

**BY ORDER OF THE COMMANDER
910 AIRLIFT WING**

910 AIR WING INSTRUCTION 31-502

10 MAY 2013



Security

**DEFENSE BIOMETRIC IDENTIFICATION
SYSTEM (DBIDS) OPERATIONS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms identified within this product are available at the AF e-Publishing website, www.e-Publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 910SFS/S5

Certified by: 910AW/CC
(Colonel James D. Dignan)

Pages: 14

This instruction defines procedures for integrating, operating and controlling the Defense Biometric Identification System (DBIDS) as base/facility Security Forces (SF) transition to automated installation entry control. Additionally, this instruction identifies procedures for the administration and management of DBIDS as performed by the SF Site Manager, and the SF Pass and Registration staff. This instruction gives the Installation Commander (910AW/CC) at the Youngstown Air Reserve Station (YARS), Vienna, Ohio, flexibility on who can be issued a DBIDS card. Reference materials for information contained within this instruction are Homeland Security Presidential Directive (HSPD-12), *Policy for a Common Identification Standard for Federal Employees*; DoD Regulation 5200.08-R., *Physical Security*; Air Force Instruction (AFI) 31-101, *The Installation Security Program*; AFI 31-113, *Installation Perimeter Access Control*; Title 5, United States Code (U.S.C) 552a, as amended, *The Privacy Act of 1974*; and applicable DBIDS instructions and manuals. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) 847, *Recommendation for Change of Publication*. Route all AF847s from the field through the appropriate chain of command to the OPR. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). See Attachment 1 for a Glossary of References and Supporting Information. **NOTE:** Any document, form, or record created using Personal Identification Information (PII) must do so within the

scope, limitations, and protection of AFI33-332, *Air Force Privacy Act Program*, and Title 5, USC 552a, as amended, *The Privacy Act of 1974*.

1. GENERAL.

1.1. Control of personnel and vehicles entering and exiting Youngstown Air Reserve Station (YARS) is necessary to provide a safe environment in which to work and to provide for the protection of government property and operational resources. The Defense Biometric Identification System (DBIDS) is an access control system designed to enhance force protection and identification management by capturing and storing biometric data of personnel that access the installation.

1.2. The system is capable of reading all existing Department of Defense (DoD)-issued identification credentials, to include dependent and retiree identifications cards. DBIDS is also capable of generating an identification card that stores a digital photograph and biometric fingerprints for contractors, students, or other personnel who do not have independent access to the installation, but have a valid and recurring need to enter the installation.

1.3. All Active Duty military personnel, military Reserve members, military Dependents, military Retirees, DoD civilian employees, and contractor personnel who require routine access to the installation must register their current identification (ID) in the DBIDS database. Installation access for all visitors, contractors, and vendors will be initiated by an OHLEG, National Crime and Information Check (NCIC) or Law Enforcement Automated Data System (LEADS) data check as applicable. DBIDS issued IDs will be restricted by date and Force Protection Condition (FPCON).

1.3.1. DBIDS will be used as an access control system specifically for enhancing force protection and security measures pertaining to access to the Youngstown Air Reserve Station. DBIDS is not intended to, and will not be used as a tool to monitor employee's performance. Information gathered through DBIDS will not be used to generate adverse actions against employees unless directly related to a security violation.

1.3.2. All civilian and military personnel assigned to YARS will have full access to the installation through FPCON Charlie. This access level also includes all Base Operating System (BOS) contract personnel (i.e., EAST Inc).

1.3.3. All assigned personnel that are identified by position as "MISSION ESSENTIAL" will have access through FPCON Delta.

1.3.4. Only those personnel identified by the installation commander will have access during FPCON Delta/POTUS.

1.4. Entry Controllers will scan ID cards utilizing the card scanner or manual validation. The on duty Entry Controller will then verify the picture and information to display on the screen against the ID card and the person presenting the ID.

