PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

CIMS - Criminal Investigative Management System

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

05/04/18

Criminal Investigation Command

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Criminal Investigative Management Systems (CIMS) is a collection of mission essential information technology systems that supports the Criminal Investigation Command (CID) and the Office of the Provost Marshal General (OPMG). Thru the CIMS, CID and OPMG developed an integrated and unified, comprehensive enterprise program / system that houses Classified and Unclassified - Law Enforcement Sensitive (LES) data, leveraging existing and future Army LE enterprise information technology assets and other external data sources providing a full range of law enforcement functions to support business objectives and mission. The primary component is a comprehensive enterprise system, known as the Army Law Enforcement Reporting and Tracking System (ALERTS). ALERTS provides Army Law Enforcement stakeholders the enhanced capability to rapidly and efficiently manage a variety of Law Enforcement and criminal intelligence functions; as well as a broader range of senior executive reporting requirements.

In addition to ALERTS, CIMS includes the Centralized Operations Police Suite (COPS) (DITPR #2822), the Resource Management Online (RM Online) (DITPR #5189) and the application components identified below:

CID Application Processing Portal (CID-APP) manages the CID agent's application process. CID-APP portal provides applicants the ability to electronically apply to become a CID agent. The portal allows the Recruiting Operations Cell (ROC) to manage and track applications from submission to approval.

i2 Portal (CI Portal) is a centralized implementation of IBM/i2 Analyst's Workstation/Notebook tool suite that is customized to work directly with the ALERTS Data Warehouse to provide comprehensive, up-to-date Law Enforcement Data.

Detainee Reporting System - National Detainee Reporting Center (DRS) - (SIPR) NDRC application manages and stores information relating to detainees and their confiscated personal property.

Data Warehouse (DW) is a database repository of ALERTS data utilized by SAP and Business Objects tools for querying and reporting law enforcement data.

Electronic Imaging (EI) is an electronic data repository of all closed CID and MP law enforcement cases utilized by the Army's Crime Records Center to provide name checks, FOIA requests, and other historical information requested by higher headquarters, DoD organizations, Congress, or individuals authorized to receive the information.

Law Enforcement Advisory Portal (LEAP) is the centralized SharePoint administrative portal utilized by CID units to collaborate and share files.

National Crime Information Center (NCIC) is the application used by the Crime Records Center (CRC) and CID units to run name checks through the Federal Bureau of Investigations. NCIC is scheduled to be rationalized in FY 2018.

Polygraph (POLY) is used by the CRC to maintain and manage polygraph records. POLY is scheduled to be rationalized into ALERTS in FY 2018.

The Defense Forensics Management Exchange (DFME), which includes Next Generation Identification (NGI), Evidence Collection Management Exchange (ECMX), and Evidence Management Portal (EMP). The DFME environment all utilize the data processed, stored, or transmitted to the ALERTS database.

NGI, also known as AFIS (Automated Fingerprint Identification System), which is the system used to transmit fingerprint records to the FBI and the U.S. Army Criminal Investigation Laboratory (USACIL) from the field units through the Livescan digital fingerprint scanners or through manually scanning finger print cards.

ECMX is the real-time repository for all crime scene evidence collection, management, and reporting.

EMP is the application portal used in conjunction with the ECMX to manage and barcode evidence that has been collected during a scene."

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The information is collected to identify persons involved as subjects, suspects, witnesses or victims of crimes and to assist in the investigative process; to verify and authenticate owners of authorized vehicles and weapons; to properly account for and administer persons in confinement; verification, authentication, and identification of information provided by applicants for creating credentials and verifying eligibility and qualification for employment. This information is also used to confirm the facts as stated in the case.

