PRIVACY IMPACT ASSESSMENT (PIA)

For the

Strength Maintenance Management System (SMMS)

Army G-1/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: 12150 (DA192907)
- ☐ **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 03/30/2012

☐ **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 (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.

SMMS is an Enterprise class platform that has consolidated 4 Strength Management systems, with 2 more scheduled by end of FY13. It presently provides 32 user modules and tools, and drives the G1 Gateway, Path to Honor, and Guard Incentive Management System (GIMS). Most tools support Accession Management, Attrition Management, Recruiting Operations, Marketing, Advertising, Resource Management, and Business Process Automation. Extensibility of tools allows support of other ARNG divisions including Chaplains, Chief Surgeon General (CSG), NGB Policy, and Education and Incentives. SMMS uses a data driven architecture in order to minimize redundancy, share common data, and provide a framework for future expansion. SMMS supports approximately 50,000 users . Ongoing discussion within GSS and NGB on consolidating other systems and applications into SMMS. Additions include Retention Management, VULCAN Modernization (Recruit Sustainment Program management tool), and the Automated Unit Vacancy System (AUVS) v2. Components and network boundaries located at the Pentagon, U.S. Army Information Technology Agency (USAITA) data center with active data exchanges to multiple Army and DoD systems. The system uses high availability features with data backups captured on a daily basis and stored offsite at a site denominated Pentagon USAITA site 2.

Types of PII collected within the system:

Name
Social Security Number (SSN)
Driver's License
Citizenship
Legal Status
Gender
Race/Ethnicity
Birth Date
Place of Birth
Personal Cell Telephone Number
Home Telephone Number
Personal Email Address
Mailing/Home Address
Religious Preference
Security Clearance
Marital Status
Medical Information
Military Records
Education Information

The following applications reside on SMMS:

Strength Maintenance Management System

G1 Gateway

Path To Honor

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

The Army considered four discreet potential privacy risks in designing and developing SMMS:
• 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 SMMS will contain, the Army is taking a "defense in depth" approach to protecting this information. Physical safeguards (e.g., data stored on accredited servers in the Pentagon), 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 SMMS. In response to the risk presented by including inaccurate information in the system, SMMS 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 is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. Data is only viewed by SMMS 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, SMMS requires that users of SMMS 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. Army Accessions Command, Army G1, Army Recruiting Command, Army Recruiting Information Support System, Military Entrance Processing Command.

☐ **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. System is maintained with contractor support from Tiber Creek Consulting and ASM Research.

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

Specify. Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG, and ASA FM&C. In addition, the DOD blanket routine uses apply to this system.

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.

Portions of the website that allow access to individuals will provide them the opportunity to object to the collection of data during the use of the system. The system prominently displays the system Privacy Act Statement and Privacy and Security notices in accordance with the law and DoD policy. Data is received from multiple sources within the Army via system to system data exchange. This data exchange is performed using the secure file transfer protocol (SFTP) and secure web services. The agencies we exchange PII with are:

(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. Users give generic consent to use their data for recruiting and retention purposes to include reporting.

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