Defense Biometrics Identification System
Standard Operating Procedures

1. Purpose. To establish and prescribe procedures for access control to Commander, Navy Installations Command (CNIC) installations via Entry Control Points (ECPs) using the Defense Biometric Identification System (DBIDS).

2. Background.

a. General. DBIDS is an enterprise identity management and perimeter installation access control solution.

b. Objective and Goals. Implementation of DBIDS is intended to:

(1) Enhance installation safety and security by using a common system across the CNIC enterprise to enroll, authenticate, credential, authorize and manage access privileges of DoD personnel and vendors/contractors coming aboard CNIC installations.

(2) Enhance efficiency and effectiveness at Visitor Control Centers (VCC) through improved business processes with a significant reduction in the issuance of contractor passes and other locally produced credentials.

(3) Enhance efficiency and effectiveness at all perimeter ECPs; specifically through the improved management of vendors/contractors, their vehicles and throughput of all vehicles coming aboard CNIC installations.

3. DBIDS Procedures.

a. Enrollment. The installation and tenant organization Sponsoring Activity's (SA) will provide the Approved Facility Contact (AFC) a list of approved vendor/contractor companies and (for each company) the name of their designated Service Contractor Administrator (SCA). For those vendor/contractor companies not included on the original approved vendor/contractor company list (ACL), the following applies:

(1) Vendors/contractors must be able to identify an SA of an installation, tenant activity or organization.

(2) Service Contractor obtains approval or denial from the Installation AFC or SA and informs the company of their status. If approved, the VCC adds the Vendor/Contractor into the ACL.

(3) The SA may also provide the names, addresses and associated identification information relating to vendor/contractors to the Service Contractor to populate the ACL in advance.

b. Registration. Once enrolled, companies may direct their employees to register into DBIDS.

c. Employee Registration and Credentialing.

(1) The vendor/contractor company must provide the DBIDS Registrar with an approved employee list. The data required either before or during registration in DBIDS may include, but is not limited to:

(a) Name
(b) Social Security Number
(c) Company/Employer Information
(d) Company Address
(e) Company Phone Number(s)
(f) Contract Number(s)
(g) Contract Date(s) of Performance
(h) Company-issued Employee Identification Number
(i) Individual Digital Photo
(j) Date of Birth
(k) Fingerprints
(l) Employee Home Address
(m) Employee Personal Phone Numbers

(2) When the vendor/contractor employee (s) registers into DBIDS, the VCC Staff conducts a background screening on each vendor/contractor employee by validating an individual's identity and biometrically authenticating their enrollment into the system.

(a) Identity Proofing Concept. Issuing authorities will employ the following baseline standards for identity proofing.

1) Applicants voluntarily provide personal information with full knowledge regarding the types of information collected, understanding the purpose of collection, how the information may be shared, and how the information will be protected. The applicant understands the lack of successful identity proofing may result in denial of access to the installation.

2) COs designate authorized personnel to perform identity proofing. Delegation will be in writing, either by position designation codified in local guidance, or name.

(b) Identity Proofing at issue site

1) The following credentials are identity proofed at the card issue site from federally authorized identity documents, and shall be considered identity proofed.

a. Common Access Card.

b. Uniformed Services ID Card (TESLIN) issued to

military retirees and military family members.

c. Non-DoD Federal Personal Identification Verification (PIV). (Persons possessing Federal PIV credentials are vetted and adjudicated by government security specialists on a National Agency Check with Inquiries (NACI) or to the Office of Personal Management (OPM) Tier I standards.)

d. Transportation Worker Identification Credential (TWIC)

e. Personal Identity Verification-Interoperable (PIV-I) Credential. This credential is issued by DoD-approved PIV-I non-federal issuers that must meet the federal bridge certification to ensure their identity proofing standards are comparable to DoD standards, thus the PIV-I is considered identity proofed, and additional identity proofing is not required. Vetting and fitness determination is required in accordance with section 1205 of CNICINST 5530.14A.

f. Veteran Health Identification Card (VHIC)

(c) Biometrics. To biometrically authenticate enrollment into the system, the credential will be scanned and the fingerprint biometric captured utilizing the handheld device provided with the system.

(3) Once the vendor/contractor employee's identity has been validated and enrollment into the system biometrically authenticated, the credential is issued.

d. Permissible Access Methods.

(1) Common Access Card (CAC). Some contractors providing long-term services and requiring access to Navy Information Technology systems may be eligible for a CAC. Eligibility for CACs *is* significantly limited by law and regulation. See Paragraph 5 of this SOP for specific procedures and CAC eligibility.

e. Impermissible Access Methods. Credentials (not specified herein), that have previously or are currently produced and/or issued by Navy regions, installations, Navy tenant commands and/or other tenant organizations to vendors/contractors or other non-employees of the Department of the Navy (DoN) or the Department of Defense (DoD) are not valid for perimeter access to CNIC installations.

f. Sponsors. CNIC uses a methodology that involves Navy activities that "sponsor" contractors and vendors for issuance of either a DBIDS credential or a CAC.

