMS employees) with all respondents replying electronically. This change is in contrast to the estimated 26 million consumer accounts (whom the vast majority were Marketplace consumers) described in the prior PRA submission in 2013. Currently, we estimate the total burden for end-user account registration in EIDM to be 300,000 hours annually (750,000 respondents x 24 min. per response / 60 min.).

16. Publication/Tabulation Dates

    Not Applicable (N/A)

17. Expiration Date

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

18. Certification Statement

    No statistical methods were employed.