2. Responsibilities.

2.1. Not Used.

2.2. Defense Force Commander (DFC):

2.2.1. Integrate DBIDS into daily operations.

2.2.2. Establish specific DBIDS mission standards and procedures.

2.2.3. Program, with the Air Force Reserve Command (AFRC) A7S function, for DBIDS sustainment costs, to include: Help Desk and technical support, DBIDS computers, allied support and support equipment.

2.2.4. Develop and publish access control policies and procedures in the Integrated Defense Plan (IDP). The following will be included in the IDP regarding access control:

2.2.4.1. Develop procedures for DoD ID-card holders to register and withdraw from DBIDS during in and out processing.

2.2.4.2. Produce procedures for retrieving access credentials from individuals who no longer require installation access such as contractors or vendors.

2.2.4.3. Implement a process to identify who requires installation access and approval authority for access during FPCON Bravo, Charlie, Delta and specialized Delta (POTUS).

2.2.4.4. Develop a process to initiate Be On the Lookout (BOLO) alerts; emergency notification (e.g., Red Cross) or other non-standard DBIDS applications.

2.2.5. Develop procedures to deny access to personnel who have not been trained to operate DBIDS.

2.2.6. Establish security procedures to prevent theft or damage at operating locations and access control points.

2.2.7. Establish registration and issuance of installation access credentials and ensure security forces personnel are trained, proficient, and certified in their assigned responsibilities; annotate training completion on the AF Form 623A in Air Force Training Records (AFTR).

2.3. Site Security Manager (SSM):

2.3.1. Serves as the installation subject matter expert for DBIDS and maintain an appropriate level of proficiency.

2.3.2. Provide a detailed report on all derogatory information received on an individual to the DFC or their designee, and flags ID card holder's account.

2.3.3. Not Used.

2.3.4. Coordinate with 910 SF Reports and Administration (S5A) and 910 SF Operations (S3O) when individual(s) are barred from the base.

2.3.5. Submit technical refresh requirement for annual DBIDS computer or system software upgrades. SM will inform AFRC/A7S when technical refresh submittals are included in the wings annual technical refresh requirements.

2.3.6. Ensure proper destruction of the old DBIDS Access Card (DAC) and make notification to the originating agency regarding its disposition.

2.3.7. Provide quality control for data integrity on data input and randomly monitors registrar operations for quality and consistency.

2.3.8. Train new personnel on DBIDS software and components as they are assigned.

2.3.9. Perform user maintenance on all DBIDS equipment to keep them in proper working order and will not exceed warrantee recommended maintenance procedures, and will notify DMDC DBIDS contractors and the helpdesk where normal maintenance has not resolved component problems.

2.3.10. Remove the computer hard drives of DBIDS workstations and laptops prior to shipping an inoperable system back for repairs.

2.3.11. Ensure equipment is not shipped back for repair without a DMDC Help Desk ticket number. Do not ship for 24 hours, as a TELOS representative may call to further diagnosis the problem. If they do not call within 24 hours and a ticket number is available, ship the item.

2.3.12. Keep track of all DBIDS consumable supplies; i.e., printer ribbon, laminates, and card stock. Attempt to limit ordering to annually.

2.3.13. Review and ensure quality of information on the Contractor Data Sheet (CDS); ensures all proper copies of required paperwork are attached; ensures the information is printed clearly and legible, and maintains CDSs in a secure location for a minimum of two years past the expiration of the DAC issued against it.

2.3.14. Coordinate/report all DBIDS major issues covered and not covered within this instruction with HQ AFRC/A7S.

2.4. Registrar:

2.4.1. The registrar is responsible for registering individuals into the DBIDS system. The registrar enters personal data, determines the correct authorization profile, captures a photo and fingerprint for each user (depending upon category), and produces DACs when required.

2.4.2. The Registrar can also make changes to existing user records, register and flag vehicles, edit the barment roster, edit the access areas, and any other function determined by SSM or appropriate authority.

