



## 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; A0190-45 OPMG

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**

One is required. POC has made contact with Army IMCO for instructions.

**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.

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 and Restitution Act of 1990 (42 USC 10606), Department of Defense- Victim and Witness Assistance, (DoD Directive 10310.1-Victim and Witness Assistance), Executive Order- Social Security (E.O. 9397 (SSN)), as amended, 5 U.S.C. 301, Departmental Regulations, 10 U.S.C. 951, 18 U.S.C. 44, Brady Handgun Violence Prevention Act, 28 U.S.C. 534, Uniform Crime Reporting Act, Army Regulation 190-45 Military Police Law Enforcement Reporting, Army Regulation 190-9, Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies, Army Regulation 190-13, The Army Physical Security Program, Army Regulation 190-14, Carrying of Firearms and Use of Force for Law Enforcement Security Duties, Army Regulation 190-47, The Army Corrections System, Army Regulation 380-13, Army Regulation 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations, Army Regulation 630-10, Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings, Status of Forces Agreement between the United States of America and the Host Country in which U.S. Forces are located, Army Regulation 690-200, General Personnel Provision, Army Regulation 195-6, Department of the Army Polygraph Activities, Privacy Act 5 U.S.C. 552(a), 10 U.S.C. 3012(g).

**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.

CIMS includes the Centralized Operations Police Suite (COPS) and the Resource Management Online (RM Online) systems. COPS is a centralized database containing five subsystems that support the Army Military Police Corps. These subsystems provide law enforcement reporting via the Military Police Reporting System (MPRS); correctional tracking via the Army Correctional Information System (ACIS) vehicle and weapons registration via the Vehicle Registration System (VRS); enemy prisoner of war and detainee accountability via the Detainee Reporting System (DRS); and parole and clemency management of inmates in Army correctional institutions via the Army Review Board Agency (ARBA). The systems contain data derived from military police reports along with details of any criminal prosecution, civil court action, or non-judicial administrative punishment. The system also records the registration of vehicles and weapons, contains details from correctional treatment records which are used to determine prisoners' custody classifications, work assignments, education needs, adjustment to confinement, and the basis for clemency, parole and restoration to duty considerations. Automated records provide pertinent information required for proper management of confinement facility population, demographic studies, status of discipline and responsiveness of personnel procedures, as well as confinement utilization factors such as population turnover, recidivism, etc. The system contains information on agency personnel, members of the public, family members, victims and witnesses of crimes. The system provides Management data on which to base crime prevention, selective enforcement, improved driving safety, statistical data for developing crime trends by major categories, (e.g., crimes against persons, drug crimes, crimes against property, fraud crimes and other offenses).

RM Online purpose is to collect information to determine the eligibility of Federal applicants for acceptance and retention in the CID special agent program. Civilian information is collected to determine the applicant's suitability for employment and the ability to hold a clearance. The type of PII collected pertains to educational, employment, military, clearance, financial data, date of birth, identification numbers, and gender.

**(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 and COPS systems, and completion of user training prior to IASO creating ACI2 account. Individuals must out-process through IASO and Security, who will then ensure ACI2, COPS, and RM Online accounts, are disabled. All ACI2/COPS/RM Online users must complete Annual Information Assurance Security briefing/training. 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), Army Staff Principals in the chain of command, Department of the Army Inspectors General, Army Audit Agency, Army Intelligence and Security Command, Assistant Secretary of the Army (Financial Management & Comptroller) Medical facilities, 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. DOD Law Enforcement Exchange (DDEX) providing data to Air Force Office of Special Investigations (AFOSI) Marine Corps CID, Navy Military Police and Naval Criminal Investigative Service (NCIS). CID Accreditation and Civilian Personnel Division and other internal authorized users.

**Other DoD Components.**

Specify.

Defense Manpower Data Center (DMDC), Defense Human Resources Activity (DHRA), United States America (USA), United States Air Force (USAF). DoD Inspector General, Defense Criminal Investigative Service, Naval Criminal Investigative Services, Defense Finance and Accounting Service and Medical facilities.

**Other Federal Agencies.**

Specify.

Office of Management and Budget, Department of Veterans Affairs, other Federal Law Enforcement and Confinement/Correctional Agencies; Bureau of Prisons, Alcohol, Tobacco & Firearms, Federal Bureau of Investigation, Office of Personnel Management, Department of Homeland Security, Federal Child Protection Services or Family Support Agencies, Immigration and Naturalization Services, Department of Justice, Internal Revenue Service, General Services Administration, National Archives and Records Administration, the Merit Systems Protection Board and the Office of Special Counsel.

**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; motor vehicle departments, State and local confinement/correctional facilities; Medical facilities; State and local child protection services and family support agencies. 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.

Micro Technologies, LLC  
CIMS development, operations and maintenance life-cycle management is maintained by contract support. The contract states that all contract personnel assigned to the contracts shall hold a Secret clearance. All information available to the contractor while performing this task, both electronic or otherwise, shall be maintained in a strictly confidential manner and protected in accordance with its designated security classification. Contract personnel working on this task order shall require access to law enforcement sensitive and legal sensitive information and shall be required to interface with anti-terrorist reporting systems, criminal intelligence systems as well as other intelligence communication systems. These personnel and work locations house Army LE data are required to meet the requirements of the Physical Security Site Survey and be certified by the USACIDC Security Officer in accordance with Army Regulation 190-13. On site or off site personnel who are authorized unrestricted access to law enforcement data, equipment, or user account management shall be required to have a Secret clearance and a Single Scope Background Investigation (SSBI).  
CACI-CMS Information Systems, Inc.  
CACI provides support for RM Online. CACI personnel signed non-disclosures indicating agreement to protect information from unauthorized use or disclosure and to refrain from using the information for any purpose other than that for which it was furnished.

**Other** (e.g., commercial providers, colleges).

Specify.

Limited information may be provided to victims and witnesses of crimes, limited information may be disclosed to foreign countries under the provision of the Status of Forces Agreements, or Treaties.

**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.

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to object. Individuals may refuse to cooperate with investigations as long as