SUPPORTING STATEMENT

DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS)

A. JUSTIFICATION

1. Need for Information Collection

In the post 9/11 era, the Department of Defense (DoD) is taking all requisite measures to enhance security for physical access to DoD facilities and access to DoD networks. This is being accomplished by applying prudent countermeasures for all potential vulnerabilities focusing on security actions to mitigate heightened threat conditions.

DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” July 2004, establishes policy for the implementation and operation of the PIP Program, to include use of DoD identity credentials and operation of the Defense Biometric Identification System (DBIDS). DBIDS is a fully configurable force protection system and serves as a physical access control and critical property registration system. DBIDS is authorized to issue identity credentials to those individuals needing physical access and not otherwise credentialed under DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," December 5, 1997. These credentials take the form of a DBIDS card which is used as an installation pass only. It is important to note that DBIDS cards are issued only to those individuals who are not eligible for a Common Access Card (CAC) which is the DoD’s PIV-compliant credential, or a Teslin Uniformed Services Identification and Privilege card; these are currently the only cards compatible with the DBIDS software. There are future plans to modify DBIDS to accept other HSPD-12 PIV credentials once they become available for review and testing with the system.

Directive-Type Memorandum (DTM) 08-003, “Next Generation Common Access Card (CAC) Implementation Guidance,” December 1, 2008, updates the requirements for CAC eligibility. Specific populations are automatically eligible for a CAC based on their personnel category within the DoD. Examples include Uniformed Service personnel, DoD civilian employees, and specific categories of personnel assigned overseas in support of the Department. CAC eligibility for other populations, including DoD contractors, non-DoD federal civilians, state employees, and other non-DoD affiliates, is based on the DoD government sponsor’s determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission. To be eligible for a CAC, the access requirement must meet one of the following criteria:

(a) The individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Department on a recurring basis for a period of six months or more (this requirement is applicable to DoD contractors only).

(b) The individual requires both access to a DoD facility and access to DoD networks on site or remotely.

(c) The individual requires remote access to DoD networks that use only the CAC logon for user authentication.

These criteria are consistent with the August 2005 OMB Memorandum M-05-24 that directs credentialing standards generally apply to such categories unless they are short-term employees (less than six months), in which case the agency has discretion based on risk and other factors. Based on these criteria, a DBIDS card for non-DoD contractor personnel (or for DoD contractor personnel for under six months) requiring recurring physical access to an installation meets a need that is not fulfilled by the HSPD-12 PIV credential policy.

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. There are rules surrounding entry to access areas, to include days and times and under which force protection conditions 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 and capabilities across installations and/or regions.

Required fields for DBIDS registration include name, Personal Identifier Type (PID), personal identifier, date of birth, height, weight, eye color, hair color, gender, and card expiration date. For a DoD ID cardholder, registration begins with a scan of the CAC or Teslin ID card. In the CONUS DBIDS software version, this 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 new ones, 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 applicants' property (e.g., vehicles, weapons), if required by an installation commander. Once registered, the DoD ID card is then presented for access at the base's access control points. Again, only those individuals not authorized a CAC or Teslin card are issued a DBIDS card, or installation pass, using the DBIDS system.

2. Use of 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 station. It may also be used for the detection of fraudulent identification cards, the issuance of alerts for missing or wanted persons, and the recording 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 access to an installation (i.e., vendors, contractors, laborers, and other country nationals).

3. Improved Information Technology

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, photograph, and fingerprint biometric identification. It uses the latest barcode scanning 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.

The DBIDS system currently utilizes four 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.

- Registration. The Registration workstation enables a Registrar to enter a person's information into the database either by scanning an 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. 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.

- Visitor Center. The Visitor Center allows for validating authorized personnel, and for sponsors to register escorted and authorized guests onto the installation.

- 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.

4. Efforts to Identify Duplication

No other government agency is responsible for this program. There is no other information collection which duplicates the information collected for DBIDS for the purpose of physical access control at those bases and stations which use DBIDS. Due to the sensitivity and statutory restrictions on recording and disclosure of some law enforcement data, that information is retained in the authoritative law enforcement systems, such as NCIC. Personnel information is redundant in these systems.

