AUTOMATED INSTALLATION ENTRY (AIE) SYSTEM
ICR REQUEST

14-Nov-13

SUPPORTING STATEMENT – PART A

A. JUSTIFICATION

1. Need for the Information Collection

In accordance with AR 190-13, the Product Manager, Force Protection Systems (PdM-FPS), under the supervision of Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD), has the responsibility for researching, developing, testing, procuring, fielding, and sustaining U.S. Army physical security material solutions.

In April 2004, HQDA assigned the Office of the Provost Marshal General (OPMG) as the lead for establishing Army standards and requirements for the installation entry security protocols in accordance with Homeland Security Presidential Directive (HSPD)-12 which mandates the standards for credentials used for entering Federal facilities. In November 2007, OPMG approved the Automated Installation Entry (AIE) standards and specifications. In August 2008, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology designated the JPEO-CBD as the materiel developer for the Army AIE Program.

In order to comply with Section 1096 of Public Law 110-181, "Standards Required for Entry to Military Installations in the United States - Access Standards for Visitors"; Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; and DoD 5200.08-R, Physical Security Program, appropriate screening requires collection and utilization of personally identifiable information (PII) to conduct identity proofing and vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of local access credentials.

2. Use of the Information

The information collected will be used to verify the identity of an individual, and as a result of proper identification, the fitness of an individual will be determined by U.S. Government (USG) personnel analysis and assessment of information obtained through USG authoritative data sources. The information requested is collected in electronic format via access control technology.

3. Use of Information Technology

Identification screening and access control technology will process information collected on individuals requesting and/or requiring access to installations, and issuance of local access credentials. The information collection methodology involves the employment of technological collection of data through electronic response submission by respondents. In accordance with (IAW) DTM 09-012, the Army has procured AIE, an electronic physical access control system (PACS), that provides the capability to rapidly and electronically authenticate credentials and individual's authorization to enter an installation.

4. Non-duplication

IAW DoD 5200.08-R, installation access control programs should establish a system f or positive identification of personnel and equipment authorized to enter and exit the installation. Also, IAW DTM 09-012, individuals requesting access will provide a valid and original form of identification for the purpose of proofing identity for enrollment into a PACS or issuance of a visitor pass; however, the PACS must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information.

As a result of initial enrollment into a PACS, collection for the purpose of installation access is a one-time event where collection data is stored in an adequately secured database and securely shared with other PACS to alleviated duplication of collection and reduce the burden of effort.

5. Burden on Small Business

In the event small entities require installation access, additional capabilities are provided with system to minimize the burden imposed by this collection via an online pre-registration application.

The web pre-registration application provides an internet platform providing web-based pre-registration capabilities for each installation. It stores data for all users requesting access to the facility and provides the data as pre-populated fields to the enrollment station at the Visitor Control Center (VCC) upon request. By entering the appropriate data online, users can initiate registration before arriving onsite. This mitigates delays in processing information of newly arrived applicants and visitors.

6. Less Frequent Collection

Because positive identification is required for installation access, at a minimum, collection would have to occur for initial enrollment into a PACS. Collection less frequent of the initial collection requested for PACS enrollment would not meet the requirements for identity proofing and vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of local access credentials.

7. Paperwork Reduction Act Guidelines

This collection does not require any special circumstances that require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d) (2).

8. Consultation and Public Comments

In compliance with Section 3506(c) (2) (A) of the *Paperwork Reduction Act of 1995,* the Department of the Army announced a proposed public information collection and sought public comment via a 60-Day Federal Register Notice [FR Doc. 2013-22248 Filed 09/12/2013 at 8:45 am] and published in the Federal Register /Vol. 78, No. 178 / Friday, September 13, 2013 /Notices; [Docket ID: USA–2013–0031]. Upon expiration of the 60-day duration, the public did not present any comments regarding the practical utility of the information collected for system employment as prescribed in the AIE operational requirements.

9. Gifts or Payment

No payments or gifts to respondents are associated with this collection. Upon proper identity proofing and vetting, an individual's fitness will be determined for authorized installation access and issuance of local access credential.

10. Confidentiality

The AIE system is a fully, DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) accredited system which is certified at the Mission Assurance Category II, Confidentiality-Sensitive level. The system also achieved an Army Certificate of Networthiness as prescribed by AR 25-2, Army Information Assurance.