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

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

Individuals give consent to use, collection, and storage of their information in identifiable form through their signing of the application for employment/agent application process. Individuals can object to the collection of PII by not signing the application. If consent is not given, the application process to determine eligibility can not proceed nor will civilian employment be considered.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

Individuals providing applications for employment/agent assignment. A voluntary application for acceptance is provided to each individual applicant stating that the collection of personal information will be solicited to facilitate eligibility in the special agent application process and for continued qualification in the CID special agent program. The information collected on the declaration for federal employment form OMB No. 306 is used to determine acceptability for federal employment.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[ ] Privacy Act Statement [X] Privacy Advisory [ ] Not Applicable

NOTICE AND CONSENT

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

ALERTS User Responsibilities:

- Maintain and safeguard FOUO/Law Enforcement Sensitive and PII information.

- Limit access to those with a need to know.

- Do not exceed your access by reviewing information that you do not have a need to know about.

- Do not provide information to others without a need to know.

- Violation of the above may result in adverse administrative or legal actions.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	HQDA, G1; Action Commanders, Staff Judge Advocates, Intelligence Agencies, Army Staff Principals in the Chain of Command, Medical Facilities, CID Accreditation and Civilian Personnel Division and other internal authorized users.
[X] Other DoD Components	Specify.	Department of Army Inspectors General, Army Audit Agency, Army Intelligence and Security Command, Assistant Secretary of the Army Financial Management & Comptroller, Army Agencies authorized to obtain information for employment and other security concerns. DOD Law Enforcement Exchange (DDEX), Air Force Office of Special Investigations (AFOSI), Marine Corps CID, Navy Military Police, Naval Criminal Investigative Service (NCIS), Defense Manpower Data Center (DMDC), Defense Human Resources Activity (DHRA), DOD Inspector General, Defense Criminal Investigative Service, Defense Finance and Accounting Service (DFAS)

[X] Other Federal Agencies	Specify.	Army and Air Force Exchange Services (AAFES), 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.
[X] 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.
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	InterImage, Inc 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.

[X] 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. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[X] Databases
[X] Existing DoD Information Systems
[X] Commercial Systems
[X] Other Federal Information Systems

Information is obtained through system and individuals, from victim and witnesses of crimes, through research involving access to multiple automated data systems, records and third parties, citizens band and commercial radio, local proactive crime watching/prevention organizations, individual applicants, Enlisted Record Brief (ERB), Official Military Personnel File (OMPF), Total Officer Personnel Management Information System (TOPMIS), Enlisted Distribution and Assignment System (EDAS), Defense Finance and Accounting System (DFAS), Automated Civilian Personnel System (ACPERS), Credit Reports submitted by Applicants (Equifax, Experian, Trans Union).

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

[X] E-mail
[X] Official Form (*Enter Form Number(s) in the box below)*
[X] Face-to-Face Contact
[X] Paper
[X] Fax
[X] Telephone Interview
[X] Information Sharing - System to System
[X] Website/E-Form
[X] Other *(If Other, enter the information in the box below)*

Investigators gather data from individuals through investigative interviews, and through research involving access to a wide variety of other services of information such as automated data systems, records, and third parties; from victims and witnesses of crimes; citizens band and commercial radio, local proactive crime watching/prevention organizations; and federal, state and local law enforcement databases and communication systems.
DA Form 2823 - Sworn Statement
DA Form 3946 - Military Traffic Accident Report
DA Form 3881 - Rights Waiver
OPM Optional Form 306, Declaration for Federal Employment

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier A0190-45 OPMG

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

NOTE: The previous name for Criminal Investigative Management System (CIMS) was Criminal Investigation Command (CID) Information Management System Records (CIMS), as is stated for the current SORN; they are one and the same

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-AU-10-0100 / RN 195

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

TE40. Event is after date of final action. Keep until event occurs and then until no longer needed for conducting business, and then retire to AEA. The AEA will destroy the record 40 years after the event.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 USC 3013, Secretary of the Army; 42 USC 10606, Victim Rights and Restitution Act of 1990; DoD Directive 10310.1, Victim and Witness Assistance; 18 U.S.C. 44, Brady Handgun Violence Prevention Act, 28 U.S.C. 534, Uniform Crime Reporting Act, Army Regulation (AR) 190-45, Military Police Law Enforcement Reporting; AR 195-2, Criminal Investigation Activities; AR 190-9, Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies, AR 190-13, The Army Physical Security Program, AR 190-14, Carrying of Firearms and Use of Force for Law Enforcement Security Duties, AR 190-47, The Army Corrections System, AR 380-13, AR 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations, AR 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, AR195-6, Department of the Army Polygraph Activities, and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