Both CAC and Teslin cards are produced through the Real Time Automated Personnel and Identification System (RAPIDS). While DBIDS can register RAPIDS-issued credentials into the DBIDS database, and can use those credentials to scan for entry into an installation, the systems serve very different purposes, have different users and are physically located at different places on an installation. The two systems complement one another in that the credentials issued by RAPIDS are used in DBIDS. The architectures are radically different and would require significant effort and funding to develop the capability to accommodate the differing purposes and connection requirements. For example, RAPIDS works directly with the DEERS database for the sole purpose of updating personnel information or verifying benefits. DEERS is the DoD repository for all individuals who are or have been either directly employed by the DoD or who are entitled to DoD benefits, and is the authoritative database for identity of those personnel. There is a single connection between a RAPIDS station and the DEERS database. DBIDS is a database containing information used for access permissions, which has multiple connections to each site - registration stations, visitor centers, law enforcement offices, and access control points - for numerous interactions of many types. These interactions include entering and updating information at the registration stations, as well as functionality such as flagging barred personnel and verifying authority to enter a site, or confirming possession of registered property.

RAPIDS is funded centrally; DBIDS is customer-purchased and funded. The significance of this is that each DBIDS site is individually responsible for its records and access permissions. In DEERS, the responsibility for the accuracy and quality of the records forwarded for inclusion in the database is held at the Service level. A key feature of the DBIDS system is the ability to catch lost or stolen cards, and to ensure that personnel entering a site have permission to access the site. As previously stated, possession of a credential, whether PIV or not, does not in and of itself allow an individual access to a site. DBIDS provides a significant capability to ensure that only the right people enter a site, positively affecting the force protection posture. DBIDS is currently being used in CONUS, South Korea, Japan, Europe, and Southwest Asia (SWA); and these DoD installations rely on it to assist in keeping their installations safe. Similarly, RAPIDS is the repository for data supporting benefits and privileges eligibility for the DoD enterprise. Both systems have critical mission-specific purposes that are complementary. However, merging the two systems is not practical or feasible.

5. Methods Used to Minimize Burden on Small Entities

Collection of this information does not involve small entities.

6. Consequences of Not Collecting the Information

If information were not collected, the Department would not have viable security measures for identifying, controlling, and accounting for non-DoD personnel requiring physical access to DoD facilities, nor the ability to register and issue a DBIDS card to eligible recipients who are authorized access to DoD installations and facilities. Lost and stolen cards could be easily used by the finder, and counterfeit cards would be used for access at face value. The

Department's overall security posture would be compromised. Additionally, without the capability to produce a DBIDS card, many other badges or cards would proliferate, resulting in an additional burden for those who are charged with verifying credentials for access and an additional cost to produce them.

DBIDS directly affects DoD's ability to prevent crime and stop terrorism. Some examples of this include:

- Southwest Asia - Over 150 individuals were identified who had fraudulently obtained installation identification cards, and two individuals listed on the Terrorist Watch List were apprehended.

- Japan – Used as a key investigative tool at Yokosuka in identifying a US Navy sailor who had attempted to murder two Japanese women off base. The suspect was sentenced to 8 years in prison.

- Korea – Led to the discovery of a Korean contractor who was found to have a counterfeit Vehicle Safety/Registration Decal on his SUV when scanned coming through Camp Henry's Gate 2 in Daugu. Subsequent investigation revealed that the decal was not only counterfeit, but there were approximately 25 or more of the same exact counterfeit decals on vehicles, all being created by the same illegitimate Korean company.

- Europe – Identified a male dependent spouse accused of multiple incidents of rape and assault.

7. Special Circumstances

There are no special circumstances associated with this data collection. This collection will be conducted in a manner consistent with guidelines contained in 5 CFR 1320.5(d)(2).

8. Agency 60-Day Federal Register Notice and Consultations Outside the Agency

An agency 60-day Federal Register Notice was published in Volume 72, Page 67596, on November 29, 2007. No comments were received.

