DBIDS/IACS PRIVACY IMPACT ASSESSMENT (PIA)

(Use N/A where appropriate)

1. **DoD Component:** Defense Manpower Data Center (DMDC)

2. **Name of IT System:** Defense Biometric Identification System (DBIDS)

3. **Budget System Identification Number:** 4035

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository):** 1391

5. **IT Investment (OMB Circular A-11) Unique Identifier (if applicable):** 007-97-01-15-01-4035-00-403-254

6. **Privacy Act System of Records Notice Identifier:** S322.70 Defense Biometric Identification System (DBIDS) (November 18, 2004, 69 FR 67552) (Soon to be republished as DMDC 10)

7. **OMB Information Collection Number and Expiration Date: NA**

8. **Authority:** 5 U.S.C. 301 Departmental regulations; 10 U.S.C. 113, Secretary of Defense, Note at Pub.L. 106-65; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 18 U.S.C. 1029, Access device fraud; 18 U.S.C. 1030, Computer fraud; 23 U.S.C. 401 et seq. National Highway Safety Act of 1966; 40 U.S.C. Chapter 25, Information technology management; 50 U.S.C. Chapter 23, Internal Security; Pub.L. 106-398, Government Information Security Act; Pub.L. 100-235, Computer Security Act of 1987; Pub. L. 99-474, Computer Fraud and Abuse Act; E.O. 9397 (SSN); E.O. 12958, Classified National Security Information as amended by E.O., 13142 and 13,292; and E.O. 10450, Security Requirements for Government Employees.

9. **Brief Summary:** The Defense Biometric Identification System (DBIDS) is a Department of Defense (DoD) system developed by DMDC as a force protection program to manage personnel, property and installation access. DBIDS is called the Installation Control Access System (IACS) in Europe. 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 and fingerprint biometric identification. The DBIDS software application is used to enter personnel data into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time. The program supports the adding, retrieving, updating, and displaying of information for individuals, who require military installation access. DBIDS enhances the military law enforcement mission by helping to provide a safe and secure community and by allowing real-time access to data. The program alerts registration personnel and installation gate guards to barred individuals across jurisdictional boundaries, and eliminates duplication of data.

This program utilizes a personal computer (PC) based client/server database system to register personnel and vehicles. It produces installation passes for personnel who are entitled to recurring and unescorted access to military installations and do not possess a DoD ID Card. The system incorporates existing Real-time Automated Personnel Identification System (RAPIDS) ID card technology for cross platform compatibility. Data elements are compatible with the Defense Enrollment/Eligibility Reporting System (DEERS) database so data can be shared and updated across both systems through barcode technology.

10. **Identifiable Information to be Collected, its Nature and Source:** name, grade, Social Security Number, status, date and place of birth, weight, height, eye color, hair color, gender, passport number, country of citizenship, geographic and electronic home and work addresses and telephone numbers, marital status, index fingerprints and photographs, and identification card issue and expiration dates. The system also includes vehicle information such as manufacturer, model year, color and vehicle type, license plate type and number, decal number, current registration, automobile insurance data, and driver's license data.

11. **Method of Information Collection**: Data is collected from existing DoD databases, the Military Services, DoD Components, and from the individual. Installations can collect data via paper, electronic, and/or verbal submission.

12. **Purpose of Collection:** Data collected is used to enter personnel data into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time, especially when the individual requires installation access.

13. **How Identifiable Information/Data will be Used:** In the case of non-DoD individuals who require base access, a DBIDS access card is produced. The records are maintained to support DoD physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the Department, and for producing facility management reports.

14. **Does system create new data about individuals through aggregation?** No

15. **Internal and External Information/Data Sharing:** Data is maintained on Regional Servers managed by DMDC.

    Internal to DoD: Used by security offices to monitor individuals accessing DoD installations and/or facilities. Data may be viewed by or shared with civilian employees, military members, and contractors assigned to DMDC DBIDS software/database technical support, by operators responsible for registering individuals into the database, by Installation Access Control Point (ACP) personnel, and by Installation Law enforcement personnel.

    External to DoD: Data may be provided to other Federal agencies under any of the DoD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/notices/blanket-uses.html.

16. **Opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted**: The DLA rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DES-B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060-6221. Once republished and managed by WHS the accessing office will be: Privacy Act Officer, Office of Freedom of Information, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301-1155.

