PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Biometric Automated Access Control System (BAACS)

2. DOD COMPONENT NAME:

Department of the Navy/United States Marine Corps

Marine Corps Installation Command (MCICOM)

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The purpose of this system is to enhance identity management of DoD Persons and streamline business functions through a physcial access control system database for designated populations. The following functions are the key processes supported by this system:

To support the DoD physical security, force protection, identity management and access control missions by identifying and/or verifying an individual through the use of a database for designated populations for purposes of protecting U.S./Coalition/allied government/national security areas of responsibility and information.

To provide personnel identification and verification capabilities during disaster scenarios or other catastrophic events.

To detect fraudulent identification cards, the issuance of security alerts for debarred, suspended, missing or wanted persons, known or suspected terrorist and registered sex offenders.

The United States Marine Corps (USMC) augments security forces who support physical access control procedures for gaining access to USMC installations, through implementation of an electronic identity authentication system. The necessity exists to collect Personally Identifiable Information (PII) from participating DOD personnel, contractors and other public persons who are seeking access to a USMC installation and/or its facilities.

The system, referred to as the Biometric and Automated Access Control System, is to be used by DOD Active Duty, DOD Retirees, DOD Civilians, DOD contractors and visitors/VIPs.

The system is owned and operated by the Marine Corps Installation Command (MCICOM), who furnishes the Commercial off the shelf (COTS) hardware and software for the system. The USMC host installation's Provost Marshal's Office, is responsible for collecting, storing and protecting PII of personnel who enroll for the system. The Provost Marshal's Office enrolls the PII in the BAACS and the system is used to electronically authenticate the identity of personnel who are seeking access to USMC installations and facilities. MCICOM and the host USMC installation's Provost Marshal's Office shares no PII beyond the authority (statutory or otherwise) specified in this document.

Participation in the system is voluntary. However, individual USMC installation commands have the authority to identify groups of personnel that may be required to use the system.

The system supports four functions: (1) Enrollment, (2) Credentialing, (3) Physical Access Control, and (4) Security Alert Notification.

Currently the system has been deployed at USMC installations across the Continental United States (CONUS) and Outside CONUS.

Types of personal information collected:

Name, SSN, Driver's license, DoD ID Number, Foreign National ID, Citizenship, Gender, Race/Ethnicity, Birth Date, Place of Birth, Home Telephone Number, Mailing/Home Address, Biometrics, Law Enforcement Information, Employment Information.

The USMC Provost Marshal's Office collects certain biographic and biometric information directly from active duty or retired DOD service members, their dependents, DOD civilians and contractors as well as visitors and vendors. The USMC PMO uses this information to manage and provide the physical access control to the installation, electronic identity authentication and background screenings.

In addition, during the enrollment process, the installation requires that individuals who do not hold a CAC or DD Form 2 or DD Form 1173 card (i.e. non-DOD persons, visitors) must present acceptable identity proofing documentation as specified on SECNAV 5512/1 per OMB 0703-0061 to verify identity. The USMC Installation's Provost Marshal's Office reviews and does not scan or store copies of these identification documents.

Biometric information collected by the USMC Provost Marshal's Office consists of the following:
• Digital photograph of face
• Digital fingerprint images
• Digital Vascular Pattern images of hand(s)
• Digital Iris images
• For all biometric information collected, images are collected and converted to template format, and then the templates are stored in the system. No images are stored in the system.

** The USMC Provost Marshal's Office may also collect from the person, their Social Security Number, however, this collection may not be required if the forms of identification are deemed satisfactory or if the person has an existing DOD Common Access Card (CAC) or DD Form 2 or DD Form 1173 that is verifiable via either the DOD Defense National Visitor Center (DNVC) or the DOD Identity Matching Engine for Security & Analysis (IMESA). Persons are not eligible to use the system if they do not provide the required information. The host USMC installation's Commander and Provost Marshal's Office has sole authority for granting or denying the person access to use the system or to access the installation via an alternative process.

Social Security Number (SSN) – The data collected as part of the enrollment into the BAACS is the basis for the Local Installation Commander making a decision to grant or deny access to his/her installation. This access control decision will include the completion of a query of the National Crime Information Center (NCIC) database, the Terrorist Screening Database (TSDB), and/or State/Local Criminal Justice Information Systems as a separate process external to BAACS. This query is completed based on submittal of the First and Last Name, Date of Birth, gender, SSN and/or Driver's License Number as primary query fields.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The PII is being collected to enter data into a database and retrieve that data for verification, identification and authentication to control physical access to DOD, DON or United States Marine Corps installations/units controlled information, installations, facilities, or areas over which the DOD, DON or United States Marine Corps has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./ Coalition/allied government/ national security areas of responsibility and information; to issue badges, replace lost badges and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit of personnel.

