PRIVACY IMPACT ASSESSMENT (PIA)

For the

RAPIDGATE (RIS)
Department of Navy - CNIC

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	DITPR ID: 14399 DITPR DON ID: 22244
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI UII: 007-000003024

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier NM05512-2

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number 0703-0061

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

SORN authorities:

10 U.S.C. 5013, Secretary of the Navy
U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14C, Navy Physical Security
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual
E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

The United States Navy ("Navy") and United States Marine Corps ("Marine Corps") have added layers of security to their identity management and physical access control procedures for granting access to Navy and Marine Corps installations, through the use of commercial services. The services are directed at (a) persons who register for services covered by the RAPIDGate Information System, or Services-Registered Persons (SRPs), consisting of vendors, suppliers, certain contractors, service providers, and frequent/long-term visitors, and (b) persons who do not register for services covered by the RAPIDGate Information System, or non-Services-Registered Persons (non-SRPs), consisting active military personnel, military dependents, guests, military retirees, civilian personnel, and occasional/short-term visitors. Features vary, but both types of services involve the collection of Personally Identifiable Information (PII) from individuals. All of the PII collected falls within the RAPIDGate Information System.

Certain sections, paragraphs, and phrases within this Privacy Impact Assessment ("PIA") apply to both Navy and Marine Corps, but certain sections, paragraphs, and phrases of this PIA apply to the Marine Corps only. When a section, paragraph, or phrase applies to the Marine Corps only, the phrase "USMC Only" will be placed in bold font within brackets at the beginning of that section, paragraph, or phrase. If "[USMC Only]" does not appear before a section, paragraph, or phrase, that section, paragraph, or phrase applies to both Navy and Marine Corps.

The SRP and Non-SRP services are furnished by a third party service provider (Service Provider). The Service Provider furnishes its own hardware and software. (Note: The Service Provider does not supply handheld computers or Guard Stations to the Navy as part of the services.) Its equipment is stand-alone and is not connected to any government network. However, it may utilize installation telephony services. The Service Provider is responsible for collecting, storing and protecting PII. The Service Provider uses the PII to operate the services. It shares limited PII collected from SRPs and from non-SRPs (DL holders only) with the Navy or Marine Corps installation associated with the PII collection.

No Navy installations use Service Provider's non-SRP services. Some, but not all, Marine Corps installations use Service Provider's non-SRP services. When this PIA discusses non-SRP services provided to the Marine Corps, it is referring only to those Marine Corps installations that have elected to make use of Service Provider's non-SRP services.

1. SRP services

The SRP services are offered on an optional basis to individuals, typically employed by companies and organizations sponsored by the installation, who desire expedited, more convenient entry to the installation. For example, an electrician who needs regular access to a Marine Corps installation for work on a building may consider utilizing the SRP services. Or, a vending machine supplier who regularly accesses Navy buildings to replenish vending machines may apply for the SRP services so that each visit to the base is not slowed by waiting in the visitor's lane or by a check-in process.

SRP participation is voluntary. However, Navy and Marine Corps installations have the authority to identify groups that may be required to process through SRP services due to previously established security risk. Persons who wish to participate register at a registration kiosk, called a Registration Station, located at the base's Visitor Center. The Registration Station contains a keyboard, CPU, monitor, camera and fingerprint reader. Individuals begin the registration process by typing in the unique PIN number for their company, organization or sponsor. Individuals then input the following biographic and biometric information:

- Full legal name
- Current residence address
- Date of birth
- Whether the individual is a U.S. citizen or U.S. national
- Mother's maiden name
- Email address

• Social security number (providing the social security number is voluntary, but failure to do so will prevent completion of the registration, performance of the background screening and manufacturing of the Vendor credential)
• Digital photograph of face
• Digital fingerprint images (four prints -- two fingers of both hands – are collected; the system is capable of collecting additional fingerprints - up to a full set of 10 fingerprints.)
• Credit card number and expiration date (for the individual's credit card, or for the company's or organization's credit card)
• Billing address

The collected PII is used to conduct background screenings (security threat assessments) on the individuals, where applicable; to verify their claimed identity; to manufacture an SRP credential that is used to verify their identity of and verify their eligibility to participate in the SRP service; to prepare aggregated statistical reports to Navy and Marine Corps installations on the total number of enrolled participating companies/organizations, registered individuals and the total number of background screening fails, passes and successful adjudications (the statistical reports contain no PII); to provide installation security personnel with limited PII on individuals addressing who has passed and who has failed the background screenings, thereby enhancing the installation's ability to detect and deter potential threats to the security of personnel and property; and to assist in the management of records and background screenings. The installation also may use PII for investigative, program eligibility and related purposes.