2.4.3. Contacts an SSM or Alternate SSM whenever issues with the DBIDS system arise.

2.5. Gate Guard:

2.5.1. Responsible for authenticating an individual's access authority by scanning their Common Access Card (CAC) or DAC at entry control facilities to the installation.

2.5.2. Verify equipment is operable upon assuming post by conducting a scan of own CAC. Report any system issues to the SSM.

3. DBIDS Recognized ID Cards.

3.1. DBIDS accepts and recognizes three different types of ID cards. The following sections describe the characteristics of each ID card type.

3.1.1. Teslin cards are produced through the Defense Enrollment Eligibility Reporting System (DEERS) for DoD affiliated members such as Active Duty, Dependent, Retiree, Civil Service, and Contractors. DBIDS reads all Teslin cards.

3.1.2. A Common Access Card (CAC), the new Teslin card with an embedded computer chip, contains the cardholder's personal information in the Portable Data File (PDF) 417 barcode and is fully supported by DBIDS. Barcode identification information is crosschecked with Biometric Fingerprint Authentication technology and personal information from the DBIDS database system.

3.1.3. DBIDS cards are produced on-site through the DBIDS application for non-DoD ID cardholders and are installation passes not DoD ID privileges card. Barcode identification information is cross-checked with Biometric Fingerprint Authentication technology and Person information from the DBIDS database system. Do not issue a DBIDS card to individuals authorized a DoD ID card.

4. DBIDS Registration Process.

4.1. All personnel requiring recurring and unescorted access to YARS, to include those issued CACs and other credentials outlined in AFI 36-3026, must enroll in DBIDS and provide digitized fingerprint minutia data (DFMD) during registration. This may be obtained during in-processing or initial pass issue or can be pulled down from DEERs provided they are on file in the DEERs system. All DoD ID-card holders assigned to YARS and YARS-pass applicants must be registered. The Installation Commanders will determine requirements for DoD-card holders who are TDY to or visiting YARS for 29 days or less and document the requirements in the IDP. Personnel TDY to YARS for more than 30 days or more must register in DBIDS. * **NOTE:** DoD ID card holders can utilize fingerprints and photos stored in DEERS and those assigned to YARS may register for the first time at the main gate.

4.2. Unique Circumstances/Special Events. The Installation Commander may grant the use of other measures including, but not limited to, Entry Access List (EAL) or access memoranda for specific special events or unique circumstances. In these cases, driver's licenses, passports, or other means of photo identification may be used in concert with the EAL for access. Names on these documents must be vetted against authoritative government databases for potential derogatory fitness information. Commanders must minimize the use of these measures and use DBIDS credentials, AF Forms 75, or other credentials when applicable. For initial access of official foreign visitors or others who require the eventual issuance of a CAC, an EAL, AF Form 75, or DBIDS credential will be used following access need determination/sponsorship, ID proofing and vetting.

4.3. All personnel requiring recurring and unescorted access to YARS must:

4.3.1. Enroll in the DBIDS and provide DFMD. This may be obtained during in-processing or initial pass issue and must be completed at the visitor center in building 102. Fingerprint-data policy is as follows:

4.3.1.1. In-processing. Personnel who possess an authorized DoD ID card and access credential pass applicants will provide DFMD during registration process unless they can be pulled down from DEERs. If a DoD ID-card holder has a manually-produced

DoD ID card, the individual must obtain a machine-produced bar-coded DoD ID card according to the appropriate military regulations and personnel systems.

4.3.2. Issuance personnel must brief the recipient on requirements listed in paragraphs through 4.3.6, this publication.

4.3.3. Carry their DoD ID card or IP (for non-DoD card holders) on their person while in duty status or when on a United States Air Force (USAF) installation. On request, they will present their DoD ID card or access credential to security forces personnel. Individuals who refuse to present their DoD ID card or IP are subject to immediate surrender of the credential and may be grounds for further administrative or punitive action.

4.3.4. Immediately report a lost or stolen DoD ID card or access credential to the local security forces (SF) or issuance office so the card can be deregistered.

