SUPPLEMENTAL INFORMATION

DBIDS History

DBIDS, originally conceived to protect the Combined (USAF – Republic of Korea (ROK)) Command Center in 1995, addressed the need for high security as well as cultural issues in Korea. It was adapted to address identification and access issues on the entire Korean Peninsula as a joint project between United States Forces Korea (USFK), the Joint Staff, and the Office of the Secretary of Defense. The following table provides key dates in the development of DBIDS since 1995.

DATE	ACTIVITY
September 2001	DBIDS fully implemented at FPCON Delta for USFK
May 2002	Remote wireless handheld scanner capability introduced; provides rapid access control at gates
2003	USAREUR launches DBIDS (known as IACS) Regional inter-service DBIDS set up with DMDC, Presidio of Monterey and Naval Postgraduate School
September 2004	First stand-alone DBIDS Implementation in CONUS at Ft. Hood
October 2004	First DBIDS implementation in Japan (Yokosuka)
November 2004	First DBIDS implementations in Kuwait and Qatar
December 2004	DBIDS Mobile Kit prototype finalized for future deployment in support of flexible NCR asset protection – joint effort with DHS and DOI
January 2007	Sent first Southwest Asia (SWA) Electronic Biometric Transmission Specification (EBTS) package to Biometrics Fusion Center matching against Automated Biometrics Identification System (ABIS)
2007	First DBIDS implementations in SWA: UAE, Kyrgyzstan, Saudi Arabia, Bahrain
April 2008	First DBIDS deployment in the Philippines
September 2008	Air Force DBIDS deployments at Peterson AFB and USAFA; first 2 of 13 AF sites in CONUS

The deployment of DBIDS to Air Force installations in CONUS was undertaken at the request of the U.S. Northern Command (NORTHCOM). NORTHCOM's mission is to anticipate and conduct Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests. NORTHCOM's Area of Responsibility (AOR) includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida.

DBIDS Authorization Categories

The rules surrounding entry to an access area are defined by regional or installation leadership and are based on authorization categories. In the case of a DoD ID cardholder, the authorization category from the ID card is used. For non-DoD ID cardholders who receive a DBIDS card, the list of authorization categories is also defined by regional and/or installation commanders. For example, Army Europe (AE) Regulation 190-16 is the governing directive for all personnel categories except for personnel employed under the provisions of CTA II. The following table lists Authorization Categories used within each of the DBIDS geographical areas.

PACIFIC COMMAND	SOUTHWEST ASIA (SWA)	EUROPEAN COMMAND	CONUS (AIR FORCE)
U.S. Embassy	CATI/TCN [non-U.S. citizen, non-screened (untrusted)]	Personal Service Employee [nanny, housekeeper, etc.]	Facilities Service
Family Member of U.S. Embassy	CATII/Foreign Military [non-U.S. citizen, screened (trusted; i.e., coalition forces)]	Visitor [immediate family member living in the USAREUR/ USAFE AOR – typically family members of local national spouse]	Maintenance
United Nations Command (Sponsor or Family Member)	CATIII/Contractors [U.S. citizen, non-screened]	Visitor [friend or family member not included above – typically family members on vacation from outside Europe]	Volunteer
Host Nation Military	CATIV/DoD ID [DoD ID – U.S. citizen, screened]	Official Guest [at local commander's discretion]	Conveyance
Host Nation Defense Agency (JSDF)	CATV/Commander's Exception [typically used for host country VIPs]	Other [often the unmarried or divorced mother of a sponsor's child]	Personal Delivery
Family Member of JSDF		Host Nation Military Member	Personal Services
Host Nation Government Official		Delivery Personnel	Facility Use
Local National Employee		Foreign Student [Marshall Center]	Visitor
Long Term Visitor (1 yr)		Dept of State/U.S. Embassy Personnel	Emergency-Essential Civilian (non-CAC)

