SUPPORTING STATEMENT - PART A

(Defense Biometric Identification System (DBIDS) 0704-0455)

1. Need for the Information Collection

The Department of Defense (DoD) is taking prudent measures to enhance security for physical access to DoD controlled areas. DBIDS is the DoD's largest Physical Access Control system (PACS). Person data is collected from members of the public who are seeking access to DoD controlled areas for the purpose of identification and suitability determination. The following authorities authorize this collection: Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009; DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended; Public Law 110-181, Section 1069, "The National Defense Authorization Act for Fiscal Year 2008," January 28, 2008; and DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program," March 2, 2016.

Individuals responsible for the monitoring of access control points and the design of automated access control systems for DoD installations and facilities must have information with which to identify authorized individuals. The possession of a DoD or other credential, to include an HSPD-12 PIV credential, is not sufficient to warrant entry. Rules surrounding entry to secured access areas, including days and times, and force protection conditions, are required to dictate when an individual may enter an installation. DBIDS was developed for the collection and maintenance of this access authorization information, and for providing it to authorized individuals and systems for decision-making purposes. DBIDS provides the capability to support tiered access control based on force protection condition and access control rules/capabilities across installations and/or regions.

2. Use of the Information

The information collected in DBIDS is used for the validation, verification and, if necessary, authentication of individuals seeking physical access to a DoD installation or base. It may also be used for the detection of fraudulent identification cards, the issuance of alerts for missing or wanted persons, and the record keeping of critical property, such as vehicles and weapons.

The respondents included in this information collection are both DoD affiliated personnel as well as non-DoD affiliated personnel requiring recurring, unescorted or escorted access

to an installation (i.e., vendors, contractors, laborers, and other country nationals). DBIDS collects, maintains, and validates Person/Vehicle/Organization data. Persons providing data are non-CAC eligible government employees, contractors, friends and family of those living on the base, and other persons who, on occasion, need access to a federally controlled area.

Required fields for DBIDS registration include name, Lifetime Personal Identifier (LPID) Type, LPID value, date of birth, photo, fingerprints (or other biometric), as well as other mandatory and optional data elements. If authoritative reach back is available and configured, DBIDS will initiate an interface with the Defense Enrollment Eligibility Reporting System (DEERS) in order to validate the card. If the record is found, the personal information specified above is displayed on the DBIDS screen, along with a photo and fingerprints, when available. The DBIDS Registrar validates the fingerprints from DEERS or captures a new set, retakes the photo, if desired, and selects at least one access area prior to saving the record. The fingerprint requirement may be overridden when fingerprints are not attainable. The system has the ability to capture information about the applicants' property (e.g., vehicles, weapons), if required by an installation commander. Once registered, the DBIDS card is printed and can be presented for access at the base's access control points. Again, only those individuals not authorized a CAC, Teslin card or other approved PIV credential are issued a DBIDS card, or installation pass, using the DBIDS system.

The DBIDS system currently utilizes three types of workstations, each designed to perform specific tasks. Future plans call for the consolidation of all, but Access Control Point functions, on one general DBIDS workstation. The types of workstations are as follows:

- Registration: The Registration workstation enables a Registrar to enter a person's information into the database either by scanning an accepted identification card or by manually typing information into data field boxes. DBIDS cards (installation passes) are issued from the Registration workstation. There is a mobile registration station option available that can provide flexibility in registration location, but this station does not issue DBIDS cards.
- Access Control Point: Access Control Point machines (commonly called gate machines) are located at installation Access Control Points to authenticate persons entering the installation and in some iterations of the DBIDS software, temporary visitor passes can also be issued. For valid DoD-issued credentials, there is also the option to auto-register service members at the gate. There is a mobile gate option available to enable credential checking at rarely used gates or at other areas where a credential check for access is deemed desirable.
- Law Enforcement: Law Enforcement systems allow for complete monitoring of personnel actions and authorities by any law enforcement activity. The system allows the Provost Marshal or Base Security Officer to flag individuals as Barred, Suspended, or Wanted.

On an access event, the DBIDS card or other base access credential is scanned and the entrant's information is displayed on the handheld computer. The displayed information is

reviewed and possibly verified by a biometric attribute. Once the guard is satisfied with the entrant's identity, the guard acknowledges the approved access and allows the entrant to proceed. If a deny recommendation is granted, the proper action is taken by the guard based on the access recommendation. Proper responses to a deny range from turning the individual around to detention of the individual. The scanning of the next entrant's credential will replace the PII on the screen with the next entrant's data, or if no scan occurs in 15 seconds, the handheld screen resets to the main screen.