[USMC Only] At Access Control Points (ACPs), a local Guard Station server (Guard Station) is housed. The Guard Station is housed in a locked metal enclosure, which is housed inside the guard shack/booth at the ACP; SRP credentials are electronically scanned for authentication and access privileges against RIS' authoritative data repository using a handheld mobile computer. PII is not stored on the handheld device. The PII is stored on the local Guard Station server (Guard Station) pursuant to U.S. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) encryption controls.

2. Non-SRP services

[USMC Only] The non-SRP services are utilized for identity management and access control of individuals who are not registered in the RAPIDGate Information System and who seek entry to the installation. Upon arrival at an installations' Access Control Point (ACP), such individuals must present to guard personnel their state-issued driver's license/i.d. (collectively DLs), or their Common Access Card (CAC card) if a military employee, or their Teslin card if a military retiree or dependent. Guard personnel, using the same portable hand-held computer device that is used to scan the system credentials of SRPs, electronically scan the i.d., and electronically "read" certain information from the magnetic stripe or PDF-417 barcode on the i.d. The read information is compared against data lists to search for any disqualifying matches.

[USMC Only] Collection of individuals' PII varies somewhat depending upon the type of identity credential presented by the individual for entry.

a. DLs
[USMC Only] The following biographic information is electronically read from DLs and displayed temporarily on the handheld device for guard personnel to review:

• First name
• Middle name
• Last name
• Date of birth
• DL expiration date
• Official DL number
• Issuer of the DL. (i.e., the issuing state)

[USMC Only] This read information is not stored on the handheld device. The read information is stored on the local Guard Station server (Guard Station) pursuant to DIACAP encryption controls. The Guard Station is housed in a locked metal enclosure, which is housed inside the guard shack/booth at the ACP. The RAPIDGate Information System stores the following PII and non-PII information that is electronically read from or generated by the electronic reading of the DL:

• Credential type (i.e., DL)
• DL expiration date
• Official DL number (18 or over only)
• Issuer of the DL
• Minor Flag (flag indicates if person is under the age of 18, based upon the date of birth and date of scan)
• First name (18 or over only)
• Middle name (18 or over only)
• Last name (18 or over only)
• Name prefix (18 or over only)
• Name suffix (18 or over only)
• Expired flag (flag indicating if credential is expired (at scan time))
• Suspect field Name (the name of any field that contained suspect data (i.e., DOB, Expiration Date))
• Suspect field reason (the reason a field was deemed suspect (i.e., missing information, format error, etc.))
• List name (the name of the list the credential matched against, if any (i.e., FBI's Ten Most Wanted)
• List match algorithm (if the credential matched against a list, what was used to identify the match (i.e., first/middle/last name/DOB match)
• Number of bytes scanned (The number of bytes returned from the Magnetic Stripe Reader (MSR) or barcode)
• Handheld i.d.
• Data scan method (barcode or MSR)
• Scan time
• Action taken (approve or deny)
• Action time (date and time that approve or deny was selected)

[USMC Only] The stored DL information is used for service management and to prepare aggregated statistical reports to Marine Corps installations on the total number of non-SRPs who are recorded as seeking installation entry (the statistical reports contain no PII). The installation may also use non-SRP PII collected from DLs for investigative, program eligibility and related purposes.

b. CAC Cards and Teslin Cards
[USMC Only] The following biographic information is electronically read from CAC cards and displayed temporarily on the handheld device for guard personnel to review:

• Branch (Army, Navy, NOAA, etc.)
• Rank
• First name
• Middle name
• Last name
• Date of birth
• Credential expiration date
• Document I.D. (EDIPI – Electronic Document Identifier Person Identifier, and/or the FASC-N - Federal Agency Smart Credential Number)

[USMC Only] The following biographic information is electronically read from Teslin cards and displayed temporarily on the handheld device for guard personnel to review:

• Branch
• Rank and if the person is a dependent
• First name
• Middle name
• Last name
• Date of birth
• Credential expiration date
• Credential i.d. (PDI – Person Designator Identifier)

[USMC Only] No read information from the CAC card or the Teslin card, either PII or non-PII, is stored on the handheld device. Moreover, no PII from the CAC card or the Teslin card is stored on the Guard Station or the RAPIDGate System. The RAPIDGate System stores non-PII information that is electronically read from or generated by the electronic reading of the CAC card or the Teslin card, up to and including the following:

• Credential type (i.e., CAC or Teslin card)
• FASC-N - Federal Agency Smart Credential Number
• Credential expiration Date
• Expired flag (flag indicating if credential is expired (at scan time))
• Suspect field Name (the name of any field that contained suspect data (i.e., DOB, Expiration Date))
• Suspect field reason (the reason a field was deemed suspect (i.e., missing information, format error, etc.))
• List name (the name of the list the credential matched against, if any (i.e., FBI's Ten Most Wanted))
• List match algorithm (if the credential matched against a list, what was used to identify the match (i.e., first/middle/last name/DOB match))
• Number of bytes scanned (The number of bytes returned from the MSR or barcode)
• Handheld i.d.
• Data scan method (barcode or MSR)
• Scan time
• Action taken (approve or deny)
• Action time (date and time that approve or deny was selected)

[USMC Only] The stored CAC card and Teslin card information is used for service management and to prepare aggregated statistical reports to Marine Corps installations on the total number of non-SRPs who are recorded as seeking installation entry (the statistical reports contain no PII).

c. Transportation Worker Identification Credential (TWIC) – Optional feature

[USMC Only] For TWICs, the information captured and displayed depends on the configuration.

[USMC Only] In TWIC QTL Mode with no pin verification the following data is captured:
• FASC-N
• Card Authentication Key Certificate
• Cardholder's fingerprint templates

[USMC Only] None of the PII is displayed on the handheld. The card's fingerprint templates are only used for comparison with templates generated from live fingerprints and are not stored. The only thing displayed is the resulting validation status of the card. The only data that is stored in the FASC-N, the card certificate's issuer, and the expiration date of the card.

[USMC Only] With pin verification configured, the following data is captured:
• FASC-N
• Card Authentication Key Certificate
• Cardholder's photo from the TWIC
• Cardholder's fingerprint templates

[USMC Only] The only PII displayed on the handheld is the cardholder's photo, but only if fingerprint verification is initiated, as well as the non-PII validation status of the card. The card's fingerprint templates are only used for comparison with templates generated from live fingerprints and are not stored. The only data that is stored is the FASC-N and the card certificate's issuer, and the expiration date of the card.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. Appropriate safeguards are in place for the collection, use and safeguarding of information.

The SRP Registration Station is owned, maintained, and controlled by the Service Provider. The Service Provider places its Registration Station at a convenient location at the installation, typically in the Visitor's Center. However, the data center that contains collected data is not under the direct physical control of the Navy or Marine Corps. The data center is housed in a secured location, compliant to MAC II Information Assurance Controls, by the Service Provider in Hillsboro, Oregon. This risk is addressed since the Service Provider currently provides the installations

with certain rights of control of biometric and associated data.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. The PII will be shared within the Navy and Marine Corps, specifically with personnel who have responsibility for identity management, access control, antiterrorism/force protection and law enforcement.

☒ **Other DoD Components.**

Specify. Department of the Navy, Air Force, Army, Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Manpower Data Center, Defense Security Service, National Guard Bureau, Office of the DoD Inspector General, Office of the Secretary of Defense, Office of the Secretary of Defense Personnel and Readiness, U.S. Military Entrance Processing Command, the Department of Homeland Security, and any other Component with express permission from the U.S. Marine Corps.

☒ **Other Federal Agencies.**

Specify. Office of Personnel Management, Federal Bureau of Investigation, Department of Veterans Affairs, Department of Homeland Security, Department of Justice, Department of Health and Human Services, Federal law enforcement and confinement/correctional agencies, Department of the Treasury, the Social Security Administration, and any other Federal agencies with express permission from the Navy or Marine Corps including those covered by the "DoD Blanket Routine Uses" SORN (http://privacy.defense.gov/blanket_uses.shtml).

☒ **State and Local Agencies.**

Specify. All state and local law enforcement agencies with express permission from the Navy or Marine Corps.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. PII is collected, used and stored by the Service Provider. The current Service Provider is Eid Passport, Inc. The Navy and Marine Corps require the Service Provider to safeguard PII and to comply with privacy laws and regulations such as the Privacy Act of 1974 and DoD Directive 5400.11-R, DoD Privacy Program and the two FAR Privacy Clauses.

☒ **Other** (e.g., commercial providers, colleges).

Specify. SRP PII is shared with the Service Provider's third-party service providers ("Commercial Providers") to conduct background screenings.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

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

Individuals who desire to register for SRP services initiate the collection and maintenance of their PII when they register with the Service Provider at the Registration Station. The SRP services are STRICTLY voluntary. If an individual decides not to participate, the individual can either exit the entry lane and leave without entering the Navy or Marine Corps base, or undergo alternate access procedures such as obtaining a day pass. The individual must have a valid government-issued i.d. (i.e., DL, CAC card or Teslin card), vehicle registration, and insurance that may be presented prior to the vehicle inspection. The individual may be required to present his/her government-issued i.d. for electronic scanning and "reading" under the identity management and access control procedures applicable to non-SRPs.

A comprehensive written notice is provided to, and is required to be read by, individuals at the time of registration for SRP services. The notice explains what information is being collected, why it is being collected and what uses will be made of the information. The written notice is in the form of a User Agreement that is displayed on the Service Provider's registration kiosk screen early in the registration process. SRPs are required to read the User Agreement in its entirety and to consent to its terms, in order to proceed with registration. SRPs must click an "I accept" button to affirm their consent to the terms of the User Agreement. After giving this consent, the registration screen displays the information fields for the SRP to type in his/her information.

[USMC Only] Non-SRPs initiate the collection and maintenance of their PII when they arrive at a Marine Corps installation ACP and seek entry. Each installation is responsible for providing a notice to the non-SRP population. Notice typically is provided to non-SRPs in the form of signage posted conspicuously at or near the ACP.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

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

Individuals registering for SRP services must read the User Agreement, which informs them that, if they do not agree to all terms, which include collection and use of their individual information, they should select the "I do not agree to the terms" button and "quit" from the registration process. Individuals registering for SRP services do not have the right to selectively consent to provide some, but not all, of the individual information they are required to provide in order to register for the service.

[USMC Only] Non-SRPs have the opportunity to consent to the use of their PII by proceeding with entry protocol. If they do not agree to the terms, they can exit the entry lane and depart without entering the Marine Corps installation. Non-SRPs cannot selectively consent to provide some, but not all, of the individual information they are required to provide in order to enter the Marine Corps installation.

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

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

A Privacy Act Statement is provided to, and is required to be read by, individuals registering for SRP services at the time of registration. The notice explains what information is being collected, why it is being collected and what uses will be made of the information. The written notice is in the form of a User Agreement that is displayed on the Service Provider's registration kiosk screen early in the registration process. Individuals are required to read the User Agreement in its entirety and to consent to its terms, in order to proceed with registration. Individuals must click an “I accept” button to affirm their consent to the terms of the User Agreement. After giving this consent, the registration screen displays the information fields for the individual to type in his/her information.

[USMC Only] Non-SRPs initiate the collection and maintenance of their PII when they arrive at a Marine Corps installation ACP and seek entry. Each installation is responsible for providing a Privacy Act notice. Notice typically is provided in the form of signage posted conspicuously at or near the ACP.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.