



Department of Defense INSTRUCTION

NUMBER 5505.17

December 19, 2012

Incorporating Change 1, Effective November 29, 2016

IG DoD

SUBJECT: Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities

References: See Enclosure

1. **PURPOSE.** This Instruction, in accordance with the guidance in DoD Directive (DoDD) 5200.27 (Reference (a)) and the authority in DoDD 5106.01 (Reference (b)), establishes policy, assigns responsibilities, and prescribes procedures for DoD law enforcement activities (LEAs) to collect, maintain, use, and disseminate personally identifiable information (PII) and law enforcement information during law enforcement functions (e.g., crime prevention, force protection, and criminal investigations).

2. **APPLICABILITY.** This Instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components.”)

b. Applies only to DoD personnel (military and civilian) performing law enforcement functions in accordance with Title 10 or Title 18 of the United States Code (References (c) and a(d)) or other authorities, and contractors supporting such DoD personnel.

c. Does not apply to defense intelligence or counterintelligence activities. Executive Order 12333 (Reference (e)), DoD 5240.1-R (Reference (f)), and DoDD 5240.01 (Reference (g)) govern the collection, retention, and dissemination of information concerning U.S. persons during defense intelligence or counterintelligence activities.

d. Does not limit or supersede any provisions of current DoD Directives, Instructions, or applicable law conferring the authority and responsibility on the DoD LEAs to enforce law, conduct criminal investigations, or protect DoD personnel and property. However, the

Instruction does clarify limitations on the collection, maintenance, use, and dissemination of PII and law enforcement information during law enforcement functions and cautions DoD LEAs when undertaking proactive measures to prevent or deter crime.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. DoD LEAs may collect, use, maintain, and disseminate PII and law enforcement information in compliance with section 552a of title 5, United States Code (also known as “The Privacy Act of 1974”) (Reference (h)), implemented in the DoD by DoDD 5400.11 (Reference (i)) and DoD 5400.11-R (Reference (j)). DoD LEAs shall also comply with privacy and civil liberties protections afforded by the U.S. Constitution and other Federal law when performing their authorized functions.

b. When proposing, developing, and implementing DoD Directives, Instructions, and Publications and other guidance that retains or enhances a particular authority, the DoD LEAs shall balance the need to exercise that authority with the need to protect privacy and civil liberties; provide adequate guidelines and oversight to properly confine its collection, use, maintenance, and dissemination; and ensure adequate protections exist to protect privacy and civil liberties in accordance with applicable laws and DoD policies.

5. RESPONSIBILITIES

a. IG DoD. The IG DoD shall monitor and evaluate compliance with this Instruction.

b. Heads of the DoD Components. The Heads of the DoD Components shall ensure compliance with and prescribe procedures to implement this Instruction.

6. PROCEDURES

a. DoD LEAs may collect PII and other information in the course of law enforcement functions, to include investigations, where that information logically relates to the detection, neutralization, or deterrence of criminal activity that affects DoD personnel, property, or mission. PII and law enforcement information will be managed in accordance with References (h) through (j) and the DoD Component's records disposition requirements. If, during the course of an otherwise lawful law enforcement function, DoD LEAs collect information related to criminal activity that does not have a DoD nexus, that information shall be forwarded to the appropriate law enforcement activity with jurisdiction over the matter. A record of this dissemination must be kept by the DoD LEA.

b. Dissemination of PII: PII collected by LEAs may be disseminated in accordance with References (h) through (j) and other applicable authorities. Examples of appropriate dissemination include dissemination to:

(1) Other U.S. LEAs with a need to know for law enforcement rather than administrative purposes.

(2) U.S. intelligence organizations with a need to know.

(3) Criminal justice authorities with jurisdiction over the matter, such as the Department of Justice, U.S. Attorney's Office, state prosecutors, and military officials responsible for the administration of military justice (e.g., staff judge advocates, trial counsel, and convening authorities), in accordance with chapter 47 of Reference (c) (also known and referred to in this Instruction as the "Uniform Code of Military Justice (UCMJ)," for those persons subject to the UCMJ.

