SYSTEM NAME AND NUMBER: "Criminal Investigation Command (CID) Information Management System Records (CIMS)," A0190-45.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: The system is located at Headquarters, U.S. Army Criminal Investigation Command (USACIDC), 27130 Telegraph Road, Quantico, VA 22134-2253.

SYSTEM MANAGER(S): Director, U.S. Army Crime Records Center, U.S. Army Criminal Investigation Command, ATTN: CICR-FP, 27130 Telegraph Road, Quantico, VA 22134-2253.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C 2773a, Departmental Accountable Officials; 10 U.S.C. 3013, Secretary of the Army; The National Defense Authorization Act for Fiscal Year 2001, Public Law 106-398; National Defense Authorization Act for Fiscal Year 2012 Public Law 112-81, National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239; National Defense Authorization Act for Fiscal Year 2014, Public Law 113-66; National Defense Authorization Act for Fiscal Year 2015, Public Law 113-291; Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458; Executive Order 13526, Classified National Security Information; 10 U.S. Code (USC) 47, 1585a, 4027, 7480, 9027; 18 USC 5, 13, 1385, 3052, 3053, 3142, 3261-3267; (Military Extraterritorial Jurisdiction Act); Title 28, Code of Federal Regulations; 31 USC 3729; DoD Instruction 3025.21, Defense Support of Civilian Law Enforcement Agencies; 42 USC Chapter 151, 42 USC 16928a; 50 USC 1801 et seq, The Foreign Intelligence Surveillance Act; DoD Instruction 1030.2, Victim and Witness Assistance Procedures; DoD Instruction 1325.07, Administration of Military Correctional Facilities and Clemency and Parole Authority; DoD Instruction 5015.02, DoD Records Management Program; DoD Directive 5106.01, Inspector General of the Department of Defense; DoD Instruction 5505.02, Criminal Investigations of Fraud Offenses;

DoD Instruction 5505.03, Initiation of Investigations by Defense Criminal Investigative Organizations; DoD Instruction 5505.07, Titling and Indexing Subjects of Criminal Investigations in the Department of Defense; DoD Instruction 5505.08, Military Criminal Investigative Organizations (MCIO) and Other DoD Law Enforcement Organizations Investigations of Adult, Private, Consensual Sexual Misconduct; DoD Instruction 5505.10, Criminal Investigations of Noncombat Deaths; DoD Instruction 5505.11, Fingerprint Card and Final Disposition Report Submission Requirements; DoD Instruction 5505.12, Anti-Fraud Program at Military Treatment Facilities (MTFs); DoD Instruction 5505.14, Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders; DoD Instruction 5505.15, DoD Contractor Disclosure Program; DoD Instruction 5505.16, Criminal Investigations by Personnel Who Are Not Assigned to a Defense Criminal Investigative Organization; DoD Instruction 5505.17, Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities; DoD Instruction 5505.18, Investigation of Adult Sexual Assault in the Department of Defense; DoD Instruction 5505.19, Establishment of Special Victim Investigation and Prosecution (SVIP) Capability within the Military Criminal Investigative Organizations (MCIOs); DoD Instruction 5525.11, Criminal Jurisdiction Over Civilians Employed By or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members; DoD Instruction 5525.16, Law Enforcement Defense Data Exchange (LE D-DEx); DoD Instruction 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB); DoD Instruction 5525.20, Registered Sex Offender (RSO) Management in DoD; DoD Instruction 6400.06, Domestic