(1) DBIDS Sponsoring Activities. A Navy Activity that desires to sponsor a vendor company for enrollment in DBIDS must be designated and approved as a SA by the AFC, normally the Force Protection/Physical Security Specialist or the VCC Supervisor. See Paragraph 3 of this document for specific procedures.

(2) DBIDS Single Source Coordinator. For vendors/contractors or companies having no specific relationship with a particular Navy activity , yet having a legitimate requirement for access (such as taxi, shuttle and limousine services), the AFC may designate a Navy activity that will serve as a Single Source Coordinator (SSC). A typical SSC might be Navy Exchange or Fleet and Family Support Center. See Paragraph 3 of this SOP for specific procedures.

(3) CAC Trusted Agents. A Navy activity that desires to sponsor a contractor employee seeking the issuance of a CAC must accomplish the application through an active duty military or civil service employee Trusted Agent (TA). TAs are approved and designated by the Trusted Agent Security Manager (TASM) under the applicable procedures of the Contractor Verification System (CVS). See Paragraph 5 of this SOP for specific procedures and CAC eligibility.

(4) Privilege of Sponsorship. Contractor and vendor sponsorship by SAs, SSCs and TAs is a privilege, not a right, and the Navy reserves the discretion to remove sponsorship at any time when in the best interests of the Government.

g. Service Contractor. CNIC will accomplish the DBIDS effort utilizing CNIC Visitor Control Center Staff.

h. Vetting/Screening Failure. If a vendor/contractor employee fails the background screening, the employee and their company are advised in writing. Listed below are specific conditions or offenses considered prejudicial to the good order, discipline and morale of the installation that may not be waived by the Commanding Officer (CO) or designated representative:

(a) Identified in the Foreign Fugitive File.

(b) Identified in the Immigration Violator File.

(c) Registered in the National Sex Offender Registry Database.

(d) Known or Appropriately Suspected Terrorist (KST) File

(e) Felony convictions for Rape, Child Molestation, Trafficking in Humans, Espionage, Sabotage, Treason, or Terrorism.

(f) Other Felony Convictions. Other than the disqualifiers listed above in paragraphs (a) through (e), any felony conviction within the past 10 years is grounds for denying installation access. COs may waive this requirement. Felony convictions more than 10 years old, except for those identified above do not require a waiver.

(g) Persons released from prison or on probation within five years after a felony conviction may apply for a waiver.

(h) Arrests for a disqualifying event without disposition (conviction, dismissal, not guilty or acquittal) more than 10 years old are not grounds for denying access.

(i) A waiver from the CO is required for persons identified in the Violent Person Crime File. The Violent Persons File lists individuals with a violent criminal history and persons who have previously threatened law enforcement.

(2) COs may deny access or access credentials based on information obtained during identity vetting such as Wanted Persons (active wants/warrants) which indicates the individual may present a threat to the good order, discipline and morale of the installation.

(3) Sex Offender. Sex offenders identified through the National or State Sex Offender Registry Databases are prohibited from accessing Navy installations and facilities.

i. Credential Issuance. Once a DBIDS participant is registered, screened, validated, approved and credentialed by the Navy, they are now eligible to access an installation. DBIDS credentials will be issued for the following timeframes:

(1) 0-179 days will be issued a DBIDS paper pass in no more than 30 day increments.

(2) Over 179 days will be issued a DBIDS card.

j. Expiration dates. DBIDS cards will now be issued with the following expiration dates:

(1) Employees who do not meet CAC requirements – Three years from issue date.

(2) Service Providers – Length of contract not to exceed three years from issue date.

(3) Unaffiliated PPV Housing Residents – Set to lease expiration date.

k. Validity. If the vendor/contractor employee passes the background screening process, the DBIDS credential that is issued to the vendor/contractor employee is valid for the term of the card. Periodic background screenings are conducted to verify continued DBIDS participation and installation access privileges. Background screening includes, but is not limited to:

(1) When a vendor/contractor employee first registers to participate in DBIDS.

(1) Daily wants and warrants check via NCIC

(2) When vendor/contractor registers for DBIDS renewal.

(3) At any time, upon request by the Region Commander, Region Security Officer (RSO), Installation Security Officer (SO) or the Commanding Officer.

l. Revocation. DBIDS access privileges will be immediately suspended or revoked if at any time a vendor or contractor employee becomes ineligible. Grounds for becoming ineligible and having access privileges suspended or revoked include, but are not limited to:

(1) A vendor or contractor employee no longer works for the company through which he/she enrolled.

