

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 (Attachment 1), 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 force protection and identity management system, using a centralized, rules-based identity management and access verification system. DBIDS will produce an identification card that will aid security personnel in identifying, controlling, and accounting for non-DoD personnel entering military installations. DBIDS maintains a centralized database that supports access control decision-making.

2. Use of Information

The purpose of this information collection is to obtain the necessary data to verify eligibility for a DoD physical access card for personnel who are not entitled to a Common Access Card (CAC) or other approved DoD identification card.

The respondents included in this information collection are non-DoD affiliated personnel requiring recurring, unescorted access to an installation (i.e., vendors, contractors, laborers, and third party nationals).

The information is used to establish eligibility for physical access to a DoD installation or facility, detect fraudulent identification cards, provide law enforcement data, and in some cases provide anti-terrorism screening.

DBIDS is used to capture and store biometric data such as photographs, fingerprints and hand geometry, as well as other information that can be used for identification or law enforcement purposes, such as vehicle data and information on weapons.

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 bar code scanning technologies to verify captured data internally against the DBIDS database and externally against available authoritative sources such as the Defense Enrollment Eligibility Reporting System (DEERS). It also is compatible with commercial software packages.

The DBIDS system utilizes four types of workstations, each designed to perform specific tasks:

- Registration Center. The Registration Center workstation enables a Registrar to enter a person’s information into the database either by scanning an identification card to retrieve the barcode-stored data, or by manually typing information into data field boxes.
- Control Point. Control Point machines are located at installation Access Control Points to authenticate persons entering the installation.
- 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 to flag individuals as Barred, Suspended, or Wanted.

Screen shots are provided of the data being captured by various installation Registration Centers to verify eligibility for a physical access card, as shown below.

	Camp As Sayliyah	
	Person Category	Expiration Date
	Contractor	19 JUN 2006
	Authorized Access To	Access Times
Access1	0600-1800	
Access2	M-F	
Sign-In Privileges	Access Authorized up to FP Condition	
Not Authorized	BRavo	
Name (Last,First, M.I.)	Rank/Grade/Title	Personal ID No.
PARKER, Susan H.	MRS.	7008957632

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.

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 was 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.

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:

Mr. Greg Torres, 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

SMSgt Walter Spigner, Information Management Control Office, Department of Air
Force, 618-229-5587

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 DBIDS using their user ID, password, and biometrics. These protection

measures safeguard the access to DBIDS to authorized users only. Respondents are asked to read the 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. This check is completed based on the 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 has issued a Directive Type Memorandum (DTM) 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.

System of Record, entitled "Defense Biometric Identification System," February 19, 2008.

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:	55,800,675
Frequency of response:	1
Total average annual responses:	55,800,675
Average annual burden per response:	10 minutes
Total average burden hours:	9,300,113

(2) Revalidation/Renewal

Total average annual respondents:	18,600,225
Frequency of response:	1
Total average annual responses:	18,600,225
Average annual burden per response:	5 minutes
Total average burden hours:	1,550,018

Total average annual respondents:	74,400,900
Total average burden hours:	10,850,131

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 – 18,600,225 x \$4.40 =	\$ 81,840,990
Medium pay respondents – 37,200,450 x \$6.60 =	\$245,522,970
High pay respondents – 18,600,225 x \$15.60 =	\$290,163,510

Total	\$617,527,470
-------	---------------

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

Equipment:	\$116,786
Personnel specialists entering information, reviewing and processing forms for respondents	\$173,602,100
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	
74,400,900 respondents x 10 minutes per specialist divided by 60 x \$14	
Total cost to the government	\$173,718,886

15. Changes in Burden

Increase in burden is due to a new information collection.

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.