



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.

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.

The Strength Maintenance Management System (SMMS) serves as the primary management and reporting tool for the Army National Guard (ARNG) Strength Maintenance division. The system tracks marketing data, leads data, applicant processing data, control number management, accessions data, and initial entry training dates in order to track resources and personnel through the accessions process. Additionally, it provides decision makers with the data and analysis they need to make decisions relevant to Strength Maintenance. The system additionally allows applicants to complete and submit an enlistment/ commissioning packet for the ARNG through the Path to Honor application, as well as submitting scheduling requests for: ASVAB testing, physical examination, and enlistment ceremony. 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: Personal, Military, Medical, Security, and Educational information

The following applications reside on SMMS: Strength Maintenance Management System, G1 Gateway and 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, Military Entrance Processing Command. In addition, if requested in support of an authorized investigation or audit, we may share information with Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG, and ASA FM&C.

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. Contract states in Section 10: "PRIVACY ACT: Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S.C. Section 552a and applicable agency rules and regulations." In addition, attachment C – "General Document Standards" lists DoD Directive 5400.11 as a reference of standards the contractor must comply with.

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.

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.

(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.

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 Strength Maintenance Management System (SMMS) serves as the primary management and reporting tool for the Army National Guard (ARNG) Strength Maintenance division. The system tracks marketing data, leads data, applicant processing data, control number management, accessions data, and initial entry training dates in order to track resources and personnel through the accessions process. Additionally, it provides decision makers with the data and analysis they need to make decisions relevant to Strength Maintenance. The system additionally allows applicants to complete and submit an enlistment/commissioning packet for the ARNG through