17. **Information Provided to the Individual, the Format, and the Means of Delivery**: Privacy Act Statements, as required by 5 U.S.C 552a(e)(3), are provided at the collection point. The statement provides the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond denial of a DBIDS card or visitors pass and denial of access to the installation, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. The DBIDS Privacy Act Statement reads as follows:

AUTHORITY: Executive Order 9397; The Privacy Act of 1974, 5 U. S. C. 552a; DODD 8500.1

PRINCIPAL PURPOSE(S): To provide necessary information to DoD installations to determine if applicant meets access control requirements. Use of SSN is necessary to make positive identification of an applicant. Records in the DBIDS system are maintained to support Department of Defense physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the DoD, and for producing facility management reports. Used by security offices to monitor individuals accessing DoD installations and/or facilities. SSN, Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to DoD installations and/or facilities.

ROUTINE USE(S): The "DoD Blanket Routine Uses" are set forth at the beginning of the DoD compliation of systems of records notices.

DISCLOSURE: Voluntary. However, failure to provide the requested information will result in denial of a DBIDS card or visitors pass and denial of entry to DoD installations and/or facilities.

18. **Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.** Computerized records are maintained in a controlled area accessible only to authorized personnel. Entry is restricted by the use of locks, guards, and administrative procedures. Access to personal information is limited to those who require the records in the performance of their official duties, and to the individuals who are the subjects of the record or their authorized representatives. Access to personal information is further restricted by

the use of unique logon and passwords, which are changed periodically.

19. **Privacy Act Interface:** Yes. System of Records Identifier listed in question 6.

20. **Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures**: Data is collected and used in a dedicated security mode. Data sharing occurs only among individuals authorized access to the system as stated in the governing Privacy Act system notice. Data screens are marked with the "for Official Use Only" data handling legend. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training. There are no dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived. The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

| | | ASSESSMENT |
|---|---|---|
| **RISKS** | **MITIGATION** | **(HIGH) (MED) (LOW)** |
| Userid/password/DBIDS card used by someone other than whom assigned | Allocation of passwords is managed and password security policies enforced. There is the possibility of loss of PII data on an individual basis. | (MED) |
| Mishandling of sensitive data, reports, or storage media | Periodic assessments of access rights and privileges are performed | (LOW) |
| Virus attacks and other malicious incidents | System controls are predicated on preventing unauthorized users from accessing DBIDS resources to minimize the risk presented by outside threats. Current DBIDS systems run on closed networks, and do not afford an outside threat the potential for system infiltration and compromise. Future DBIDS versions (3.0 and later) will utilize web services, which will increase risk. Intrusion prevention and detection methods certified and approved for use by the JTF GNO will be employed to assure security of operations. Internal threat mitigation will occur through network and Regional server monitoring to detect, identify and prevent installation of malware, and by workstation audit and configuration validation/verification by the local site SSM. We will have training certification for operators and periodic audits of installed applications and software/ hardware components by SSM, which will minimize risk by assuring only authorized products are present, installed and functioning in a manner consistent with DoD security policy. | (LOW) |

| | | |
|---|---|---|
| PII data appears on certain reports | The security requirements for the safe use, handling, storage and destruction of PII data is included in the training provided during the installation of DBIDS at each site, and is reinforced during routine site support visits. PII security awareness is included in the web based training that is developed in support of DBIDS 2.7. The proper secure handling of reports is covered in site standard operating procedures to prevent unintended exposure of data, and to preclude data loss. Reports printed out by the site must be labeled "FOUO" when they contain Privacy Act data. Locally, PII awareness must be a sustained focus of the individual DBIDS Site Managers and command sponsors; their daily management of the sites provides assurance against PII data compromise. | (MED) |
| Loss of DBIDS card | It is the responsibility of the card holder to inform issuance authorities and/or the Provost Marshall/Directorate of Emergency Services in the case of a lost or stolen credential. The credential can then be flagged as lost or stolen in the DBIDS software. Until this action is performed, however, there is a chance the credential could be used by an unauthorized individual to gain access to a facility or installation. The requirement to immediately notify the local installation authorities is formally provided to the card recipient at time of issuance, and is re-advertised periodically as a matter of local command policy. This risk is mitigated by the capability of DBIDS to provide the photo of the card recipient; this photo is required to be compared to the face of the cardholder to confirm identity. Additionally, at the discretion of the local installation commander, use of a fingerprint biometric to confirm identity may be required as a matter of normal business, under selected situations or periods of time, or during periods of heightened Force Protection Condition. | (MED) |

21. **Classification and Publication of Privacy Impact Assessment:** This document will be published in full form on the DMDC public website http://www.dmdc.osd.mil/