SUPPORTING STATEMENT - PART A

Automated Installation Entry (AIE) System – OMB Control Number 0702-0125

Summary of Changes from Previously Approved Collection

- Burden increased due to updated estimates
- New collection instrument

1. Need for the Information Collection

In accordance with Army Regulation (AR) 190-13, the Product Manager, Force Protection Systems (PM FPS), under the supervision of Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEW&S), has the responsibility for researching, developing, testing, procuring, fielding, and sustaining U.S. Army physical security material solutions.

In April 2004, Headquarters, Department of the Army (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. On 31 Mar 2016, PM FPS organizationally transitioned from JPEO-CBD to PEO IEW&S. PEO IEW&S is now the Milestone Decision Authority (MDA) for the AIE Program.

In order to comply with Section 1069 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 requested is collected in electronic format via access control technology provided by the AIE System from all individuals requesting access to Army Installations including active duty military, dependents, retirees, Government civilians and contractors and visitors. The information collected is used to verify the identity of an individual, and as a result of proper identification, the fitness of an individual is determined

by U.S. Government (USG) personnel analysis and assessment of information obtained through USG authoritative data sources.

Individuals requesting access to Army Installations will provide a valid and original form of identification for the purpose of proofing identity for enrollment into a Physical Access Control System (PACS) or issuance of a visitor pass. Sensitive PII is required of the respondent in order to conduct identity proofing and vetting for determination of an individual's fitness for requiring installation access. This information is collected electronically by the AIE System from an individual's form of identification and through input by the respondent using an electronic device that interfaces with the AIE System.

All individuals desiring access to Army Installations must report to a Visitor Control Center (VCC) where this information is collected by the AIE Registration System. The System processes the personal information by authenticating against authoritative data sources to include the Defense Enrollment Eligibility Reporting System (DEERS), National Crime Information Center (NCIC) Interstate Identification Index (III), FBI Wants and Warrants file, State Department of Motor Vehicles and State crime databases. Signs located at each Installation Gate provide visitors with appropriate instructions for requesting access. No other notices or invitations are issued to respondents.

Although the AIE System must collect SSNs, the System does not use the SSN locally for processing or maintaining personal information records. Instead, the AIE System relies on an Electronic Data Interchange Personal Identifier (EDIPI), also known as the DoD Identification Number, which is a unique ten (10) digit number assigned to a person's record. When the authoritative data sources with which the AIE System interfaces for vetting and credential authentication eliminate the use of SSNs as primary identifiers, AIE will no longer collect SSNs.

Successful processing and authentication of respondents' personal identity information by the AIE System results in access to Installations being granted and local identification badges being issued as appropriate. Protection of DoD Installations and personnel is inherent to commands throughout the Joint Services. Successful identity proofing and vetting of respondents ensures the Army's ability to better protect its Soldiers, Civilians and Installations across the U.S.

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 100% of 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 an individual's authorization to enter an installation.

4. Non-duplication

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

5. Burden on Small Businesses

This information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

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 frequently of the initial collection requested for PACS enrollment would not meet the requirements in Section 1069 of Public Law 110-181 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 of information does not 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

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice (FRN) for the collection published on Thursday, September 20, 2018. The 60-Day FRN citation is 83 FRN 47609.

No comments were received during the 60-Day Comment Period.

A 30-Day Federal Register Notice for the collection published on Wednesday, February 5, 2020. The 30-Day FRN citation is 85 FRN 6534.

Part B: CONSULTATION

Consultation usually occurs every three years with the authoritative sources upon review of the Memorandum of Agreements (MOU) in place with these agencies, which occurs upon the expiration of the AIE System's current Authorization to Operate (ATO). The pursuit of a newly granted ATO will necessitate revisiting any existing MOUs with an authoritative source.

Because the AIE System performs information collection in compliance with Section 1069 of Public Law 110-181, as promulgated by DTM 09-012 and DoD 5200.08-R, it is not obligated to consult with general visitor population respondents regarding availability of requested information, frequency of collection, or clarity of instructions.

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

The AIE system established Risk Management Framework (RMF) for Department of Defense (DoD) Information Technology (IT) requirements and the National Institute of Standards Technology Special Publication (NIST SP) 800-53 Security Control objectives and assessment procedures.