4.3.5. Inform the sponsoring organization of any change to the official relationship that served as the basis for access.

4.3.6. Turn in access credentials to the issuance office or sponsoring organization when the credential expires or when the basis for obtaining the credential no longer exists.

4.4. Types of credentials. USAF installations currently employ a variety of temporary access credentials. The USAF goal is to employ a standard credential which is capable of electronic interrogation and interoperable among all DoD Services. Currently, the format being employed across the Services in this capacity is DMDC's DBIDS. Once fully implemented at YARS, the DBIDS credential will be used as the primary means for allowing non-CAC eligible populations physical access to installations. Installation visitor passes will only be issued in person to the applicant or a sponsoring CAC holder.

4.4.1. DBIDS Credential. Once issued, these credentials are approved for physical access to YARS.

4.4.2. AF Form 75, Visitor Pass/Vehicle Pass. 910 SFS may continue to use the AF75 as an access credential to YARS in the event DBIDS is temporarily inoperative or as prescribed by S3O.

5. Registration Categories.

5.1. The following are categories of personnel to be used during the registration process:

5.1.1. DoD ID-Card Holder: An individual authorized to possess a DoD ID card to include children 10 years and older. The status of a DoD ID-card holder will supersede other person categories. For example, an LN employee, married to a service member and entitled to a DD Form 1173, Uniformed Services Identification and Privilege Card, will be treated as a DoD ID card holder for the purpose of this regulation and will not be issued an IP nor require sponsoring.

5.1.2. Contractor: A person contracted to work for DoD, but is not a DoD ID-card holder.

5.1.3. Delivery Personnel: Individuals who need recurring access to YARS to make deliveries or perform a similar service related to their employment (i.e., pizza delivery, taxi driver) in a service authorized to conduct business on the installation.

5.1.4. Vendor or Commercial Solicitor: Individuals authorized to sell merchandise or provide services on USAF installations.

5.1.5. Base Services User: Personnel with limited access to an installation to attend courses or other services as authorized by the Installation Commander.

5.1.6. Member of Private Organization: A member of an approved private organization who has no other reason to enter YARS other than to participate in private organization functions approved by the Installation Commander.

5.1.7. Visitor (Friend or Family Member Not Included in Category Above): A visiting family member or friend of the requester who is not authorized a DoD Identification Card.

5.1.8. Official Local Guest: A broad category designed for individuals requiring recurring access for official business or access based on an official relationship (for example, visits by local city officials such as the mayor, fire chief, or other civic leaders). Sponsoring organizations will not use this category when the applicant meets the definition of another, more restrictive person category. This category is specifically designed for personnel, who by their position or standing within the community, are considered trustworthy. The S5 section will coordinate with sponsoring agencies to verify need for access of all personnel identified under this category and forward those approved for access.

5.1.9. Department of State, U.S. Embassy Personnel, or Other Federal Agencies: An individual assigned to or on duty with the United States Department of State, an American Embassy, U.S. diplomatic or consular posts, or other Agencies of the Federal government.

5.1.10. Other: An individual who requires recurring and unescorted access, but does not meet the definition of any other category. Sponsoring organizations will not use this person category if the applicant meets the definition of another, more restrictive person category. This category is appropriate for a former spouse without base privileges whose children are military dependents with base privileges, but are not old enough to utilize base facilities without parental supervision.

5.1.11. Dual-Category Individuals: A dual-category individual (for example, a military retiree who is also a contractor) will be registered in the person category with the greatest access privileges. The Official Guest and Other person categories will never be used as a dual-category qualifier.

6. Requesting Authority (RA) for DBIDS Access Card.

6.1. The RA for DBIDS Access Cards for contractors is usually the contracting office/contracting officer or the contracting office/contracting officer representative. In cases where the contracting office is not involved it can also be the commander of the unit initiating the contract, and in certain cases, a US military member or US Government employee (i.e., General Schedule (GS)) requesting access for an individual not affiliated with a contract or company but has legitimate reason for access that conforms to all applicable policies, instructions, and regulations.