CIMS is exempt from obtaining an OMB number per DoD Manual 8910.01, Volume 2, Enclosure 3, paragraph 1.b(1), "Information is collected and utilized during the conduct of a federal criminal investigation or prosecution or during the disposition of a particular criminal matter in accordance with section 3518(c)(1) of Title 44, United States Code (U.S.C.) (Reference (v))"

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[X] Child Information
[X] Citizenship	[X] Disability Information	[X] DoD ID Number
[X] Driver's License	[X] Education Information	[X] Emergency Contact
[X] Employment Information	[X] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[X] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[X] Medical Information
[X] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[X] Passport Information	[X] Personal E-mail Address	[X] Photo
[X] Place of Birth	[X] Position/Title	[ ] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[X] Records	[X] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[X] If Other, enter the information in the box below	

Physical descriptions of individuals, next of kin information, family member information, registration form for items of restricted property, permit application for restricted activities, provisional passes, blotters/journals, receipts for prisoners or detained persons, prisoners visitor rosters, prisoner release/transfer rosters, Victim/Witness Notification of Inmate Status, Inmate Observation Report, Inmate Disciplinary Report, Prisoner Sentence Computation Report, Daily/Monthly/Yearly Confinement Reports, Clerk of the Court Inmate Roster Report, Contact/Attorney Report, Global Cult/Extremist Association Report, Discharged Inmate Reports, Global Gang Affiliation Report, Global Sexual Offender Registration Current Reports, Global Inmate Confining Offense Report, Inmate Civilian Education/Contact Roster, Inmate DNA Sample Report, Inmate Racial Report, Inmate Roster, Inmate to Inmate Relations Report, Inmate Minimum Release Date Report, Inmate Special Status History Report, Institutional VWC/SOR Contact Roster, Abatement Reports, Inmate Appt/Pass Forms and Reports, Inmate Housing Roster, Disposition Boards, Evidence Room Inventory, H&C Reports, Inmate Court Martial Report, Inmate Diet Roster, Inmate Photo/Presence History Reports, AWOL Report, Barred Listings and Detailed Reports, Capture Card, Death Certificate, Detainee Processing/Presence Reports, ICRC Arrivals Death Escape Release, Repatriated, Transfer Reports, TDRC Daily Scrub, Detainee Picture, DNA, Fingerprint Card, MACOM/Installation 1805 & 1408 Listing, Court Dockets, BOLOs, DA Form 4833, Commander Report of Disciplinary or Administrative Action, Housing History, Personnel Records, MPI Man Hour Report, Name Check Audit, Repeat Offender Roster, Revocations, Traffic Violations Reports, Registration of vehicles, Decal history Report, Registration of Privately Owned Firearms, Personal Pets, Barred Individuals, Police and Criminal Intelligence, Military and Civilian Criminal History on Individuals, Safety Reports, Correctional Treatment Records, Detainee Records, information on warrants of unauthorized absentees, System Administrators, User Accounts and User Information Reports, warrant for arrest, passport numbers, retention control sheets, victims names, names of informants, name of law enforcement officers and investigators, clemency actions, psychologist's report, certificate of parole, certificate of release from parole.

LE investigation cases may involve nearly any conceivable PII data. Some PII may not be in structured data fields, but may be in the report narrative. There is no automated exchange of data between CIMS and any other systems currently. CIMS data are transferred as a query result to the SADMS system (via manual SFTP). CIMS data are transferred as a query result to the DIBRS system (via manual SFTP) CIMS data are recorded in EI (via electronic scanning). CIMS data are transferred to DCII (via manual SFTP).

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

David P. Glaser
MG, USA
Commanding
23-Jan-2018