AIE components operate at a System High Security Mode and employs IA-enabled components/ security features to comply with appropriate security configuration guidelines. The secured enclave provides a layered defense against categories of non-authorized or malicious penetrations and prevents compromise or disclosure of sensitive information.

Respondent information is collected via electronic submission. Once information enters the system, a variety of security protocols and services (e.g. VPNs, AES-256 data encryption data-at-rest/data-in-transit, IPSec-based protocols, etc.) are employed to protect sensitive data. Respondents are informed that AIE is a DoD-accredited system and have to give consent to final submission of their information to the PACS for the purpose of identify proofing and vetting for the purpose of installation access.

The collection for the AIE system has been authorized by an approved SORN, SORN ID/Title: A0190-13 OPMG Security/Access Badges (July 25, 2008, 73 FR 43430). Also, the Army CIO/G-6 has completed a PIA on the AIE system on 30 Mar 2010. Copies of both documents are included with the information collection package.

11. Sensitive Questions

Sensitive information is required of the respondent in order to conduct identity proofing and vetting in order to determine an individual's fitness for requiring installation access. DTM 09-012 requires the following:

Non-Federal Government and non-DoD-issued card holders who are provided unescorted access require identity proofing and vetting to determine fitness and eligibility for access. Installation government representatives shall query the following government authoritative data sources to vet the claimed identity and to determine fitness, using biographical information including, but not limited to, the person's name date of birth, and social security number:

- The National Crime Information Center (NCIC) database.
- The Terrorist Screening Database.
- Other sources as determined by the DoD Component or the local commander and/or director.

Information requested of the respondents do not violate the Privacy Act as implemented by DoD 5400.11-R. Respondents are informed the data collected is used to installation commanders and law enforcement officials with means by which information may be accurately identified to determine if applicant meets authorized access requirements. The collection of data is voluntary; however, failure to provide the requested information will result in the denial of an authorized access pass (or equivalent) and denial of entry to Army installations.

12. Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden

The information system used for collection creates a database record for each respondent recorded and keeps an account of all records established in the database on a one-to-one relationship. Each system can generate a report of the total number of respondents registered into its database. All systems' respondent registration numbers were added (29,385) and multiplied by the 3 minute/per person processing registration time to add collected data to the database. Consequently, the result of this multiplication was divided by 60 minutes and resulted in approximately 1469 hours of respondent burden annually.

b. Labor Cost of Respondent Burden

The annualized labor cost to the respondents regarding the burden hours imposed by the collection were calculated by generating a portrayal of the average hourly wage of all respondents and multiplying it by 1469 hours. The result of this computation identified the annualized labor cost to respondents to be $42,814, as illustrated in the following chart:

Respondents	**Cost Burden**
Civilian Hourly Salary	$ 21.63
Visitor Hourly Salary	$ 21.63
Contractor Hourly Salary	$ 41.15
Retiree Hourly Salary	$ 12.28

Average Hourly Salary	$ 29.14
Total Respondent Hours	x 1469
Total Labor Cost	$42,814

13. Respondent Costs Other Than Burden Hour Costs

There are no other annualized costs to the respondents as a result of this collection.

a. Total capital and start-up costs annualized over the expected useful life of the items.

Non-applicable.

b. Total operation and maintenance costs.

Non-applicable.

14. Cost to the Federal Government

The annual operations and maintenance (O&M) expense to the Federal Government for the collection of this information will vary year-to-year as the number of sites with AIE increase. Identification screening and access control technology will process information collected (locally) on individuals requesting and/or requiring access to installations, and issuance of local access credentials by querying the following government authoritative data sources (which have already collected the information) to vet the claimed identity and to determine fitness, using biographical information. The average projected annual O&M cost to sustain AIE is estimated at $165,463.

15. Reason for Change in Burden

This is a new collection in use without an OMB control number; therefore, the reason for change in burden would be determined as a "Program Change".

16. Publications of Results

The results of this collection will not be published for statistical use, outline plans for tabulation, statistical analyses, or publication.

17. Non-Display of OMB Expiration Date

Non-applicable.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

Non-applicable.