In order to balance the need to reduce the amount of PII in the system and reduce the burden on the public to provide data, DBIDS removes PII in two ways. If a year passes without any scanning events, DBIDS removes the entrant's PII data from the DBIDS cache. Once the entrant's data is removed from the cache, the entrant has four years to reestablish themselves in the system by either entering a DBIDS-enabled base, updating their information with DBIDS, or be deemed a threat by one or more installations. If none of these events occur, the entrant's data is removed from DBIDS entirely.

Records are maintained in secure, limited access, or monitored areas. Physical entry by unauthorized persons is restricted through the use of locks, passwords, or other administrative procedures. Access to personal information is limited to those individuals who require the records to perform their official assigned duties. All users of the DBIDS application are vetted by their respective commands and are given explicit access to the application as users.

The information is collected and stored in the DBIDS database. Database users are required to log into fixed DBIDS workstations using their ID card and fingerprint; name and password are required for mobile gate and mobile registration stations. These protection measures safeguard the access to DBIDS to authorized users only. Data is protected by the Privacy Act of 1974 and according to the regulations therein and by related DoD instructions and directives.

3. Use of Information Technology

Of the 2,500,000 annual responses, 100% are collected electronically.

DBIDS is a centralized, rules-based access and identity management system that was developed as a force protection program to manage personnel, property, and installation access at DoD installations. It is a networked client/server database system designed to easily verify the access authorization of personnel entering military installations by the use of barcode technology, contact and contactless technology present on PIV compatible credentials, photograph, and fingerprint or other biometric identification. It uses the latest barcode scanning, contact and contactless technologies to verify captured data internally against the DBIDS database and externally against available authoritative sources, such as DEERS. It also is compatible with commercial off-the-shelf software packages.

Additionally, the DBIDS application will be modified to read and interpret data available via the contactless interface of a PIV credential.

DBIDS interfaces with the Identity Matching Engine for Security and Analysis (IMESA). This interface has access to over 60 million active and historical identities. When an applicant is providing data to the DBIDS registration interface, DBIDS sends this information to IMESA. When IMESA has the appropriate data to establish identity, a response is then sent to DBIDS. DBIDS immediately interrupts the data entry process in order to confirm a match. Once the match is confirmed, the routine data collection process ceases and only confirmation of items, such as current primary address and contact information, are validated. A match confirmation can be achieved after entering three pieces of data (Name, DOB, SSN/TIN). If confirmation of identity is achieved, up to 90% of the applicant's data will be automatically attributed to the applicant, thus greatly reducing the burden to the public.

4. Non-duplication

DBIDS takes great care to ensure only one identity exists per registered individual. For persons with an existing DoD credential requesting access, the information is populated electronically and base authorization is then determined. If a person not holding a DoD credential requests access, the person's name, LPID, and date of birth is requested. That information is then searched across the available identity databases. If a match is made and validated, the person's previous information is populated and registration is completed.

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

The majority of DoD areas require annual verification of authorization for access. The record is brought up by a scan of existing credential or pass, and once authorization is confirmed, the DBIDS process is complete. On occasion, some information must be updated to reflect changes such as, but not limited to, name, gender, eye color, or authorization.

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 for the collection published on Monday, February 5, 2018. The 60-Day FRN citation is 83 FRN 5074.

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

Part B: CONSULTATION

No additional consultation apart from soliciting public comments through the 60-Day Federal Register Noticed was conducted for this submission.

9. Gifts or Payment

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

10. Confidentiality

Respondents are asked to read a Privacy Act Statement prior to providing the requested information.

A draft copy of the SORN (DMDC 10 DoD) has been provided with this package for OMB's review.

Draft SORN: 

A draft copy of the PIA, Defense Biometric Identification System (DBIDS) Defense Manpower Data Center (DMDC), has been provided with this package for OMB's review.

Draft PIA: 

Records are deleted three to five (3-5) years after deactivation or confiscation of access credentials.

11. Sensitive Questions

This information collection does not ask the respondent to submit proprietary, trade secret, or confidential information to the Department.