(2) A vendor or contractor employee does not pass the background screening (initial, daily, on renewal)

(3) A vendor or contractor employee or company violates any DBIDS rules, terms or conditions.

(4) A vendor or contractor company requests their employee be removed from DBIDS.

(5) A vendor or contractor company is no longer eligible, ends their participation or no longer does business aboard the installation .

(6) At the direction of an RSO/ISO/CO.

m. Return of Credentials. Participating companies are required to immediately collect employee DBIDS credentials and notify the Service Contractor or the AFC in writing:

(1) That an employee has departed the company without having properly returned or surrendered their DBIDS credentials.

(2) That there is a reasonable basis to conclude that an employee, or former employee, might pose a risk, compromise, or threat to the safety or security of the installation or anyone therein.

n. Appeals. Appealing initial disqualification, suspension or revocation of participation in DBIDS.

(1) Any person being denied initial participation in DBIDS or who has their DBIDS privileges suspended or revoked for any reason, may appeal the denial/suspension/revocation.

(2) Vendor or contractor employees may initiate the adjudication process when a background screen failure results in disqualification from participation in DBIDS and the vendor or contractor employees do not agree with the reason for disqualification. The adjudication process must be initiated within 30 days of receiving written notice of disqualification.

(3) Vendor or contractor employees may apply for a waiver when a background screening failure results in disqualification from participation in DBIDS. The waiver process must be initiated within 60 days of receiving written notice of disqualification. Members on the Sexual Offenders Register will not be waived.

(a) All waiver requests will be initiated with the ISO. The CO will be the final waiver determination authority.

(b) The CO shall consult with the Installation Staff Judge Advocate when determining suitability.

o. Entry Control Point (ECP) Standards. On every ingress through a perimeter ECP, all DBIDS participants will present their credential. ECP personnel will scan the credential which will result in the verification of the credential, and grant of general access privileges and specific access profiles (time of day, day of week) for that installation. ECP personnel may biometrically authenticate (using a fingerprint scan} the person presenting the credential to ensure that this is the same person who registered into DBIDS. The following provides the procedures, roles, and responsibilities to successfully implement and execute the System:

(1) The participant presents their DBIDS credentials at the perimeter ECP to the sentry who will scan the credential utilizing the handheld device provided with the system.

(2) The handheld device will display a digital picture, the name of the DBIDS participant, and the company name with whom the participant is associated. This information will be checked against the local access control workstation to determine if the DBIDS participant has current access privileges and meets the specific access profile (day of week and time of day).

(3) If the system responds in the affirmative, and if in the opinion of the sentry the data matches the individual requesting access, AND no other mitigating safety and security factors are present, access to the installation may be granted.

(4) Generally, DBIDS participants will have access to all perimeter ECPs during all hours they are open, excluding vehicle size limitations and other physical ECP constraints. However, at credentialing the BSO or SSM, can limit and/or assign a specific ECP to be used.

(5) Other than for Random Anti-Terrorism Measures (RAM) or in the case of an elevation of Force Protection Conditions (FPCON) no vehicle inspection is required.

(6) If the identity of the individual requesting entry is in question, or in the case

of a RAM or elevated FPCON, a biometric (fingerprint) authentication will be made to confirm the individual is a DBIDS participant.

(7) If the biometric check authenticates the individual and access privileges are current, AND no other mitigating safety and security factors are present, access to the installation may be granted.

(8) RAMs and biometric validation of the DBIDS participants and their vehicles may also be conducted as deemed appropriate by the CO.

(9) DBIDS participants may not act as escorts for other person (s).

(10) Unaffiliated Civilians/Housing Occupants (sponsored by PPV Housing Office) over the age of 10 will be issued a DBIDS card and are authorized to sponsor individuals onto the installation they are affiliated with/assigned to, but sponsorship privileges will be limited to their particular housing area only.

(11) DBIDS participants are not authorized access to restricted areas unless they have their DBIDS credential and are authorized access (and as locally required) for the restricted area. DBIDS participants may also be required to present a Commercial Bill of Lading or Government Bill of Lading when access to restricted areas is required.

p. Taxi, Limousine and Shuttle Access. Access procedures and standards for taxis, limousines and shuttle services will be governed by:

(1) At the election of the CO, under the process and procedures outlined in CNICINST 5530 .l4A. In the event this process is made available to taxis, limousines and shuttles, the CO must ensure compliance with all of the standards of those laws and regulations found at Appendix B of this SOP. Until these standards can be adhered to, paper passes will be limited in duration to one day.

4. DBIDS Paper Passes. In the event that a visitor, vendor, or contractor employee elects not to participate in DBIDS, or is ineligible to receive a CAC, the individual will be issued DBIDS paper pass in order to access to the installation.

a. Minimum Standards. Installations procedures in issuing paper passes will comport with the provisions of Federal, DOD, Navy, and CNIC guidance, and will ensure, at a minimum:

(1) Processing must occur at the Visitor Control Center under local and higher directive procedures.

