



DEPARTMENT OF THE ARMY
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
27130 TELEGRAPH ROAD
QUANTICO, VA 22134-2253

CIIM-ZA

MEMORANDUM THRU Army Privacy Office (AAHS-RDF), 7701 Telegraph Road,
Casey Building, Alexandria, VA 22315-3802

FOR Defense Privacy, Civil Liberties, and Transparency Division, 4800 Mark Center
Drive, Alexandria, VA 22350-3100

SUBJECT: Justification for the Use of the Social Security Number (SSN) – Criminal
Investigative Management System (CIMS), DITPR #1616

1. This memorandum is to satisfy the requirements of DoDI 1000.30 (Reduction of Social Security Number (SSN) Use Within the DoD), 1 August 2012, pertaining to justification to collect and use the SSN.

2. The CIMS is a collection of mission essential information technology systems that supports the U.S. Army Criminal Investigation Command (CID) and the Office of the Provost Marshal General (OPMG). Through 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 Law Enforcement 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). The 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. The following systems are registered as child dependencies of CIMS:

- a. Centralized Operations Police Suite (COPS) (DITPR #2822).
- b. Resource Management Online (RM Online) (DITPR #5189).

The SSN is necessary to link appropriate identification information to new agents and identify individuals for law enforcement purposes. It is the only Personally Identifiable Information that is exclusively unique to an individual. The DoD identification number cannot be utilized as Army Law Enforcement frequently indexes individuals who have no DoD affiliation.

CIIM-ZA

SUBJECT: Justification for the Use of the Social Security Number (SSN) – Criminal Investigative Management System (CIMS), DITPR #1616

3. The applicable acceptable uses for collection and use of the SSN are (2), Law Enforcement, National Security, and Credentialing; (5) Confirmation of Employment Eligibility.

4. The forms and the System of Records Notices associated with the CIMS system are as follows: DA Form 2823, Sworn Statement; DA Form 3946, Military Traffic Accident Report; DA Form 3881, Rights Waiver; A0190-45 OPMG, Criminal Investigative Management System.

5. Authorities supporting collection of the SSN are: 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 (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); AR 195-6 (Department of the Army Polygraph Activities); and E.O. 9397 (SSN), as amended.

6. Multiple steps are taken to protect the SSN utilized in the CIMS environment. Information in the system is collected, stored, and maintained in a secure 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.

7. The point of contact for this action is Ms. Lee S. Borden at (571) 305-4065 or lee.s.borden.civ@mail.mil.

DAVID P. GLASER
Major General, USA
Commanding