PACIFIC COMMAND	SOUTHWEST ASIA (SWA)	EUROPEAN COMMAND	CONUS (AIR FORCE)
Local National Contractor		Contractor [U.S. citizen based in CONUS]	U.S. Government Civilian (non-CAC)
Local National Contractor - Awaiting Background Check)		Member of Privat Organization [e.g., Red Cross]	U.S. Government Contractor (non-CAC)
Local National Contractor – Escort Required		Local National Employee [do not require computer access]	Foreign Military (non-CAC)
Personal Services (e.g., Domestic labor workers)		NATO Member Assigned	Foreign Government Civilian
Taxi Driver		Host Nation Government Official [mayor, police chief, building inspectors, etc.]	Foreign Government Contractor
Third Nation Military Command Sponsored		IACS Gate Guard	Foreign Military Dependent
Third Nation Military Non-Command Sponsored		Contractor (living in host nation) [e.g.,U.S. citizens living in Europe and working as local nationals]	Foreign Military Retiree
Distinguished Visitor (CDR defined)		Vender/Commercial Solicitor [licensed salespeople]	Foreign Civilian Visitor
Short Term Visitor (less than 30 days)			
Visitor – Escort Required			
Family Member under 10 years of age			
Non-SOFA Civilian Living in Japan (no DoD ID card)			
JSOTF U.S. Contractor (no CAC) – Philippines Special Operations specific			

Vetting of DBIDS Cardholders

In CONUS, applicants for a DBIDS card are required to provide appropriate identification (e.g., a government issued photo) and additional documentation as required based on their authorization category and regional/local requirements for each category. Some categories require an installation sponsor.

In foreign locations, the vetting requirements for receiving the DBIDS installation pass vary by location. In Europe, all background checks on local nationals are conducted by the host nation and, in most cases, the results are provided directly to the DBIDS staff. Background checks are most thorough in Germany where the bulk of U.S. forces are stationed. Fingerprint capture is problematic in the European Union, and governed by local and national laws. In Germany, the capture of a photo and fingerprints is allowed because they are stored locally in the DBIDS database. The data is used exclusively for individual identification in connection with access to and presence on U.S. Forces installations. The data is protected against unauthorized access by state of the art access control systems and accessible only by personnel responsible for installation protection. In many countries, such as Italy, Spain and Greece, the host country owns the base and controls access; U.S. forces are essentially tenants on those bases and must abide by host country laws.

Throughout Asia all foreign nationals are vetted with background checks. Some background checks are done by the host nation, some are done in coordination with the host nation. In Korea, Army Korea Regulation 190-7 governs installation access and specifies, among other things, when and what types of background checks are required for the issuance of a DBIDS card. Background checks in USFK consist of three parts: a local check through the local U.S. military law enforcement agency or USFK Joint Police Information Center (JPIC), a check conducted through the Korean National Police Agency (NPA) and, as required, an additional check through US Embassy-Korea.

Due to the heightened security requirements in SWA, individuals who fall into Category I (CATI/TCN) are vetted prior to receiving a DBIDS card. In addition to the frontal photograph and two fingerprints required of each registrant in other regions, other country nationals that have not been vetted by “trusted” sources, e.g., coalition military service members and U.S. contractor personnel, are required to provide iris scans, ten-print fingerprints, hand geometry, and five photographs for facial recognition. They must also provide additional demographic information including nationality, place of birth, aliases, race, tribe, blood type and marital status. In the next version of DBIDS for SWA, which is undergoing testing at the present time, the registrant will be required to provide more demographic information, including names of family members, identifying credential information, employer information, sponsor information, and requesting official information.

Collected biometric and demographic information is submitted to an element of the Biometrics Task Force (BTF), formerly known as the Biometrics Fusion Center. Upon receiving applicant data the BFF verifies the data using the Automated Biometric Identification System (ABIS) against various authoritative sources such as the Integrated Automated Fingerprint Identification System (IAFIS), maintained by the Federal Bureau of Investigations (FBI), and their own red force database. The BTF returns a message stating whether there is match for the individual in these authoritative sources, indicating a potential "person of interest".

If there was no match, the message is referred to as a NONIDENT. If a match exists, the message is called an IDENT. The IDENT may be low in criticality – it may reflect the individual as already enrolled in another biometric system such as the Biometric Identification System for Access (BISA) or the Biometric Automated Toolset (BAT), in use elsewhere in the Area of Responsibility (AOR). The IDENT could be of higher criticality – the individual's print matched a latent print associated with counter insurgency activities, i.e., a print on an Improvised Explosive Device (IED). In the second case, the screening official at the DBIDS registration site is directed to check the Biographical Intelligence Analysis Report (BIAR) from the National Ground Intelligence Center (NGIC) website. After reviewing the BIAR, the screening official makes a decision to approve issuance of a DBIDS identification card, reject the application, or detain the individual.

This vetting process is consistent with the process at foreign locations described in the Office of Personnel Management Memorandum, dated July 31, 2008.