(2) The vetting of personal identification information and background checks should include, but is not limited to:

(a) National Crime Information Center (NCIC) "Persons Files" and Interstate Identification Index (III)

(b) The requirements set forth in OPNAVINST 1752.3, Policy for Sex Offender Tracking, Assignment, and Access Restrictions within the Navy of 27 May 2009 and CNICINST 1752.1, Policy for Sex Offender Tracking, Assignment, and Installation Access Restriction s of 7 February 2011.

(c) NCIC National Sex Offender Registry (NSOR).

(d) Terrorist Screening Database (TSDB).

(e) DOJ National Sex Offender Public Website (NSOPW)

(f) Additional checks as required by current, revised, or newly issued federal directives, DoD policy, DoN Policy or CNIC Directives.

b. Time Limitation. The CO has the authority to permit access to the Installation, together with the responsibility to ensure that permitted access comports with applicable law, regulation, and policy. Accordingly, the following guidance is provided:

(1) The enterprise-wide time standard for the validity of a pass to access an installation will be not more than thirty (30) days.

(2) If a CO identifies a need to issue passes that exceed the enterprise-wide time standard, the Installation SOP will identify the basis and rationale for the time period of passes issued. Factors such as security posture, resources for monitoring, high-risk assets, and related considerations must be considered and addressed.

(3) Periods of validity for passes may be curtailed or restricted in the future by Federal, DOD, Navy, and CNIC guidance.

c. Local Standard Operating Procedures (SOP). As stated elsewhere in this document, installations will issue local SOPs implementing this guidance.

(1) Proposed installation SOPs will be submitted to the Regional Commander for review and approval. An information copy of all Installation SOPs will be furnished to Headquarters CNIC N3AT.

(2) The SOPs will include detailed standards and procedures for the application, issuance, and the authentication of passes.

5. Common Access Cards (CAC). In most cases, general vendors/contractors are not eligible for a CAC. A CAC is not appropriate for vendor/contractor employees who provide temporary services; who are hired for short-term (less than six months) ; who merely deliver goods or supplies to Navy installations; or who are employed to provide goods or services wholly

ancillary to the core Navy missions (such as workers at an on-base concession store/snack bar). Only those individual contractors who have a legitimate basis for requesting a CAC, such as embedded (co- located) advisory and assistance contractors; contractors having long-term and routine access to multiple installations to support core Navy functions; contractors performing duties requiring access to Navy Information Technology systems (e .g., the Navy Marine Corps Internet [NMCI]); and contractors performing under Statements of Work (SOWs) and Performance Work Statements that properly and legitimately identify their personnel as qualified for a CAC will be considered eligible. For this purpose, entitlement to a CAC will require a need for both physical access to a Navy installation or facility AND logical access to NMCI.

6. Responsibilities.

a. Enrollment and registration into DBIDS is the sole responsibility of the vendor or contractor company.

b. Installations will issue written guidance, implementing local SOPs that articulate the specific provisions and requirements of the project. This SOP may be supplemented by Installations to the extent that it does not conflict or give authority beyond the guidelines established in the SOP, federal law and DoD/DON policy. All Installation supplements must be approved by the parent Navy Region.

c. COs have the authority over, and responsibility for, the safety and security of an installation. While discretion is vested in the authority of the CO, compliance with all legal requirements must be adhered to, and deviation from the guidance of this SOP must be subject to careful consideration.

d. Installations will identify an Approved Facility Contact (AFC). Responsibilities may include, but are not limited to, providing an Approved Company List (ACL), identifying the DBIDS sponsor(s), coordinating command, installation and tenant sponsor briefings, coordinate guard/police training, development of SOPs for implementation of DBIDS installation access.

e. Tenant organizations will provide an ACL, identify DBIDS sponsor(s), and ensure updates to both.

Appendix A

List of Applicable Authorities

- HSPD-12, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

- DTM-09-12, Directive Type Memorandum, Interim Policy Guidance for DoD Physical Access Control

- FIPS-201-2, Federal Information Processing Standards, Personal Identity Verification of Federal Employees and Contractors

- Public Law 110-181 (FY 2008) Section 1069, Standards for Entry to Military Installations in the United States

- OPNAVINST 1752 .3, Policy for Sex Offender Tracking, Assignment and Access Restrictions within the Navy

- CNICINST 1752.1, Policy for Sex Offender Tracking, Assignment, and Installation Access Restrictions

- CNICINST 5530.14A, CH-2, Chapter 12, Commander Navy Installations Command Ashore Protection Program

- DBIDS User Manual, Release 4.1.21