Abuse Involving DoD Military and Certain Affiliated Personnel; DoD 4160.21–M, Defense Materiel Disposition Manual; DoD 6025.18–R, DoD Health Information Privacy Regulation; DoD Manual 8910.01, Volume 1, DoD Information Collections Manual: Procedures for DoD Internal Information Collections; DoD Instruction 7730.47, Defense Incident-Based Reporting System (DIBRS); DoD Directive 5505.06, Investigations of Allegations Against Senior DoD Officials; DoD Directive 5525.1, Status of Forces Policies and Information; DoD 7730.47-M, Volume 1, Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; AR 15–130, Army Clemency and Parole Board; AR 27–10, Military Justice; AR 27–40, Litigation; AR 40–66, Medical Record Administration and Healthcare Documentation; AR 190–9, Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies; AR 190–11, Physical Security of Arms, Ammunition, and Explosives; AR 190–13, The Army Physical Security Program; AR 190–30, Military Police Investigations; AR 190–45, Law Enforcement Reporting; AR 190–47, The Army Corrections System; AR 190–58, Personal Security; AR 195–2, Criminal Investigation Activities; AR 335–15, Management Information Control System; AR 340–21, The Army Privacy Program; AR 360–1, The Army Public Affairs Program; AR 380–5, Department of the Army Information Security Program, AR 380–10, Foreign Disclosure and Contacts with Foreign Representatives); AR 380–13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations); AR 381–10, U.S. Army Intelligence Activities, AR 381–12, Threat Awareness and Reporting Program; AR 525–13, Antiterrorism, AR 600–20, Army Command Policy; AR 600–37, Unfavorable Information; AR 600–63, Army Health Promotion; AR 600–85, The Army Substance Abuse Program; AR 608–18, The Army Family Advocacy Program; AR 630–10,

Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings; and AR 710–2, Supply Policy Below the National Level.

PURPOSE(S) OF THE SYSTEM:

To provide the military chain of command with timely information regarding serious incidents to permit a valid early determination of possible implication; to provide an early indication of acts or conditions which may have widespread adverse publicity.

To conduct criminal investigation, crime prevention and criminal intelligence activities; suitability for access to continued access to classified information; suitability for promotion, employment, or assignment; suitability for access to military installations or industrial firms engaged in government projects/contracts; suitability for awards or similar benefits; use in current law enforcement investigation or program of any type including applicants; use in judicial or adjudicative proceedings including litigation or in accordance with a court order.

To provide detailed criminal investigative information and timely information regarding serious incidents to designated Army officials, commanders, criminal justice agencies, and designated Army officials to foster a positive environment, promote and safeguard the morale, physical well-being, and general welfare of Soldiers in their units. To enable the maintenance of discipline, law and order through investigation of complaints and incidents and possible criminal prosecution, civil court action, or regulatory order in accordance with United States law. To identify individuals in an effort to anticipate, prevent, or monitor possible criminal activity directed against or involving the U.S. Army.

To monitor performance and reliability; to check utilization of sources; to maintain an accounting of expenditures connected with the sources; to answer Congressional inquiries

concerning misuse of mistreatment of sources of those who allege they are not sources; to document fear-of-life transfers for military sources.

To enter data in the Federal Bureau of Investigations (FBI) National Crime Information Center wanted person file; to ensure apprehension actions are initiated/terminated promptly and accurately; and to serve management purposes through examining causes of absenteeism and developing programs to deter unauthorized absences.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Any individual, civilian, government civilian employee, or military personnel (Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve), involved in or suspected of being involved in, reporting or witnessing possible criminal activity affecting the interests, property, and/or personnel of the U.S. Army and who are used as sources by USACIDC and installation law enforcement.

CATEGORIES OF RECORDS IN THE SYSTEM: Reports and supporting document of criminal activity directed against or involving the U.S. Army, including but not limited to full name, social security number (SSN), DoD identification (ID), rank, grade, date and place of birth chronology of events, reports of investigation and criminal intelligence reports containing statements of witnesses, suspects, subject and responding police officer, summary and administrative data pertaining to preparation and distribution of the report, basis for allegations, serious or sensitive incident reports, modus operandi and other investigative information from Federal, State, and local investigative and intelligence agencies and departments. Indices contain codes for the type of crime, location of investigation, year and date of offense, names and personal identifiers consisting of photos, driver license numbers, Service component, organization, sex, marital status, height, weight, eye color, hair color, race, ethnicity,

complexion, nation of origin, home and work telephone numbers, and citizenship of persons who have been subjects of electronic surveillance, suspects, subjects, victims, and witnesses (for example, informants and sources of information) of crimes, report number which allows access to records noted above; agencies, firms, Army and Defense of Department organizations which were the subjects or victims of criminal investigations, and disposition and suspense of offenders listed in criminal investigative case files.

