



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

CID Information Management System (CIMS)

USACIDC

### **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      1616 (DA 00826)
- 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      007-21-01-03-02-0364-00

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      A0195-2b USACIDC; A0690-200 DAPE

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**

2010-8928

**Enter Expiration Date**

30 September 2010

**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.

The authority to collect information (statutory or otherwise)

The authority is listed in the federal register notice: United States Code - Secretary of the Army (10 USC 3013), Army Regulation- Criminal Investigation Activities (AR 195-2), United States Code-Victim Rights-(42 USC 10606) et seq., Department of Defense- Victim and Witness assistance, (DoD Directive 1030.1-Victim and Witness assistance), and Executive Order- Social Security (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 CIMS program is a criminal investigation case management system that includes criminal intelligence querying and reporting capabilities in compliance with regulatory and policy standards for Army Law Enforcement regarding investigation of felony crimes. CIMS captures criminal case investigative information regarding incidents, location descriptors, entities, agent assignment, crime description and identifiers, statements, property data, laboratory tests; verifies and stores this data for criminal intelligence purposes: and reports this information to the proper authorities from the Division Commanding Officer to the United States Grand Jury. The system extracts necessary data for consolidation and input to Defense Incident-Based Reporting System (DIBRS) monthly reports, National Incident-Based Reporting System (NIBRS) monthly reports and the Defense Clearance and Investigations Index (DCII) daily updates.

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

**Threats:**

Information in the system is collected, stored, and maintained in a secured and accredited system and network, alleviating threats to the collection, use, and sharing of data. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance awareness training. Data sharing occurs only among individuals with authorized access to the system records.

**Dangers:**

Individuals can decide not to provide the personal information and are made aware that to opt out will be detrimental to their possibility of employment or ability to become an agents/federal employees.

**Risks:**

The security risk associated with maintaining data in an electronic environment has 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

Only personnel with a need-to-know in order to perform official government duties have access without the consent of the individual. Administrative Security controls include verification that new personnel have a favorable SSBI background investigation and are cleared U.S. citizens, completed initial Information Assurance Security briefing, signed user memorandum of agreement that includes rules for ACI2 system, and completion of user training prior to IASO creating ACI2 account. Individuals must out-process through IASO and Security, who will then ensure ACI2 account, is disabled. All ACI2 users must complete Annual Information Assurance Security briefing/training. Physical security controls include limiting access to USACIDC offices. All visitors are processed through the Security Office with security guards at the main building entrance and are escorted as required. Outside windows do not open. Technical security controls are employed to minimize unauthorized disclosure, modification, or destruction of data and are in compliance with Army Gold Standard and applicable DoD automated systems security controls requirements. System security controls are reviewed and tested annually at a minimum to ensure compliance.

**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.

HQDA, G1  
Within the Army and Department of Defense (DoD): Action Commanders, Staff Judge Advocates, Intelligence agencies, Morale and Welfare, Army and Air Force Exchange Services (AAFES), and Army Agencies authorized to

obtain information for employment and other security concerns. Limited information can be shared in support of the victim/witnesses assistance program.

**Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC), Defense Human Resources Activity (DHRA), United States America (USA), United States Air Force (USAF)

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify. In addition to those disclosures generally permitted under 5 U.S.C. 552 a (b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S. C. 552a (b) (3) as follows:  
Information concerning criminal or possible criminal activity is disclosed to Federal, State, local and/or foreign law enforcement agencies in accomplishing and enforcing criminal laws; analyzing modus operandi, detecting organized criminal activity, or criminal justice employment. Information may also be disclosed to foreign countries under the provisions of the Status of Forces Agreements or Treaties.

**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.

Individuals may refuse to cooperate with investigations as long as their actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters USACIDC and the Army Board of Correction of Military Records.

(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.

(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.

In most cases, individuals must invoke the Freedom of Information Act ( FOI/PA) to obtain information from the system. Information is sent hardcopy via mail. Some information is provided verbally to individuals through the investigative process, and via victim/witness assistance.