



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Law Enforcement Audio/Video Recorder and Download Software (TASER CAM™)

US Army Medical Command – Defense Health Program (DHP) Funded Application

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
- 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

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.

10 U.S.C. 3013, Secretary of the Army; 18 U.S.C. 44, Brady Handgun Violence Prevention Act; 28 U.S.C. 534, Uniform Crime Reporting Act; 42 U.S.C. 10606, Victims Rights and Restitution Act of 1990; DoD Directive 10310.1, Victim and Witness Assistance; Army Regulation 190-45, Military Police Law Enforcement Reporting and E.O. 9397 (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 TASER CAM™ law enforcement audio/video recorder offers increased accountability - not just for police officers, but for the people they arrest. Without video, it can be the officer's word against the suspect's word. The TASER CAM is integrated into the TASER® Electronic Control Device power supply and is activated any time the safety is in the "ARMED" position. The TASER CAM allows officers to capture vital audio and video information prior to, during, and after the potential deployment of the TASER. The TASER CAM download software allows for easy download and review of videos from the TASER CAM to designated computers. This information is collected to review or investigate usage of the TASER and provides another layer of accountability to support law enforcement officers' reports.

The types of PII derived from audio and video captured by the TASER CAM include name, gender, race/ethnicity, law enforcement information, and recognizable photographic images.

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

The risks associated with the collection, use, and storage of PII are unauthorized access and unauthorized disclosure. There are security measures in place to mitigate these risks. Access to information is controlled; limited to authorized personnel having official need to know. Designated computers are located in limited access area for protection from unauthorized use. Access to information is also controlled by passwords for authorized designated computers users.

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.

The PII will be shared within the medical treatment facility using this application and any Army law enforcement entity conducting an authorized investigation into an incident involving use of the TASER.

Other DoD Components.

Specify.

The PII will be shared with any DoD law enforcement entity conducting an authorized investigation into an incident involving use of the TASER.

Other Federal Agencies.

Specify.

The PII will be shared with any Federal law enforcement entity conducting an authorized investigation into an incident involving use of the TASER.

State and Local Agencies.

The PII will be shared with any state or local law enforcement entity

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.

(2) If "No," state the reason why individuals cannot object.

The individual's participation is due to their uncooperative response to previous security force commands. Appropriate security force action is verified by the TASER CAM. Any PII collected is a secondary product of the use of the TASER which activates the TASER CAM video/audio recorder.

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.

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

The individual's participation is due to their uncooperative response to previous security force commands. Appropriate security force action is verified by the TASER CAM. Any PII collected is a secondary product of

the use of the TASER which activates the TASER CAM video/audio recorder.

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.

The individual's participation is due to their uncooperative response to previous security force commands. Appropriate security force action is verified by the TASER CAM. Any PII collected is a secondary product of the use of the TASER which activates the TASER CAM video/audio recorder.

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.