

## **Supporting Statement for Individuals Authorized**

### **Access to the CMS Computer Services**

#### **A. Background**

The Centers for Medicare and Medicaid Services (CMS) is requesting the Office of Management and Budget (OMB) approval of the Individuals Authorized to Customer Service Application for Access to CMS Computer Systems. CMS has planned to provide a centralized user provisioning and administration service that supports the creation, deletion, and lifecycle management of enterprise identities. This service creates accounts, supports Role Based Access Control (RBAC), the form flow approval process and enterprise identity audit and recertification, and provides business application integration points. An application integration point allows business application owners to use the form flow process of the user provisioning service to approve or deny requests for access to business applications.

The primary purpose of this system is to implement a unified framework for managing user information and access rights, for those individuals who apply for and are granted access across multiple CMS systems and business contexts. Information in this system will also be used to: (1) support regulatory and policy functions performed within the Agency or by a contractor or consultant; (2) support constituent requests made to a Congressional representative; and (3) to support litigation involving the Agency related to this system. We have provided background information about the proposed system in the "Supplementary Information" section below. Although the Privacy Act requires only that the "routine use" portion of the system be published for comment, CMS invites comments on all portions of this notice. See "Effective Dates" section for comment period.

#### **B. Justification**

In its administration of the Medicare Modernization Act, 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.

IACS provides identification and authentication (I&A) of users gaining access to the CMS systems.

##### **1. Need and Legal Basis**

HIPAA regulations require covered entities to verify the identity of the person requesting 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 Section 164.312(a)(2)(i) to "{a}sign 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."

##### **2. Information Users**

The Application for Access to CMS Computer Systems electronic form is used by CMS to capture certain information whereby a person voluntarily discloses name, social security number, email address, office telephone number, company name, company telephone number, address, city, state and zip code which is reviewed and authorized prior to the access being granted.

##### **3. Use of Information Technology**

CMS has planned to provide a centralized user provisioning and administration service that supports the creation, deletion, and lifecycle management of enterprise identities. This service creates accounts, supports Role Based

Access Control (RBAC), the form flow approval process and enterprise identity audit and recertification, and provides business application integration points. An application integration point allows business application owners to use the form flow process of the user provisioning service to approve or deny requests for access to business applications.

CMS has provided an application that will streamline our information technology environment so that existing and new applications can work more effectively by sharing information, and so that CMS can be more responsive to the demands of changing business needs and emerging technology. CMS plans to make our data more readily accessible to our beneficiaries, partners, and stakeholders in a secure, efficient, and carefully planned manner.

Registering and provisioning users for the IACS application is fundamental to the design and implementation of business applications and application planned for the CMS target enterprise architecture. Centralizing this service, while allowing for distributed administration, not only standardizes the process for account administration for all applications, but also improves security because Identification and Authorization and user roles are stored in a single location for all users.

The IACS framework consists of two major components: and identity management service and a set of authentication or access management services. These two components will enable a single identity to be used throughout CMS and will ensure that users authenticate to applications using a level of assurance equal to the sensitivity of the application and/or data. As CMS moves into the web-enabled application arena for mission critical applications, the need to securely manage this environment is a major concern. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements, e-Authentication guidance and the Personal Identity Verification initiative make the need for a security services framework even more important.

When an account/identity is created, a unique identifier will be generated to universally associate a user with CMS. There is 100% electronic usage which reduces the burden placed upon users. The provisioning service uses a seven-character algorithm to generate user IDs that are unique across the CMS enterprise. The provisioning service will also provide a mechanism to assign roles that will be maintained in the central data store. An application integration point will be established to allow business application owners to use the user provisioning service to approve or deny requests for access to business applications.

Initial users of IACS will be primarily CMS business partners such as health care plans and customer inquiry service personnel who answer queries to 1-800-MEDICARE. Three entities are key in providing this support: The Customer Support for Medicare Modernization Support, the CMS IT CITIC Service Desk and the Centers for Beneficiary Choices. Future users will consist of but are not limited to Plans and Providers, Providers Hospitals, Group Practitioners, Physicians and Beneficiaries.

This form is new and does not duplicate other collection efforts and does accept an electronic signature.

4. Duplication of Efforts

There is not a duplication of efforts in utilizing the electronic form. Previously only CMS employees and contractors had access. Through IACS, plans, providers and beneficiaries will have access.

5. Small Businesses

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

6. Less Frequent Collection

This information will be collected one time for users wishing to access CMS systems.

7. Special Circumstances

Responders must complete the Application for Access to CMS Computer Systems form and obtain authorization prior to gaining access to any system.

8. Federal Register / Outside Consultation

The 60-day Federal Register notice for this information collection request published on June 15, 2007.

9. Payments / Gifts to Respondents

There are no payments or gifts to respondents.

10. Confidentiality

The information collected will be gathered and used solely by CMS and approved contractor(s). The data will not be shared with any outside organizations.

11. Sensitive Questions

There are no sensitive questions on the Application for Access to CMS Computer Systems form.

12. Burden Estimates

The user community that is expected to request access to the IACS is estimated to be at a 4,000,000 with all of the respondents to reply electronically. The estimated time to read, execute, and submit this form is approximately 10 minutes and the total burden is estimated to be 668,000 hours (approximately 670,000 hours).

13. Capital Costs

There are no capital costs to the respondents.

14. Cost to Federal Government

The yearly cost to the Federal Government is estimated at \$2,125,000. This is to maintain the hardware (\$250,000), the software (\$625,000), end user administration (\$750,000) and ongoing professional services by the software developer (\$500,000).

15. Changes to Burden

The original estimates of 60 million respondents and 15 million burden hours reflected the total number of expected users in the system. These users would consist of Medicare and Medicaid service providers and beneficiaries. A provider in this case is defined as the individual practioners and large organizations such as hospitals that may have multiple users.

During calendar year, CMS expects approximately 4 million users to request access to CMS systems. This number is derived from 400,000 provider organizations and 1.5 million individual practioners. **The time to read, execute and submit the form has been reduced based on observation of the system over the past two years.** The new time is approximately 10 minutes. Therefore the total burden is 668,000 hours (approximately 670,000 hours).

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

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

C. Collections of Information Employing Statistical Methods

No statistical methods were employed.