Department of Defense
INSTRUCTION

NUMBER 5525.18
October 18, 2013
Incorporating Change 3, Effective October 1, 2020

USD(I&S)

SUBJECT: Law Enforcement Criminal Intelligence (CRIMINT) in DoD

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Establishes policy and assigns responsibilities for DoD law enforcement (LE) CRIMINT in accordance with the authority in DoD Directive 5143.01 and June 29, 2018 Deputy Secretary of Defense approval of the Under Secretaries of Defense for Personnel and Readiness/Intelligence memorandum (Reference (a) and (b)), and Secretary of Defense Correspondence Action Report (Reference (c)).

b. Establishes guidelines and principles for the collection, analysis, and distribution of LE CRIMINT within and externally to the DoD in accordance with the National Criminal Intelligence Sharing Plan (Reference (d)).

2. APPLICABILITY. This instruction:

a. Applies to:

(1) 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, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

(2) DoD LE officers (LEOs), including police officers, criminal investigators, LE CRIMINT analysts (General Schedule (GS) 1800 and 0100 series as defined in U.S. Office of Personnel Management, "Handbook of Occupational Groups and Families" (Reference (e)), and supporting personnel who are assigned, attached, or detailed to DoD LE agencies (LEAs).

b. Does not apply to:

(1) Security officers: Security Administration (GS 0080 series) or Civilian Security Guards (GS 0085 series) as defined in Reference (e), who are not assigned, attached, or detailed to DoD LEAs.

(2) Antiterrorism and force protection officers: Military and Civilian Security Administration (GS 0080 series) as defined in Reference (e), who are not assigned, attached, or detailed to DoD LEAs.

(3) Counterintelligence personnel.

(4) Corrections specialists who are not DoD LEOs as defined in the Glossary.

(5) Intelligence activities as identified in Executive Order (E.O.) 12333 (Reference (f)) and DoD 5240.1-R (Reference (g)).

3. POLICY. It is DoD policy that:

a. CRIMINT gathering is a fundamental and essential element in the all-encompassing duties of all DoD LEAs.

(1) Intelligence-led policing executed by DoD LEAs focuses CRIMINT gathering at the local military crime unit level so as to protect DoD functions and property, military and civilian personnel, and defense activities and installations. As such, CRIMINT is a mission enabler in DoD operations.

(2) Protective intelligence (PI) executed by DoD LEAs focuses CRIMINT gathering on the specific mission of protecting DoD personnel and property, and especially assigned high risk personnel (HRP). As such, PI can aid in identifying threats, preventing terrorist acts directed at DoD, and capturing evidence necessary for conviction. When threats are identified through a threat assessment process, vulnerability assessments can be conducted and a thorough analysis of all potential danger may be evaluated.

b. When acquired, CRIMINT can aid in crime prevention, threat disruption, offender pursuit and apprehension, and evidence capture necessary for conviction.

c. CRIMINT gathering by DoD LEAs against specific individuals or organizations that are reasonably suspected, as defined in Part 23 of Title 28, Code of Federal Regulations (Reference (g)), of being potentially involved in a definable criminal activity or enterprise affecting DoD interests can occur provided the respect for the rights of those involved are upheld in accordance with DoD Instruction 5400.11 (Reference (i)) and all applicable laws and policies.

d. In accordance with DoD Directive 5200.27 (Reference (j)) the gathering of CRIMINT and PI regarding persons without a connection to DoD or reasonable expectation of threat or direction of interest toward DoD personnel or facilities is prohibited.

e. DoD CRIMINT collection, maintenance, use, and dissemination of personally identifiable information and law enforcement information will occur in accordance with DoD Instruction (DoDI) 5505.17 (Reference (k)), as applicable.

f. DoD CRIMINT dissemination may occur under the USA Patriot Act (Reference (l)) requirements for information sharing.

g. Gathered CRIMINT and PI will be retained in electronic files as stipulated by agency or organization procedures

h. This policy does not affect existing policies governing:

(1) DoD intelligence and counterintelligence component activities. DoD intelligence and counterintelligence components collect, retain, and disseminate information concerning U.S. persons pursuant to procedures set forth in References (f) and (g).

