



## DoD INSTRUCTION 5505.17

# PERSONALLY IDENTIFIABLE INFORMATION AND LAW ENFORCEMENT INFORMATION HANDLING BY DoD LAW ENFORCEMENT ACTIVITIES

---

|                               |  |
|-------------------------------|--|
| <b>Originating Component:</b> | Office of Inspector General of the Department of Defense   |
| <b>Effective:</b>             | August 22, 2023  |
| <b>Releasability:</b>         | Cleared for public release. Available on the Directives Division Website at <a href="https://www.esd.whs.mil/DD/">https://www.esd.whs.mil/DD/</a> .  |
| <b>Reissues and Cancels:</b>  | DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012, as amended |
| <b>Approved by:</b>           | Robert P. Storch, Inspector General of the Department of Defense   |

---

**Purpose:** In accordance with the authority in DoD Directive (DoDD) 5106.01 and operational guidance in DoDD 5200.27, this issuance 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 such as crime prevention, force protection, and criminal investigations.

## TABLE OF CONTENTS

|   |    |
|---|----|
| SECTION 1: GENERAL ISSUANCE INFORMATION ..... | 3  |
| 1.1. Applicability. ....                      | 3  |
| 1.2. Policy. ....                             | 3  |
| 1.3. Information Collections. ....            | 4  |
| SECTION 2: RESPONSIBILITIES .....             | 5  |
| 2.1. IG DoD.....                              | 5  |
| 2.2. DoD Component Heads. ....                | 5  |
| SECTION 3: PROCEDURES .....                   | 6  |
| 3.1. Collection. ....                         | 6  |
| 3.2. Dissemination. ....                      | 6  |
| 3.3. Handling.....                            | 7  |
| GLOSSARY .....                                | 8  |
| G.1. Acronyms. ....                           | 8  |
| G.2. Definitions.....                         | 8  |
| REFERENCES .....                              | 11 |

## **SECTION 1: GENERAL ISSUANCE INFORMATION**

### **1.1. APPLICABILITY.**

This issuance:

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 Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

b. Applies only to DoD personnel (military and civilian) performing law enforcement functions or physical security duties in accordance with Title 10 or Title 18 of the United States Code (U.S.C.) or other authorities, and contractors supporting such DoD personnel.

c. Does not apply to defense intelligence activities. Executive Order 12333, DoDD 5240.01, and DoD Manual 5240.01 govern the collection, retention, and dissemination of information concerning U.S. persons during DoD intelligence 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.

e. Clarifies 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.

f. Nothing in this issuance will infringe on the IG DoD’s statutory independence and authority in accordance with the Inspector General Act of 1978, as amended and specified in Chapter 4 of Title 5, U.S.C. In the event of any conflict between this issuance and the IG DoD’s statutory independence and authority, the Inspector General Act of 1978 takes precedence.

### **1.2. POLICY.**

a. DoD LEAs may collect, use, maintain, and disseminate PII and law enforcement information in compliance with Section 552a of Title 5, U.S.C. (also known as the “Privacy Act of 1974”), implemented in the DoD by DoD 5400.11-R and DoD Instruction (DoDI) 5400.11. DoD LEAs must also comply with privacy and civil liberties protections afforded by the U.S. Constitution and other Federal law when performing their authorized functions.

b. DoD LEAs must:

(1) Balance the need to exercise authority with the need to protect privacy and civil liberties when proposing, developing, and implementing DoD issuances and other guidance that retains or enhances any authority.

(2) Provide adequate guidelines and oversight to properly confine their collection, use, maintenance, and dissemination of PII and law enforcement information, while properly marking such information as controlled unclassified information in accordance with DoDI 5200.48 or, when appropriate, with the proper classification markings pursuant to Volume 1 of DoD Manual 5200.01 and the controlling security classification guide.

(3) Ensure adequate protections exist to protect privacy and civil liberties in accordance with applicable laws and DoD policies.

### **1.3. INFORMATION COLLECTIONS.**

PII and law enforcement information collected by DoD LEAs, referred to throughout this issuance, do not require:

a. Licensing with a report control symbol in accordance with Paragraph 1.b., Enclosure 3, Volume 1 of DoD Manual 8910.01; or

b. An Office of Management and Budget control number in accordance with Paragraphs 8a(2)(a) and (b), Enclosure 3, Volume 2 of DoD Manual 8910.01.

## **SECTION 2: RESPONSIBILITIES**

### **2.1. IG DOD.**

The IG DoD monitors and evaluates compliance of DoD Components with this issuance.

### **2.2. DOD COMPONENT HEADS.**

The DoD Component heads must ensure compliance with, and prescribe procedures to implement, this issuance.

## SECTION 3: PROCEDURES

### 3.1. COLLECTION.

- a. DoD LEAs may collect PII and law enforcement information during 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 missions.
- b. PII and law enforcement information will be managed in accordance with Title 5, U.S.C., DoD 5400.11-R, DoDI 5400.11, and the DoD Component's records disposition requirements.
- c. If, during an otherwise lawful law enforcement function, DoD LEAs collect information related to criminal activity that does not have a DoD nexus, that information will be forwarded to the appropriate agency that has jurisdiction over the matter.
- d. The DoD LEA must retain a record of this dissemination in the investigation or information file. The investigation or information file will be retained in compliance with DoD, Service, and DoD LEA records retention policies.

