PRIVACY IMPACT ASSESSMENT (PIA)

For the

AAA Sensitive Automated Information System
U.S. Army Audit Agency

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: 4072 DA03905
- ☐ **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 A0036-2 USAAA

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.

* DoDI 7600.02 "Audit Policies" dated April 27, 2007, Section 6.2.1 states that DoD audit organizations should have full and unrestricted access to all personnel, facilities, records, reports, databases, documents, or other information or material in accomplishing an announced audit.

AR 36–2 , "Audit Services in the Department of the Army", dated 19 September 2007, Section 1–6c. states that: Audited activities will provide information that is factual, accurate, and representative of the situation being assessed. Audited activities will not unreasonably delay the progress of the audit when providing this information. Audit organizations will have full access to all personnel, facilities, records, reports, databases, and documents. Audited activities will make all accounts, books, records, documents, papers, facilities, equipment, and other assets available for examination and observation by auditors and make available knowledgeable personnel who can discuss the information. (This material includes letters, memorandums, endorsements, reports, memorandums for the record, contingency plans, relevant working papers, and documents and media of any type, including automated or electronic records and systems with any needed associated passwords.) Audited activities will not require written requests unless one is needed for clarification.

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 AAA unclassified network enclave provides a standard centralized office and administrative type environment. The environment supports formal audit of record as directed by the Secretary of the Army and other senior leaders. It also provides all Manpower; Budget and Resources; Personnel Security; Audit Application of Record; WEB access (Intranet/Internet/Extranet); data storage; Database management (SQL/ ORACLE) capabilities; Information Technology Services and Support; Cyber Security; Knowledge Management services as well as Video Teleconferencing for the Army Audit Agency.

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

There are always risked associated with maintaining users personal information. The known and identified risks and the solutions to mitigate the risks are listed below:
* Current ITA provided server supporting most of the agency's large PII data sets, audit reports, working papers and shared storage areas are not data at rest compliant. The AAA requested to fund a compliant server for the sensitive data within its repositories. Awaiting FY15 to resubmit request for server procurement. The server also sits behind the security stack which is monitored by the PENTCIRT and systems administrators for unusual or malicious activity.
* Auditors frequently manipulate and utilize large data sets of PII data from consolidated Army and DOD repositories. All AAA workstations and auditor laptops are encrypted with Bit Locker. In addition, every user is required to logon with the Common Access Card. All employees are required to use the ITA provided client VPN to perform all work through a secure connection to the servers and data repositories from all remote access locations. All GDIT IT service and support staff are issued OA certificates to perform administration on the network as well as the help desk technicians are also issued technical certificates to perform their duties.
* The agency's AAASist database is being reviewed to delete public users accounts and data (old user accounts and associated data) to meet AR 25-2 and PII requirements.
* All users take annual PII awareness training for reporting and protecting PII.
* Cyber Security, Personnel Security and General Counsel also brief PII protection in their training and awareness briefs.
* Employees must provide PII for the hiring process and other administrative actions. This data is restricted to a need to know role based access. In addition the information is maintained in centrally managed Army repositories created for the data required.

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. Our data exchanges occur within the Army and the Defense Finance and Accounting Service for Army records. No AAA employee shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be IAW 5 U.S.C. 552b (1-12).

☐ **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.

The Contract (HC1028-08-D-200 -0007) GDIT IT Service and Support Contract states in paragraph:
12. Security.
Storage of Classified Information.
Storage facilities for classified information will be provided by the Government and in accordance with the DD Form 254. The Contractor shall comply with all appropriate security regulations in handling and storing material in publishing reports and other products. The Contractor shall be well versed and follow established Information Assurance guidelines IAW regulations governing the storage, safeguarding, reporting, and protection of classified, personal identifiable and sensitive information.
Contractors shall report all security incidents to the Agency Security Manager, COR, and Supervisor immediately upon discovery, or as soon as possible as the situation warrants. Provision of the Department of the Army (DA) regulations will apply to the performance of all work for these tasks. The Contract (HC1028-08-D-200 -0007) 12. Security. Security Clearance Requirements. All individuals requiring access to USAAA information technology systems shall obtain and maintain the clearance and background investigation for the role to which assigned per AR 25-2 and DoD 8500.2, and will be granted access according to their security clearance, need-to-know and their IT Position Category. All IT Service and Support staff as well as the IA Staff sign non disclosure agreements as part of their requirements for privileged level access.
14. Other Pertinent Information or Special Considerations.
c. Identification of Non-Disclosure Requirements. The instances for the implementation of the non-disclosure are scenario based as well as regulatory. The list below is not inclusive of every case scenario or regulatory compliance in which the non-disclosure requirement would be invoked.
• USAAA Audit Work Papers and Data (Classified and Unclassified)
• USAAA Personally Identifiable Information or Data
• USAAA Network Hierarchy (architecture, routing, passwords, known vulnerabilities, etc.)
• Any Security Event regardless of nature
• Any contract information that may be discovered during the course of standard operations and management of the network data

The Prophecy Group Consulting Contract (W9124P-14-C-0054) Part 10.1 Directives. All persons performing work under this SOW must comply with all applicable Federal, Department of Defense (DoD) and U.S. Army directives, instructions and standard operating procedures when working in Government facilities, working on behalf of the Government, or accessing and handling information as part of this contract. DA provides access to DA publications on their web site at http://www.apd.army.mil/. Army Audit provides access to all other pertinent publications on its internal web page. 10.2 Coordination. The contractor shall coordinate with USAAA security officer to ensure identification and compliance with security regulations, requirements, and practices, and shall ensure that all personnel have appropriate clearances as required.

☐ **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.

The Privacy Act Statement's Mandatory or Voluntary Disclosure clearly defines the affects of not providing the requested information.

(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.

The Privacy Act Statement clearly defines the Principle Purpose for the collection, the Routine Uses of the information collected and the Mandatory or Voluntary Disclosure of the information collection. No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be IAW 5 U.S.C. 552b (1-12).

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