(a) DoD intelligence component personnel assigned to LEAs to perform CRIMINT functions are subject to the provisions of this instruction.

(b) DoD intelligence component personnel assigned or attached to LEAs to perform intelligence functions are subject to the provisions of Reference (g).

(2) DoD Component acquisition of information concerning non-DoD personnel and organizations. DoD non-intelligence components may acquire information concerning non-DoD personnel and organizations and share terrorism information in accordance with References (j) and (k), and E.O. 13388 (Reference (m)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release.** This instruction is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 3. This administrative change updates:

a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92 (Reference (n)).

b. Administrative changes in accordance with current standards of the Office of the Chief Management Officer of the Department of Defense.

8. EFFECTIVE DATE. This instruction is effective October 18, 2013.

Jessica L. Wright
Acting Under Secretary of Defense for
Personnel and Readiness

Change # 2 (Switching office of primary
responsibility to OUSD(Intelligence))
Approved 8/9/2019 by:
Joseph D. Kernan
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. CRIMINT Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
(b) Under Secretary of Defense for Personnel and Readiness and Under Secretary of Defense for Intelligence Memorandum, "DoD Directive 5525.IC, Protection of Buildings, Grounds, Property, and Persons, and Implementation of Section 2672 of Title 10, United States Code," May 21, 2018[1]
(c) Secretary of Defense Correspondence Action Report, "Lead for Integrating DoD Crime Databases into a Federal System," August 2, 2005
(d) Department of Justice, "National Criminal Intelligence Sharing Plan," October 2003[2]
(e) U.S. Office of Personnel Management, "Handbook of Occupational Groups and Families," May 2009
(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(g) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982, as amended
(h) Part 23 of Title 28, Code of Federal Regulations
(i) DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019
(j) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
(k) 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
(l) Title VII of Public Law 107-56, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001," October 26, 2001
(m) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
(n) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019
(o) International Association of Law Enforcement Intelligence Analysts (IALEA)[3], as amended
(p) United States Northern Command Force Protection Directive 11-100, "Information Reporting Requirements," April 10, 2011
(q) Secretary of Defense Executive Order for Standup of United States Northern Command Continental United States Antiterrorism-Force Protection Responsibility, DTG 071901Z, May 2004
(r) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended

[1] Action 2 approved by the Deputy Secretary of Defense June 29, 2018. Available from Chief, Law Enforcement, Office of the Under Secretary of Defense for Intelligence and Security
[2] Available at http://www.it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf.
[3] IALEIA resources available at http://www.ialeia.org.

(s) DoD Instruction O-2000.22, "Designation and Physical Protection of DoD High-Risk Personnel," June 19, 2014, as amended
(t) DoD Instruction 2000.12, "DoD Antiterrorism (AT) Program," March 1, 2012, as amended
(u) DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY. The Under Secretary of Defense for Intelligence and Security:

a. Develops and maintains policy for LE CRIMINT within DoD.

b. Monitors compliance with this instruction.

c. Represents DoD in interagency and professional association forums, councils, and working groups concerning LE CRIMINT.

2. INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE. The Inspector General of the Department of Defense monitors compliance with this instruction as it relates to the Defense Criminal Investigative Organizations.

3. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense provides advice and assistance on all legal matters, including the review and coordination on all proposed policies, DoD issuances, and proposed exceptions to the DoD policies regarding LE CRIMINT.

4. DoD COMPONENT HEADS WITH ASSIGNED LE AGENCIES OR ACTIVITIES. The DoD Component heads with assigned LEAs or activities:

a. Ensure compliance with this instruction.

b. Develop policy and procedures supporting the establishment of LE CRIMINT capabilities within their Component.

c. Establish and maintain an LE CRIMINT function within their LEAs.

ENCLOSURE 3

CRIMINT PROCEDURES

1. MISSION. The purpose of DoD LE CRIMINT activities is to prevent crime and aid enforcement objectives identified by DoD LEAs. This is done by gathering information from sources, in a manner consistent with the law, to provide tactical and strategic LE CRIMINT on the existence, identities, and capabilities of criminal suspects and organizations.