6.2. The requesting unit commander must delegate individuals in writing and forward delegation to 910 SFS/S5L to act on behalf of the unit as the RA.

6.3. For contract modifications resulting in a reduction in the contract expiration date, the RA must notify the DBIDS office within 24 hours of the modification.

6.4. If the contract date is extended the RA must ensure a memorandum is submitted to the Approving Authority, requesting an extension to the expiration date. The Approving Authority must approve, sign and date the memorandum and submit it to 910 SFS/S5L.

6.5. New DACs will be reissued upon receipt of the memorandum. DACs will not be reissued if the extension time is 30 days or less, but new expiration dates will still be entered into the database and the SM will furnish SFS/S5L with a written list in the event the gate system becomes in-operational and the visual inspection of the DAC is used for access.

6.6. Sponsor Responsibilities.

6.6.1. Sponsors who are supervisors within a contracted company will identify individuals in their organization who require access on a regular basis, certify they are trustworthy, and pose no threat to the installation. Contract sponsors will initiate the application process with applicants, validating that all information is accurate, and submit completed applications to 910 SFS/S5L. Non-compliance and lack of enforcement of this policy without approved exception will result in termination of these positions and possible revocation of issued DACs. Sponsors who are US military members or US Government employees are responsible for the actions of any individual they sponsor for access and will assist the individual with the application process.

6.6.2. Coordinate with PASS and REGISTRATION to get applicants onto the DBIDS enrollment schedule. The sponsor must ensure the applicant has a completed CDS and has all available identification, to include identification, employment contracts, driver's licenses, vehicle registrations, military service documentation, birth certificates or National ID Card, and background check, paperwork forwarded from 910 SFS/S5L at the time of biometric enrollment and have not expired. Copies of this paperwork are required and will be retained and attached to the CDS.

6.6.3. Individuals will pick up and activate their own DAC.

6.6.4. If an applicant is fired or quits, the sponsor retrieves all access cards, credentials and/or vehicle passes possessed by the applicant, notifies the PASS and REGISTRATION of the worker's status (i.e., escorted off the installation or worker transferred), and coordinates with the RA to furnish any discrepancies incurred with the return of access cards and any derogatory information on the applicant.

6.6.5. If an individual is being barred from the base and it is feasible, bring the individual to the DBIDS office for a full biometric registration whereas the registrar will input into the Reason Fingerprinted field the comment: .ALERT ALERT – Barred from YARS.

6.6.6. Coordinates with the RA for the return of all access cards, credentials and/or vehicle passes to the DBIDS office within 24 hours of applicant termination.

7. DBIDS Program Management.

7.1. Enrollment: All U.S. military, civilian personnel, retirees and visitors will enroll into DBIDS database by the Pass and Registration Section or at the main gate upon initial in-processing and during ID card issuance.

7.2. Security Forces personnel trained as ECC controllers will contact the SSM to be registered into the system with the appropriate privileges.

7.3. Assigning a DBIDS User Account: DBIDS operators accounts will be assigned by S3O and activated by the SSM.

7.4. Trouble Calls: If DBIDS does not function properly after attempting the operator's troubleshooting protocol utilizing the DBIDS troubleshooting guide, log the nature of the problem into the DBIDS logbook located at each entry control point and notify an SM for assistance. Write down the message displayed in the RED screen in its entirety. If the problem cannot be fixed, the SM or ECC will contact the DBIDS Help Desk for assistance. If assistance is required after duty hours or during weekends, the Help Desk is closed. The SM will notify the on-call maintenance person and request additional assistance.

7.4.1. The DBIDS Log book will be annotated with the nature of the problem, who was notified, corrective actions, and an estimated completion date. This information will be annotated in the log book and passed on from shift to shift until problem is fixed. The DBIDS log sheet will be turned into ECC upon completion of each shift.