### 3.2. DISSEMINATION.

PII collected by DoD LEAs may be disseminated in accordance with Title 5, U.S.C., DoD 5400.11-R, DoDD 5205.16, DoDI 5400.11, and other applicable authorities. Examples of appropriate dissemination include dissemination to:

- a. Other agencies in the United States that have a need to know for law enforcement purposes.
- b. U.S. intelligence organizations that have a need to know.
- c. Criminal justice authorities that have 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 (such as staff judge advocates, trial counsel, and convening authorities), in accordance with Chapter 47 of Title 10, U.S.C., also known and referred to in this issuance as the "Uniform Code of Military Justice (UCMJ)," for those persons subject to the UCMJ.
- d. Other DoD Components that require the information to detect and mitigate insider threats and to make debarment, security clearance eligibility, special access suitability, and other administrative determinations. The receiving DoD Component may not make a law enforcement record a permanent part of its system of records without prior coordination with the originating DoD LEA.

e. Other DoD Components that may receive aggregate or statistical law enforcement information, provided such information does not contain PII, for the purposes of assessing issues impacting military members, DoD civilians, and others in the DoD community.

### **3.3. HANDLING**

DoD LEAs will mark and handle documents and records containing PII or law enforcement information as controlled unclassified information in accordance with DoDI 5200.48 or, when appropriate, with the proper classification markings pursuant to Volume 1 of DoD Manual 5200.01 and the controlling security classification guide.

## GLOSSARY

### G.1. ACRONYMS.

| ACRONYM | MEANING  |
|---------|--|
| 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               |
| U.S.C.  | United States Code                             |

### G.2. DEFINITIONS.

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

| TERM                          | DEFINITION  |
|-------------------------------|---|
| <b>counterintelligence</b>    | Defined in DoDD 5143.01.  |
| <b>crime prevention</b>       | Law enforcement or security procedures that are conducted to discourage criminal acts.  |
| <b>criminal investigation</b> | An investigation into reported or apparent violations of law that is conducted for purposes that include the collection of evidence in support of potential criminal prosecution.   |
| <b>criminal threat</b>        | 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. |
| <b>defense intelligence</b>   | Defined in DoDD 5143.01.  |

| <b>TERM</b>                        | <b>DEFINITION</b>   |
|------------------------------------|---|
| <b>DoD LEA</b>                     | <p>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 LEA 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.</p> <p>Examples are the Pentagon Force Protection Agency, National Security Agency Police, U.S. Army Military Police and Military Police Investigations, U.S. Navy Masters-at-Arms and Masters-at-Arms Investigations, U.S. Air Force Security Forces and Security Forces Investigations, U.S. Marine Corps Military Police and Criminal Investigation Division, and the Service correctional commands. These activities, as designated, may take reasonably necessary and lawful measures to maintain law and order to protect installation personnel and property.</p> <p>Other examples of a DoD LEA are the DoD Office of Inspector General and the Defense Criminal Investigative Organizations (Defense Criminal Investigative Service, U.S. Army Criminal Investigation Division, 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 reported or suspected criminal violations of Federal laws and the UCMJ.</p> |
| <b>force protection</b>            | <p>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.</p>   |
| <b>law enforcement functions</b>   | <p>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 personnel are crime prevention, force protection, and criminal investigations.</p>   |
| <b>law enforcement information</b> | <p>Information collected 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.</p>   |

| <b>TERM</b>                              | <b>DEFINITION</b>  |
|--|--|
| <b>PII</b>                               | Defined in Office of Management and Budget Circular A-130. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.    |
| <b>system of records</b>                 | A group of records under the control of a DoD Component from which personal information about an individual can be retrieved by the individual's name, identifying number, symbol, or other information that is assigned and unique to the individual. |
| <b>valid DoD law enforcement purpose</b> | An independent DoD purpose intended to maintain law and order on DoD property, as well as protect the force from credible criminal threats.  |

## REFERENCES

- DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- DoD Directive 5106.01, “Inspector General of the Department of Defense (IG DoD),” April 20, 2012, as amended
- DoD Directive 5143.01, “Under Secretary of Defense for Intelligence and Security (USD(I&S)),” October 24, 2014, as amended
- DoD Directive 5200.27, “Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense,” January 7, 1980
- DoD Directive 5205.16, “The DoD Insider Threat Program,” September 30, 2014, as amended
- DoD Directive 5240.01, “DoD Intelligence Activities,” August 27, 2007, as amended
- DoD Instruction 5200.48, “Controlled Unclassified Information (CUI),” March 6, 2020
- DoD Instruction 5400.11, “DoD Privacy and Civil Liberties Programs,” January 29, 2019, as amended
- DoD Manual 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012, as amended
- DoD Manual 5240.01, “Procedures Governing the Conduct of DoD Intelligence Activities,” August 8, 2016
- DoD Manual 8910.01, Volume 1, “DoD Information Collections Manual: Procedures for DoD Internal Information Collections,” June 30, 2014, as amended
- DoD Manual 8910.01, Volume 2, “DoD Information Collections Manual: Procedures for DoD Public Information Collections,” June 30, 2014, as amended
- Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended<sup>1</sup>
- Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource,” July 28, 2016
- United States Code, Title 5
- United States Code, Title 10
- United States Code, Title 18

---

<sup>1</sup> Available on the National Archives Federal Register website at: <https://www.federalregister.gov/d/E8-17940>