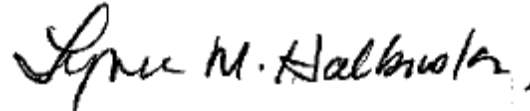
(4) Other DoD Components, which require the information to make determinations regarding debarment, eligibility to hold security clearances, special access, suitability determinations and other administrative determinations. The recipient DoD Component may not make a law enforcement record a permanent part of its system of records without prior coordination with the originating LEA.

7. INFORMATION COLLECTION. PII and other information collected by LEAs, referred to throughout this issuance, does not require licensing with a report control symbol in accordance with paragraph 1b(2) and (8) of Enclosure 3 of Volume 1 of DoD Manual 8910.01 (Reference (k)), or an Office of Management and Budget (OMB) control number in accordance with paragraph 8a(2)(a) and (b) of Enclosure 3 of Volume 2 of DoDM 8910.01 (Reference (l)).

8. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update references for accuracy and add the information collection section in section 7 above.

9. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

9. EFFECTIVE DATE. This Instruction is effective December 19, 2012.

A handwritten signature in black ink that reads "Lynne M. Halbrooks". The signature is written in a cursive, flowing style.

Lynne M. Halbrooks
Principal Deputy
Performing the Duties of the
Inspector General of the
Department of Defense

Enclosure
References
Glossary

ENCLOSURE

REFERENCES

- (a) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (b) DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012
- (c) Title 10, United States Code
- (d) Title 18, United States Code
- (e) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (f) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982
- (g) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
- (h) Title 5, United States Code
- (i) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- (j) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (k) DoD Manual 8910.01, Volume 1, "DoD Information Collections: Procedures for DoD Internal Information Collections," June 30, 2014
- (l) DoD Manual 8910.01, Volume 2, "DoD Information Collections: Procedures for DoD Public Information Collections," June 30, 2014
- (m) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),", November 23, 2005

GLOSSARY

PART I. ABBREVIATIONS AND ACONYMS

DoDD	DoD Directive
DoDI	DoD Instruction
IG DoD	Inspector General of the Department of Defense
LEA	law enforcement activity
PII	personally identifiable information
UCMJ	Uniform Code of Military Justice

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

crime prevention. Law enforcement or security procedures undertaken to discourage criminal acts.

criminal investigation. Investigation into alleged or apparent violations of law undertaken for purposes which include the collection of evidence in support of potential criminal prosecution.

criminal threat. Information disclosed to or obtained by law enforcement personnel that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained investigator to presume a threat of criminal activity exists and that the threat will affect DoD personnel or property without employing law enforcement countermeasures to lessen or stop the threat. Indiscriminate criminal activity that occurs miles away from an installation or DoD function does not constitute a credible criminal threat unless that entity has the ability to affect an installation, DoD function, or their personnel from a distance.

defense counterintelligence. Defined in DoDD 5143.01 (Reference (m)).

defense intelligence. Defined in Reference (m).

DoD LEA. An agency or organization, or any subdivision thereof, chartered and empowered to enforce the criminal laws of the United States on DoD property or during DoD functions anywhere in the world. A traditional DoD law enforcement activity that employs recognized law enforcement officers are those organizations designated for the security or protection of DoD property, personnel, or places that are subject to the jurisdiction, administration, or in the custody of the Department.

Examples are the Pentagon Police Department, National Security Agency Police Department, U.S. Army Military Police, U.S. Navy Masters-at-Arms, U.S. Air Force Security Forces, U.S. Marine Corps Military Police, and the Service correctional commands. These activities as designated may take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property.

Other examples of a DoD law enforcement activity are the DoD Inspector General and the Defense Criminal Investigative Organizations (i.e., Defense Criminal Investigative Service, U.S. Army Criminal Investigation Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations). These activities are designated to provide oversight or engage in work related to the planning, conducting, or managing of criminal investigations related to alleged or suspected criminal violations of Federal laws and the UCMJ.

force protection. Preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

law enforcement functions. Lawful acts or services performed by certified or credentialed personnel empowered to enforce criminal laws that deter or prevent crime. The primary functions of DoD law enforcement officers are crime prevention, force protection, and criminal investigations.

PII. Defined in References (h) and (l).

system of records. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

valid DoD law enforcement purpose. An independent DoD purpose intended to maintain law and order on DoD property as well as protect the force from credible criminal threats.