



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Records Information Management (TRIM) for the Army Review Boards Agency

Department of Army

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

10704-0003
0704-0004

Enter Expiration Date

June 30, 2011 {new exp. date has beerg}

D 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.

5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 3013, Secretary of the Army;
10 U.S.C. 1552, Correction of military records: claims incident thereto;
10 U.S.C. 1214, Armed Forces; Right to Full and Fair Hearing
10 U.S.C. 1216, Secretaries, powers, functions and duties
10 U.S.C. 1553, Review of Discharge or Dismissal
10 U.S.C 1554, Military Personnel Benefits
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 Deputy Assistant Secretary of the Army Review Boards Agency (ARBA) is responsible to the Assistant Secretary of the Army, Manpower and Reserve Affairs (ASA(M&RA)) for the review and adjudication of applications and cases submitted by various parties for the correction of military records for past and present members of the United States Army (USA) and Army National Guard (NG) or their authorized representative. TRIM is a database management package that works with ARBA Case Tracking System (ACTS) to provide electronic image management capabilities, the capability to manage multiple renditions of the image and to restrict access to the image if required, and a bar-coding capability that assists users at ARBA with their record management and workflow processes.

TRIM Context is a Commercial Off the Shelf (COTS) product. The system is owned by the Chief of Staff, ARBA. System components are located in Arlington, VA. TRIM is a private system and its database servers are located behind a firewall. Its only interconnection is to the ARBA Case Tracking System (ACTS), also owned by ARBA, where documents are inserted and retrieved from TRIM Context using ACTS as an interface. Documents are scanned and stored as Tagged Image File Format (TIFF) files, which are called up from ACTS.

Full database backups are run daily. Transaction log backups are run hourly. The information is copied to a tape library for off-site storage. There are three types of backup schedules; Daily/Differential, Weekly/Full and Monthly/Full. Weekly/Full tapes have a shelf life of 5 weeks and Monthly/Full tapes are archived off-site for 1year.

The information in identifiable form that will be collected includes: name, date of birth, current grade/rank or briefs/arguments, advisory opinions, findings, conclusions and decisional documents of the Boards. The information is collected directly from the activity with pertinent records, the applicant, a surviving spouse or next of kin or legal representative. This information is provided voluntarily using DD Form 149 or DD Form 293, which are scanned into TRIM. Other supporting documentation containing information in identifiable form is collected in hardcopy format from the Army's interactive Personnel Electronic Record Management System (iPERMS) and/or from the National Archive and Records Administration (NARA). Information will be collected from any activity having a stake in, or responsive information pertaining to, an applicant's request for collection.

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

TRIM Context reduces risk by having data stored with unique numbers that do not reference a person's name or personal data. Only those persons authorized to view a case may view the file. To reduce risk, TRIM Context has a comprehensive security system. Access is granted by group or individual basis. Along with Passwords, data is protected by security level and Security Caveat such as Records, locations, and Classifications. Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

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. Not all information in identifiable form is shared with all the Army agencies

listed below. Only final determinations are sent to relevant agencies to initiate appropriate changes related to that decision (e.g. a decision regarding a pay grade may be sent to DFAS in order to initiate a change in pay for the individual). Information in identifiable form may be shared with the following Army agencies: Army Inspector General (IG); Assistant Secretary of the Army for Manpower and Reserve Affairs (ASA(M&RA)); Deputy Chief of Staff, G-1; Human Resources Command (HRC); Human Resources Command-St. Louis (HRC-St. Louis); Office of the Chief, Army Reserve (OCAR); Army General Counsel (GC); Secretary of the Army; US Army Reserve Command (USARC); Army Recruiting Command (USAREC); US Army Cadet Command; US Army Military Academy (USMA); Army Physical Disability Agency (PDA);

Other Army agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, In addition, the Army blanket routine uses apply to this system.

181 Other DoD Components.

Specify.

Not all information in identifiable form is shared with all the DoD agencies listed below. Information in identifiable form may be shared with the following DoD agencies: Office of the Judge Advocate General (OTJAG); National Personnel Records Center (NPRC)(a division of the National Archives and Records Administration (NARA)); States' Adjutants General for all states and territories; National Guard Bureau

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Criminal Investigative Service. In addition, the DoD blanket routine uses apply to this system.

D Other Federal Agencies.

Specify.

D State and Local Agencies.

Specify.

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

Specify.

D 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.

Applicants are given the opportunity to consent to the use, collection and storage of their information in identifiable form by signing DD Form 149 or DD Form 293, each of which contains a Privacy Act Statement. A Privacy Notice is located on the ACTS Online website that informs the individual of their option to consent by signing, or object to the collection and/or use of their information in identifiable form. It also informs the applicant of ARBA's use, sharing and collection practices.

(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 D No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Applicants are given the opportunity to consent to the use, collection and storage of their information in identifiable form by signing DD Form 149 or DD Form 293, each of which contains a Privacy Act Statement. A Privacy Notice is located on the ACTS Online website that informs the individual of their option to consent by signing, or object to the collection and/or use of their information in identifiable form. It also informs the applicant of ARBA's use, sharing and collection practices.

(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.

181 Privacy Act Statement D Privacy Advisory
 D Other D None

Describe each The Privacy Act statement reads as follows:

applicable
format.

PRIVACY ACT INFORMATION: The authority for collection of information on the DD Form 149 is Title 10, U.S. Code, section 1552, EO 9397. The principal purpose is to initiate an application for correction of military records. The form is used by Board members for review of pertinent information in making a determination of relief through correction of military record. Routine Use: None. Disclosure is voluntary; however, failure to provide identifying information may impede processing of this application. **SOCIAL SECURITY INFORMATION:** The request for Social Security number is strictly to assure proper identification of the individual and appropriate records.

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.