AIE components operate at a System High Security Mode and employ 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, Transparent Data Encryption (TSE), Transport Layer Security (TLS) AES-256 data encryption data-at-rest, IPSec-based protocols, etc.) are employed to protect sensitive data. Respondents are informed that AIE is a DoD-accredited system and must 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. As required by Title 5 U.S.C. 552a (e) (3), a Privacy Act Statement addressing the voluntary provision of PII is displayed at all AIE registration locations.

Collection for the AIE system has been authorized by an approved SORN, SORN ID/Title: A0190-13 OPMG Security/Access Badges (July 11, 2014, 79 FR 40082). Also, the Army CIO/G-6 has completed a PIA for the AIE system on 23 Oct 2018. Copies of both documents are included with the information collection package and can also be accessed at the links below:

http://ciog6.army.mil/Portals/1/PIA/2015/AIE.pdf

http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569989/a0190-13-opmg/

Respondent information collected during installation access approval processing is maintained for three months after turn-in of respondent's badge or card and then destroyed.

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 and other sources as determined by the DoD Component or the local commander and/or director.

Information requested of the respondents does not violate the Privacy Act as implemented by DoD 5400.11-R. Respondents are informed the data collected is used by Installation Commanders and law enforcement officials with means by which the information may be accurately identified to determine if an 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 onto Army installations. Collection of a respondent's full Social Security Number (SSN) is required in order to conduct identity proofing and vetting for processing of installation access approval. An SSN Justification Memo is included as part of this package.

12. Respondent Burden and its Labor Costs

Part A: ESTIMATION OF RESPONDENT BURDEN

1) Collection Instrument
   [AIE Registration]
   a) Number of Respondents: 3,122,116
   b) Number of Responses Per Respondent: 1
   c) Number of Total Annual Responses: 3,122,116
   d) Response Time: 2 Minutes
   e) Respondent Burden Hours: 104,071 hours

2) Total Submission Burden
   a) Total Number of Respondents: 3,122,116
   b) Total Number of Annual Responses: 3,122,116
   c) Total Respondent Burden Hours: 104,071 hours

Part B: LABOR COST OF RESPONDENT BURDEN

1) Collection Instrument
   [AIE Registration]
   a) Number of Total Annual Responses: 3,122,116
   b) Response Time: 2 mins
   c) Respondent Hourly Wage: $44.36

d) Labor Burden per Response: $1.33
e) Total Labor Burden: $4,152,414.00

2) Overall Labor Burden
   a) Total Number of Annual Responses: 3,122,116
   b) Total Labor Burden: $4,152,414.00

The Respondent hourly wage was determined by using the [Department of Labor Wage Website] ([http://www.dol.gov/dol/topic/wages/index.htm])

13. Respondent Costs Other Than Burden Hour Costs

There are no annualized costs to respondents other than the labor burden costs addressed in Section 12 of this document to complete this collection.

14. Cost to the Federal Government

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument(s)
   [AIE Registration]
   a) Number of Total Annual Responses: 3,122,116
   b) Processing Time per Response: 2 Minutes
   c) Hourly Wage of Worker(s) Processing Responses : $15.94
   d) Cost to Process Each Response: $0.48
   e) Total Cost to Process Responses: $1,492,996

2) Overall Labor Burden to the Federal Government
   a) Total Number of Annual Responses: 3,122,116
   b) Total Labor Burden: $1,492,996

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Cost Categories
   a) Equipment: $770,000
   b) Printing: $122,400
   c) Postage: $0
   d) Software Purchases: $0
   e) Licensing Costs: $1,214,338
   f) Other: $4,500,000

2) Total Operational and Maintenance Cost: $6,606,738

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: $1,492,996

2) Total Operational and Maintenance Costs: $6,606,738

3) Total Cost to the Federal Government: $8,099,734

15. Reasons for Change in Burden

Additional AIE sites and systems have come online since 2015, which increases the total number of annual respondents and the annual hours of respondent burden; therefore, the reason for change in burden would be determined as an "Adjustment."

16. Publication of Results

The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

We are not seeking approval to omit the display of the expiration date of the OMB approval on the collection instrument.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

We are not requesting any exemptions to the provisions stated in 5 CFR 1320.9.