RECORD SOURCE CATEGORIES: The individual; subjects; suspects; victims; informants; sources; witnesses; Military Police and/or USACIDC special agents and criminal analysts; investigative and law enforcement persons of Federal, State, local, and foreign government agencies; third parties when pertinent information is furnished.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act of 1974, as amended, the records contained in this system may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. Section 552a(b)(3) as follows:

a. To the appropriate Federal, State, local and/or foreign law enforcement agencies in accomplishing and enforcing criminal laws concerning criminal or possible criminal activity; analyzing modus operandi, detecting organized criminal activity, or criminal justice employment.

b. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of criminal intelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland

security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

c. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or of which they were a victim.

d. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

e. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

f. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

g. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 USC 2904 and 2906.

h. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

i. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

j. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper records are maintained in file folders; electronic storage media, in accordance with the safeguards as stated below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: By the individual's full, name; aliases or other names used (for example, maiden name); date of birth; place of birth; SSN and/or DoD ID. Without SSN the record may not be located or take additional time to locate.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Criminal investigative case files are retained for 50 years after final action pursuant to Public Law 112-81 and DoD Instruction 5505.18, Investigation of Adult Sexual Assault in the

Department of Defense, except that at USACIDC subordinate elements, such files are retained from 1 to 5 years depending on the level of such unit and the data involved.

Criminal intelligence reports are destroyed when no longer needed. Except reports containing information of current operation value may be kept and reviewed yearly for continued retention, not to exceed 20 years. Group headquarters destroy after 5 years. Battalion and field office elements destroy after 3 years or when no longer needed. Laboratory reports at the USACIDC laboratory related to: (1) sexual assault investigations and (2) cases determined to be of historical value, will be maintained in the associated law enforcement database for each Service and are destroyed after 50 years. All other laboratory files are retained for 25 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Paper and electronic records are protected in accordance with policies in DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI). Records are stored on servers in secured buildings. Physical access requires identification and is limited to individuals having an official requirement for entry. System data are encrypted, and access to data and data storage is controlled and limited to authorized personnel who are properly trained, screened, and cleared for need-to-know, and access is further restricted by requiring use of a Common Access Card and PIN and/or strong passwords that are changed periodically according to DOD and Army security policies.

In-depth physical, technical, and administrative controls have been established to safeguard electronic data. Users are required to successfully undergo and complete Tier 5 or Tier 3 security check. Access to the system is managed by the Headquarters, USACIDC access control procedures and policies. All aspects of privacy, security, configuration, operations, data

retention, and disposal are documented to ensure privacy and security are consistently enforced and maintained.

RECORD ACCESS PROCEDURES: Individual(s) seeking access to information about themselves contained in this system should address written requests to the Director, U.S. Army Crime Records Center, U.S. Army Criminal Investigation Command, ATTN: CICR-FP, 27130 Telegraph Road, Quantico, VA 22134-2253. Signed, written requests should contain the individual's full name, any aliases or other names used (e.g., maiden name), current street address, date of birth, place of birth, telephone number, email address, and social security number (optional, but record are more difficult to locate without it). The individual must provide a legible copy of a government identification (e.g., driver's license).

CONTESTING RECORD PROCEDURES: The Army's rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 505, the Army Privacy Program and AR 25-22, The Army Privacy Program, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individual(s) seeking access to information about themselves contained in this system should address written requests to the Director, U.S. Army Crime Records Center, U.S. Army Criminal Investigation Command, ATTN: CICR-FP, 27130 Telegraph Road, Quantico, VA 22134-2253. Signed, written requests should contain the individual's full name, any aliases or other names used (e.g., maiden name), current street address, date of birth, place of birth, telephone number, email address, and social security number (optional, but record are more difficult to locate without it). The individual must provide a legible copy of a government identification (e.g., driver's license).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(2), but only to the extent that such material would reveal the identity of a confidential source.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 505. For additional information contact the system manager.

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].