The information collection was reviewed and approved by the following individuals:

Ms. Becky Allen, Director of Security, Office of Under Secretary of Defense (Intelligence), 703-604-1175
Mr. Bret Vincent, Senior Security Officer, Office of Provost Marshal General, Department of Army, 703-692-5541
Mr. Mark Muck, Privacy Team Leader, Department of the Navy, 703-602-4412
Mr. Ben Swilley, Department of Air Force Privacy Officer, 703-696-6172
Ms. Cindy Allard, OSD/JS Privacy Officer, Washington Headquarters Services, 703-588-2386

9. Payments to Respondents

No payments will be made to respondents for collected information.

10. Assurance of Confidentiality

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

11. Personal Identifying Information and Sensitive Questions

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. Respondents are asked to read a Privacy Act Statement prior to providing the requested information.   All data are protected by the Privacy Act of 1974 and according to the regulations therein and by related DoD instructions and directives.

For identity verification tracking purposes, the following information is being requested:

- Gender.

The gender of the individual is requested for demographic tracking purposes only. Gender is not a factor in determination of eligibility.

- Social Security Number (SSN).

The data collected as part of the enrollment into the DBIDS solution is the basis for making access control decisions on the part of the facility commander. This access control decision may include the completion of a check of the National Crime Information Center database as a separate process external to DBIDS. This check is completed based on the SSN. Other Identifier Types are accepted if the person seeking access does not have an SSN.

The Office of Management and Budget (OMB) has required that every Federal agency develop and implement a plan to reduce the unnecessary use of the SSN. To meet this requirement, DoD issued Directive Type Memorandum (DTM) 07-015 which focuses on reducing SSN use in DoD. This DTM mandates that SSNs should not be used in DoD unless there is a specific legal/legislative requirement for using the SSN. Also, the SSN Reduction Plan provides for a comprehensive review of new and existing DoD forms and systems where SSNs are currently used or proposed. This DTM will be followed by a DoD Instruction on SSN use over the next several months.

12. Estimates of Annual Response Burden and Labor Cost for Hour Burden to the Respondent for Collection of Information

The following information is our best estimate. As we obtain more accurate data, updates will be provided.

a. Response Burden

(1) Initial Registration

Total average annual respondents:	1,216,115
Frequency of response:	Annually
Total average annual responses:	1,216,115
Average annual burden per response:	8 minutes
Total average burden hours:	162,148

(2) Revalidation/Renewal

Total average annual respondents:	405,372
Frequency of response:	Annually
Total average annual responses:	405,372
Average annual burden per response:	5 minutes
Total average burden hours:	33,781

Total average annual respondents:	1,621,487
Total average burden hours:	195,929

b. Explanation of How Burden was Estimated

Burden was estimated by observation of the process.

c. Labor Cost to Respondent

The labor cost to respondent is calculated in the following manner:

Low-pay respondents – 304,029 x $4.40 =	$1,337,728
Medium pay respondents – 729,669 x $6.60 =	$4,815,814
High pay respondents – 182,417 x $15.60 =	$2,845,705
Total	$8,999,247

13. Estimates of Other Cost Burden for the Respondent for Collection of Information

a. Total Capital and Start-up Cost. There are no capital or start-up costs associated with this data collection. Respondents will not need to purchase equipment or services to respond to this information collection.

b. Operation and Maintenance Cost. There are no operation or maintenance costs associated with this information collection.

14. Estimates of Cost to the Federal Government

Personnel specialists entering information, reviewing and processing forms for respondents Military personnel: $12 hr (average military pay grade E-4) Federal civilian employees: $13 hr (average grade GS-5) Contractor personnel: $16 hr (average hourly pay) Overall average hourly wage: $14 (1,621,487 respondents x 8/60 x $14)	$3,026,775
Total cost to the government	$3,026,775

15. Changes in Burden

Decrease in burden is due to fewer initial registrations than planned.

16. Publication Plans/Time Schedule

The results of collection of this information will not be published for statistical use.

17. Approval Not to Display Expiration Date

Approval not to display the expiration date is not being requested.

18. Exceptions to the Certification Statement

No exceptions to the certification statement are being requested.

B. COLLECTION OF INFORMATION EMPLOYMENT STATISTICAL METHODS

Statistical methods are not employed for collection of this information.