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Persons initiate the collection and maintenance of their PII when they enroll with the local installation's USMC Provost Marshal's office access control registrar to use the system.

Before information is collected, the individual is provided the opportunity to read the Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), thereby affording the individual to make an informed decision about providing the data.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [X] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Information is only used for the purpose already consented to by the individual at the time of collection. Information is not used for other

purposes. If individual persons are authorized to consent to specific uses of their PII, the USMC's cannot protect the buildings, grounds, and property that are owned or occupied by the USMC and/or other DOD or federal agencies or ensure the safety and security of personnel and assets within such property.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

SECNAV 5512/1 DEPARTMENT OF THE NAVY LOCAL POPULATION ID CARD/BASE ACCESS PASS REGISTRATION, OMB 0703-0061, paper form.
PRIVACY ACT STATEMENT:
AUTHORITY: 10 U.S.C. 113, Secretary of Defense; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); DoDM 5200.08 Volume 3 Physical Security Program: Access to DoD Installations; DoDI 5525.19 DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Database (TSDB) ; and E.O. 9397 (SSN), as amended; OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program; Marine Corps Order 5530.14, Marine Corps Physical Security Program Manual; SORN NM05512-2 Badge and Access Control System Records; SORN DMDC 16, Identity Management Engine for Security and Analysis (IMESA): http://dpcld.defense.gov/Privacy/SORNsIndex
PURPOSE(S): To control physical access to Department of Defense (DoD), Department of the Navy (DON) or U.S. Marine Corps Installations/Units controlled information, installations, facilities, or areas over which DoD, DON, or U.S. Marine Corps has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./Coalition/allied government/national security areas of responsibility and information; to issue badges, replace lost badges, and retrieve passes upon separation; to maintain visitor statistics; collect information to adjudicate access to facility; and track the entry/exit times of personnel.
ROUTINE USE(S): To designated contractors, Federal agencies, and foreign governments for the purpose of granting Navy officials access to their facility.
DISCLOSURE: Providing registration information is voluntary. Failure to provide requested information may result in denial of access to benefits, privileges, and DoD installations, facilities and buildings.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	The USMC Provost Marshal's Office regularly provides to the host installation's USMC Provost Marshal's Office access control manager representative, PII that consists of the person's name and the date, time and location reflecting that the individual has utilized the system to gain access to the USMC installation.
☐ Other DoD Components	Specify.	US Army, US Air Force, US Navy, DOD OSD Defense Manpower Data Center, Defense Logistics Agency, Pentagon Force Protection Agency
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	KBRWyle Technology Solutions, LLC (under Contract N00178-14-D-7748/N6523617F3131) includes 52.224-1 and 52.224-2 clauses. A contract modification is being initiated to add FAR 39.105.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☐ Other Federal Information Systems

For DOD persons who possess a DOD CAC or DD Form 2 or DD Form 1173, the PII is collected in person, directly as a result of the person presenting one of the above forms of ID and electronic authentication against the DOD authoritative data source (i.e. IMESA).

For non-DOD persons (those who do not possess a DOD CAC or DD Form 2 or DD Form 1173), the PII is collected directly from the individual who appears in person at the USMC registration facilities and who cooperatively completes the SECNAV 5512/1 Department of

the Navy Local Population ID Card/Base Access Pass Registration form and submits it to the local installation's USMC Provost Marshal's Office registrar.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [ ] Information Sharing - System to System
- [ ] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

SECNAV 5512/1 DEPARTMENT OF THE NAVY LOCAL POPULATION ID CARD/BASE ACCESS PASS REGISTRATION, OMB 0703-0061, paper form.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

[x] Yes [ ] No

If "Yes," enter SORN System Identifier NM05512–2; DMDC 16 DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-NU-2015-0005

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Badges and passes are destroyed three months after return to the issuing office. Records and issuance are destroyed six months after a new accountability system is established or one year after final disposition of each issuance record is entered in retention log or similar record, whichever is earlier. Visit request records are destroyed two years after final entry or two years after date of document, whichever is later. Collection forms, paper and/or plastic badges/passes are shredded or incinerated using DOD approved procedures. If any IT system or data storage media fails and must be replaced, the data storage component (e. g. hard drive) is removed from the hardware and degaussed with DOD approved degaussing systems and are then mechanically destroyed prior to disposal.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

SORN NM05512-2 Authorities:
Badge and Access Control System records (April 09, 2014, 70 FR 19593)

10 U.S.C. 5013; Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; OPNAVINST 5530.14E, Navy Physical Security and law Enforcement program; Marine Corps Order 5530.14A, Marine Corps Physical Security Program Manual; and E.O. 9397 (SSN), as amended.

