PRIVACY IMPACT ASSESSMENT (PIA)

For the

Reserve Component Manpower System - Guard (RCMS-G)
Army National Guard

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 1290 (ATIR DA01348)

☐ **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 A0600-8-23 AHRC

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 0704-0173

Enter Expiration Date 03/31/2010

☐ **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 600-8-23, Standard Installation/Division Personnel System Database Management; and E.O. 9397 as amended (SSN).

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 Reserve Component Management System - Guard is a multifaceted legacy system providing automated data processing and information technology support to the Chief, Army National Guard. RCMS - Guard, a robust set of databases has, since 1985, processed and consolidated source data from multiple locations into usable information that serves as the source information for force structure-forecasting models, decision support applications, tools and reporting capabilities. RCMS - Guard is a diverse suite of web-based and web-enabled tools that utilize a tiered security system based on Army Knowledge Online/Guard Knowledge Online login. Access authorization is based on functional lead defined permission schema. There is one authentication/permission utility for all RCMS - Guard applications.

RCMS - Guard is a comprehensive information system, a one-stop shop for all National Guard Bureau (NGB) personnel-related data, decision support systems, workflow management, and planning tools. RCMS - Guard processes all of the personnel transactions every month for the Army National Guard and maintains force structure-forecasting models that are used for personnel policy analysis and force structure budget development.

Type of PII collected within the system is personal, financial, medical, military, education, and employment.

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

The Army National Guard considered four discreet potential privacy risks in designing and developing RCMS:

- Unauthorized access
- Inaccurate information
- Privacy and due process right protection
- Unauthorized disclosure

In response to the risk of unauthorized access to the sensitive information that records within RCMS will contain, the Army National Guard is taking a "defense in depth" approach to protecting this information. Physical safeguards (e.g., data stored on accredited servers in the Army National Guard Readiness Center), technical safeguards (e.g., encryption; common access card, password protection) and procedural safeguards (e.g., physical access to data based on duty position) are employed in series to ensure only those personnel that demonstrate "need to know" can access information contained within RCMS. In response to the risk presented by including inaccurate information in the system, RCMS correlates information from authoritative sources only. In response to the risk of violating the rights of the individuals involved in the collection process, the Army National Guard is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. Data is only viewed by RCMS users and personnel that require access to the information in the performance of their duties. In response to the risk presented by unauthorized disclosure of information contained, RCMS requires that users of RCMS receive information assurance awareness and system training in order to mitigate risks involved. This multi-faceted approach to safeguarding information provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

Threats: Threats to the collection, use, and sharing of data are alleviated by collecting and maintaining the data in a secure and accredited system. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training. In addition, data sharing occurs only among individuals authorized access to the system of records as stated in the governing Privacy Act system notice.

Danger: There are no dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the 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. National Guard Bureau (NGB), including States, Territories, District of Columbia,NGB-ASM (Army Strength Maintenance) U.S. Army, U.S. Army Reserve, Training and Doctrine Command (TRADOC), U.S. Army Recruiting Command (USAREC), Office of the Secretary of Defense (OSD), Defense Manpower Data Center (DMDC), Army Research Institute, Department of the Army Inspector General (DAIG), Army Criminal Investigations Division Command (USACIDC), Assistant Secretary of the Army - Financial Management and Comptroller (ASA FM&C), U.S. Army Audit Agency (AAA), United States Army Intelligence and Security Command (INSCOM), Provost Marshall General (PMG)

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

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

Specify.

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.

When the soldier initially enlists in the Army National Guard, a statement exists on the enlistment forms that gives consent to collect the individuals PII.

(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.

Consent is given during enlistment or inquiry into joining the Army National Guard. Once the data is within the Army National Guard it is used between systems.

(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.	Privacy Act Statement Authority: 10 U.S.C. 3013, Secretary of the Army; Army Regulation 600-8-23, Standard Installation/ Division Personnel System Database Management; and E.O. 9397 (SSN) Principal Purpose: The Reserve Component Management System - Guard (RCMS-G) collects data verify eligibility for benefits, incentives, and to process and consolidate source data from multiple locations into usable information that serves as the source information for force structure-forecasting models, decision support applications, tools and reporting capabilities.

Routine Uses: None. This information will not be disclosed outside of the Department of Defense other than the "Blanket Routine Uses" as published in the Federal Register.

Disclosure: Providing the solicited information is voluntary; however, failure to provide this information may result in the Army National Guard being unable to process your request for education benefits, incentives, etc.

Furnishing of the information solicited is voluntary; however, failure to provide this information may result in the Army National Guard being unable to process your request for education benefits, incentives, etc.

Registration Information

Why do we need your Social Security Number?
Social Security Number (SSN), Date of Birth (DOB) and other verifiable data is gathered from enlistment records covered under blanket routine uses to authenticate who you are. Additional verifiable data fields can be modified to reflect updated information. Your SSN will be stored with your account and is shared with agencies and organizations involved in the benefits eligibility process and strength forecasting.

Is it safe?

Security during transmission is ensured using a 128-bit Secure Socket Layer (SSL) connection. This is the highest industry standard and establishes an encrypted session between your computer and RCMS-G site services. We use the same technology that other major companies operating on the World Wide Web (WWW) use to protect personal information and guard against identity theft. Look for the little yellow padlock at the bottom of your browser window to ensure that you have established a secure connection. There are no alternate means of registration as this is the most secure method of protecting your information.

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.