Personal Identifying Information (PII): Respondents are advised that their data are FOR OFFICIAL USE ONLY and will be maintained and used in strict confidence in accordance with Federal law and regulations and that those procedures are in place to protect the confidentiality of the information.

Social Security Number (SSN) or other lifetime federal identification number: This is required for those persons asserting their U.S. citizenship when registering with DBIDS. The SSN or other federally issued number is used to correlate identities with the national criminal databases and was deemed necessary.

Sensitive Questions (i.e. gender, race and ethnicity, and citizenship): Gender is a field that can be (and typically is) captured across all of the DBIDS applications and is used to help ensure that the identity being asserted is the same physical identity of the person making that assertion. The DBIDS database receives updates, matches, and alerts from two major databases: DEERS and the Identity Matching Engine for Security and Analysis (IMESA). DEERS and IMESA maintain valid values for gender of "unknown," so it has been provided as an option – though only rarely used – and removing it would cause data errors in the system. Gender, race and ethnicity are not factors in determination of eligibility. However, per Department of State's list of "State Sponsors of Terrorism," anyone from a country on that list has to be approved for base access by the local base or community commander. The rationale used is that people from countries on this list require extra scrutiny to come to the US, the same goes for access to US bases overseas.

Data collected on race is currently being captured by only one theater using DBIDS, but is only captured for Third Country Nationals (TCNs). It is packaged with a number of other data elements that are then sent to the Biometrics Identity Management Activity (BIMA) for vetting of that person. Once that vetting has been completed, the results are returned from BIMA to DBIDS.

12. Respondent Burden and its Labor Costs

a. Estimation of Respondent Burden

1. **[DBIDS]**
a. Number of Respondents: 2,500,000
b. Number of Responses Per Respondent: 1
c. Number of Total Annual Responses: 2,500,000
d. Response Time: .125
e. Respondent Burden Hours: 312,500 hours

2. **Total Submission Burden** (Summation or average based on collection)
a. Total Number of Respondents*:* 2,500,000
b. Total Number of Annual Responses: 2,500,000
c. Total Respondent Burden Hours: 312,500 hours

b. Labor Cost of Respondent Burden

1. **[DBIDS]**
a. Number of Total Annual Responses: 2,500,000
b. Response Time*:* .125 hr
c. Respondent Hourly Wage: 14.50 (double federal minimum wage)
d. Labor Burden per Response: $1.81
e. Total Labor Burden *(P: A multiplied by B multiplied by C)*: $4,531,250

2. **Overall Labor Burden**
a. Total Number of Annual Responses: 2,500,000
b. Total Labor Burden: $4,531,250

The Respondent hourly wage was determined by using the Department of Labor Wage Website (http://www.dol.gov/dol/topic/wages/index.htm) federal minimum wage multiplied by two based on anecdotal evidence. The spectrum of wages is broad and the categories of participant has varying membership. Based on the information provided we believe the above estimate to be correct.

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

a. Labor Cost to the Federal Government

1. **[DBIDS]**
a. Number of Total Annual Responses: 2,500,000
b. Processing Time per Response: .125 hours
c. Hourly Wage of Worker(s) Processing Responses: $14.5
d. Cost to Process Each Response: $1.81
e. Total Cost to Process Responses: $4,531,250

2. **Overall Labor Burden to Federal Government**
a. Total Number of Annual Responses*:* 2,500,000
b. Total Labor Burden*:* $4,531,250

b. Operational and Maintenance Costs

a. Equipment: $7,000,000
b. Printing: $3,000,000
c. Postage: $0
d. Software Purchases: $8,000,000
e. Licensing Costs: $2,000,000
f. Other: $3,000,000
g. Total: $23,000,000

1. Total Operational and Maintenance Costs: $23,000,000
2. Total Labor Cost to the Federal Government: $4,531,250
3. Total Cost to the Federal Government: $27,531,250

15. Reasons for Change in Burden

This is a reinstatement with change to a previously approved collection for which licensing has expired. The burden has increased since the previous approval due to an increase in the areas in which DBIDS is fielded. As the locations have increased, the number of members of the public requesting access though DBIDS has gone up. It is important to note that although DBIDS has over doubled its areas and population size, the amount of registrations is lower on a percentage basis. This can be attributed to those people having previously been enrolled at another location.

Other than this slight increase in burden, the collection instrument and process are not changing at all from the previous submission.

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.