SORN DMDC 16 DoD Authorities:
Identity Management Engine for Security and Analysis (IMESA) (December 21, 2015, 80 FR 79310)

10 U.S.C. 113, Secretary of Defense; DoDD 1000.25 DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; E.O. 9397 (SSN), as amended.

Other Authorities:
E.O. 12333; United States Intelligence Activities;
E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;
National Defense Authorization Act of 2008, Section 1069;
DoDD 8521.01E, Department of Defense Biometrics;
DoDD 8500.1, Information Assurance;
DoDI 5525.19 DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Database (TSDB) (supersedes OUSD DTM 14-005);
DoDM 5200.08 Volume 3 Physical Security Program: Access to DoD Installations (supersedes OUSD DTM 09-012);
AR 25-2, Information Assurance;
SSN USE REVIEW AND JUSTIFICATION FOR FORMS, Memorandum for the Record, dated MM/DD/YYYY.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ Yes ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0703-0061
Expires 31 JAN 2021 (in process of renewal at the time this PIA was drafted)

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[ ] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[X] Driver's License	[ ] Education Information	[ ] Emergency Contact
[ ] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[X] Law Enforcement Information	[ ] Legal Status
[X] Mailing/Home Address	[ ] Marital Status	[ ] Medical Information
[ ] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[ ] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[ ] Passport Information	[ ] Personal E-mail Address	[X] Photo
[X] Place of Birth	[X] Position/Title	[ ] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[ ] Records	[ ] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[X] If Other, enter the information in the box below	

Identifying information including, Foreign national ID, DOD assigned Local Population EDI PI unique identifier, physical features (hair color, eye color, height, weight).

Biometrics: Digital photograph of face, Digital fingerprint images, Digital Vascular Pattern images of hand(s), Digital Iris images.

Law Enforcement Information: The system allows authorized USMC security officials to flag individual registration records with security alerts in the form of Debarment, Suspension, Revocation, Be-on-Lookout, or National Crime Information Center felony Wants/Warrnts for individual persons. Due to the sensitivity and statutory restrictions on recording and disclosure of some law enforcement data, that information is retained in separate authoritative law enforcement systems, such as the National Crime Information Center (NCIC) or the DON Criminal Law Enforcement Operations Combined (CLEOC) system or other DoD Criminal Justice information Systems. BAACS only stores a unique identifier reference record that is used by Base Security officials to perform external criminal justice system record checks within the separate authoritative law enforcement system(s), therefore, the law enforcement data is not redundant in BAACS.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Acceptable Use Criteria for Systems Collecting SSNs established in DODI 1000.30, August 1, 2012:
Law Enforcement, National Security and Credentialing: Almost every law enforcement application must be able to report and track individuals through the use of the SSN. This includes, but is not limited to, checks of the National Crime Information Center, state criminal histories and Federal Bureau of Investigation records checks.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

The SSN is provided by the individual who enters it on the SECNAV 5512/1 paper form and hand delivers the form to the local installation USMC Provost Marshal's Office access control registrar, who uses the information for the purposes cited in section 1.c above. The local installation Provost Marshal's Office access control registrar securely stores all SECNAV 5512/1 paper forms per the retention specified in SORN NM05512–2. The SSN is not re-printed on or copied to any other paper form(s), reports or DoD identification cards or passes.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

There is no planned or scheduled date for either the substitution or elimination of the SSN from the SECNAV 5512/1 or the BAACS collection instruments. The DoD enterprise level authoritative data sources and the federal law enforcement data sources utilize the SSN, and must first be addressed before the SECNAV 5512/1 form or the BAACS can be updated to align business practices and information exchange with any new identifier that may be used as a SSN substitute or replacement at the DoD enterprise level.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☐ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☐ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☒ If Other, enter the information in the box below

Each local installation USMC Provost Marshal's Office will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

The Physical Access Control System controls access to USMC Data Center facility/equipment rooms.
The Intrusion Detection System (i.e. the Data Center Alarm System) secures the USMC Data Center facility/equipment rooms.
All PACS and IDS electronic equipment and IT system cabinets are physically secured with a lock as well as tamper alarm circuits that report to the Intrusion Detection System.

(2) Administrative Controls. *(Check all that apply)*

- ☐ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☒ If Other, enter the information in the box below

Backups are securely stored on-site at the same USMC installation, but at a separate location/facility.

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☐ Firewall
- ☐ Role-Based Access Controls
- ☐ Virtual Private Network (VPN)
- ☐ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☐ Used Only for Privileged (Elevated Roles)
- ☐ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☒ External Certificate Authority Certificates
- ☐ Least Privilege Access
- ☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

1. Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
2. Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

3. Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
4. Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
5. Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.