8. Training. System operators must complete the DBIDS computer based training. Additionally, system operators will be given hands on training using a train the trainer method with materials provided by DBIDS.

JAMES D. DIGNAN, Colonel, USAFR
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI31-101, *Integrated Defense (FOUO)*, 8Oct2009

AFI31-101_AFRCSUP, *Integrated Defense (FOUO)*, 24Aug2011

AFI31-113, *Installation Perimeter Access Control (FOUO)*, 26Jan2012

AFI33-332, *Air Force Privacy Act Program*, 16May2011

AFMAN33-363, *Management of Records*, 1Mar2011

DoDI5200.08R, *Physical Security Program, Defense Biometric Identification System Operators Manual*, 27May2009

HSPD12, *Policy for a Common Identification Standard for Federal Employees*, 27Aug2004

Title 5, USC Code 552a, as amended, *The Privacy Act of 1974*,

Adopted Forms

AF623A, Air Force Training Record

AF847, Recommendation for Change of Publication

AF75, Visitor/Vehicle Pass

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFTR—Air Force Training Record

AW—(910) Airlift Wing

CAC—Common Access Card

CDS—Contractor Data Sheet

DAC—DBIDS Access Card

DBIDS—Defense Biometric Identification System

DEERS—Defense Enrollment Eligibility Reporting System

DFC—Defense Force Commander

DFMD—Digitized Fingerprint Minutia Data

DMDC—Defense Manpower Data Center

DoD—Department of Defense

DODR—Department of Defense Regulation

ECC—Emergency Control Center

EAL—Entry Access List

FPCON—Force Protection Condition

HSPD—Homeland Security Presidential Directive

ID—Identification

IDP—Integrated Defense Plan

LEO—Law Enforcement Operations

OHLEG—Ohio Law Enforcement Gateway

NCIC—National Criminal Information Center

POTUS—President of the United States

RA—Requesting Authority

SSM—Site Security Manager

SF—(910) Security Forces

VC—Visitor Center

YARS—Youngstown Air Reserve Station

Attachment 2

Sample letter identifying Requesting Authority for DBIDS

Air Force Reserve Command



MEMORANDUM FOR 910 SFS/S5

(Date)

FROM: *(Unit commander or section chief)*

SUBJECT: Requesting Authority for DBIDS Access cards.

1. This letter identifies the Requesting Authority (RA) for Defense Biometrics Identification System (DBIDS) access cards for *(xxxx squadron/unit)* assigned to the 910 Airlift Wing, Youngstown Air Reserve Station, Vienna, Ohio. DBIDS access cards will not be produced or issued without a current RA letter on file with the 910 AW/SFS Pass and Registration section (910 SFS/S5P).

	<u>Name</u>	<u>Unit</u>	<u>Rank</u>	<u>Phone#</u>
<i>Primary</i>				
<i>Alternate</i>				

2. These requirements are in accordance with 910AWI31-502, Chapter 4. All questions or concerns should be directed to 910 Security Forces/S5 office, base telephone 609-1096

//Signature Block//, USAFR
Commander, (Orgn Name)

Attachment 3

CONTRACTOR DATA SHEET

NOTICE: The Federal Privacy Act of 1974 as amended applies. This spreadsheet contains information that must be protected in accordance with DoD 5400.11R, and it is intended For Official Use Only (FOUO).

Contract Number: _____

Project Number and Title: _____

On-Base Work Site Location (Facility and Room Number): _____

Prime Contractor's Expected Period of Performance for the Contract/Project: _____

910CONF (Contracting Office) Point of Contact: _____

Primary Contractor Firm Name, Complete Address and Office Phone Number:

Prime Contractor's Project Manager Name and Phone Number (Mobile Number Preferred):

Subcontractor Firm Name, Complete Address and Office Phone Number:

Subcontractor's Crew Supervisor Name and Phone Number (Mobile Number Preferred):

Period of Performance (Dates) of Work On-Base by the Above Subcontractor:

