



PRIVACY IMPACT ASSESSMENT (PIA)

For the

RAPIDGate/Rapid-RCx

Department of The Army Directorate of Emergency Services

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
- 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

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

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

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.

10 U.S.C. 3013, Secretary of the Army; Army Regulation 190-13, The Army Physical Security Program and 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 Army is adding layers of security to its identity management and physical access control procedures for granting access to Army installations, through the use of a contract for commercial services. The services are directed at Vendors and non-Vendors, i.e., visitors, active military personnel, military dependents, guests, military retirees and civilian personnel. Features vary, but both services involve the collection of Personally Identifiable Information (PII) from individuals. All of the PII collected falls within the RAPIDGate Information System.

Vendor participation is voluntary. However, Army installations have the authority to identify groups that may be required to process through the Vendor service due to previously established security risk. Vendors who wish to participate register at a registration kiosk, called a Registration Station, located at the base's Visitor Center. The Registration Station is a sit-down station with semi-enclosed sides for privacy. It contains a keyboard, camera and fingerprint reader. Vendors begin the registration process by typing in their Vendor Company's unique PIN number. Vendors then input the following biographic and biometric information.

The collected PII is used to conduct background screenings (security threat assessments) on individuals to verify their claimed identity; to manufacture credentials used to verify their identity; to prepare aggregated statistical reports to Army installations on the total number of enrolled Participant Vendor Companies and their registered employees 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 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 Vendor records and background screenings. The installation may also use Vendor PII for investigative purposes.

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. The Guard Station is housed in a locked metal enclosure, which is housed inside the guard shack/booth at the ACP.

The stored DL information is used for service management and to prepare aggregated statistical reports to Army installations on the total number of non-Vendors who are recorded as seeking installation entry (the statistical reports contain no PII). The installation may also use non-Vendor PII collected from DLs for investigative purposes.

The Vendor and Non-Vendor services are furnished by a third party service provider (Service Provider). The Service Provider furnishes its own hardware and software. 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 Vendors and from non-Vendors (DL holders only) with the Army installation associated with the PII collection.

(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 Vendor 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 U.S. Army. The data center is housed by the Service Provider in Portland, Oregon. This risk is addressed since the Service Provider currently provides the installation with right of ownership and dual-control to biometric and associated data.

[Empty rectangular box]

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 U.S. Army, specifically with personnel who have responsibility for identity management, access control, antiterrorism/force protection and law enforcement. This includes all Army components and major commands which includes Active Duty, Army Accessions Command, Army Audit Agency, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army Intelligence and Security Command, Army Medical Department, Army Research Institute, Army Reserve Command, Army Training and Doctrine Command, Assistant Secretary of the Army (Financial Management & Comptroller), Department of the Army Inspectors General, Provost Marshal General, Army Staff Principals in the chain of command, and Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

Other DoD Components.

Specify.

Department of the Navy, Air Force, Marines, 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 Army."

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 Army, 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 Department of the Army.

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 Army's contract with the Service Provider specifically requires 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.

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

Specify.

Vendor PII is shared with a third-party service provider 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.

Submission of PII is strictly voluntary, however, if an individual does not wish to provide their PII they will be denied access to the Army base.

(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 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 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.

Individuals who have a government issues ID (military, CAC) 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 Army installation. They cannot selectively consent to provide some, but not all, of the individual information they are required to provide in order to enter the Army 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.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

A Privacy Act Statement is provided to, and is required to be read by, individuals 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 Vendor to type in his/her information.

Individual with government IDs (military, CAC) initiate the collection and maintenance of their PII when they arrive at an Army installation ACP and seek entry.

Each installation is responsible for providing a privacy 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.