2. ORGANIZATION

a. The LE CRIMINT function will be organized at the discretion of the heads of the Military Services and Defense Agencies.

b. The organization of LE CRIMINT within the Military Service and Defense Agency LEAs can include installation-level policing and criminal investigative services.

c. Authorities, missions, and functional requirements will drive the degree of collaboration between CRIMINT and other DoD LE functions performed by Military Services and Defense Agencies.

3. PROFESSIONAL STANDARDS

a. Information gathering for LE CRIMINT purposes will be premised on circumstances that provide a reasonable suspicion, as defined in Reference (h), that specific individuals or organizations may be planning or engaging in criminal activity having a connection to DoD.

b. LE CRIMINT techniques employed will be lawful to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

c. DoD LEAs will maintain records of the source of information received during the conduct of CRIMINT functions.

d. Information gathered and maintained by a component LEA for CRIMINT purposes may be disseminated only to appropriate persons for legitimate LE purposes in accordance with law and procedures established by that agency.

e. CRIMINT having potential force protection implications, but not reaching the threshold of imminent danger to DoD interests, may be sanitized, thus supporting broader dissemination to DoD organizations with force protection responsibilities not directly involved in LE activities.

4. CRIMINT GATHERING

a. CRIMINT data that should be captured include, but are not limited to:

(1) Subject, victim(s), and complainant information as allowed by relevant law and policy.

(2) A summary of suspected criminal activity.

(3) Anticipated results and outcomes.

(4) Problems with or operational and legal restraints to CRIMINT collection, or conflicts of interest.

b. LEAs will not retain CRIMINT or other official documentation for personal reference or other purposes or beyond statutory timelines for expungement.

c. CRIMINT will be gathered in a legally accepted manner and in accordance with procedures established for their use by DoD and specifically for that DoD LEA.

d. All local, State, regional, and federal civilian criminal justice agencies (CJAs) and CRIMINT sharing systems are authorized sources of information in the information-gathering process.

5. RECEIPT, EVALUATION, AND RETENTION OF INFORMATION

a. Information, documents, and reports related to criminal activity will be provided to the LEA with primary responsibility for the matter. The material remains the property of the LEA with primary responsibility and will be further disseminated only with that agency's consent.

b. When information is received in any form, it will be evaluated for reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible to guide others in using the information.

c. Written evaluations of CRIMINT will be retained when completed.

6. ANALYSIS

a. Each DoD LEA's LE CRIMINT function will establish a process to ensure the information gathered is reviewed and analyzed to derive its meaning and value for crime prevention, threat disruption, and the pursuit and apprehension of offenders.

b. LEA CRIMINT analysts whose professional training and practical experiences are consistent with the professional standards articulated by the International Association of LE Intelligence Analysts (Reference (o)) will perform the analysis.

7. DISSEMINATION AND INFORMATION SHARING

a. All restricted files will be secured, and the originating LEAs will establish procedures to control access to all CRIMINT information.

b. Analytic material (e.g., tactical or strategic CRIMINT) will be compiled and provided to authorized recipients as soon as possible when meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals emerge.

c. CRIMINT relevant to active cases or that requires immediate attention will be forwarded to responsible investigative personnel as soon as possible.

d. The fusion of CRIMINT with other intelligence and subsequent sharing within and outside of DoD will rest with the DoD Component's normal threat fusion function.

e. Sanitized, domestic force protection threat information, as defined by United States Northern Command (USNORTHCOM) Force Protection Directive 11-100 (Reference (p)), collected as part of the LE CRIMINT process, may be shared with the USNORTHCOM LE Threat Information Cell under the authority of Secretary of Defense Execute Order (Reference (q)), in accordance with Reference (p). Originating LEAs control their CRIMINT shared with USNORTHCOM.

f. Sanitized LE CRIMINT will be shared with DoD non-CJAs whose missions include responsibilities for DoD insider terrorist threats, foreign terrorist threats, and antiterrorism/force protection measures as defined by DoD Instruction 5420.26 (Reference (r)), HRP as defined in DoD Instruction O-2000.22 (Reference (s)), References (f) and (g), and DoD Instruction 2000.12 (Reference (t)). Originating LEAs retain responsibility for LE CRIMINT shared with a DoD non-CJA.

(1) DoD non-CJAs are authorized, under regulations described in paragraph 7f(2), to review the provided LE CRIMINT and determine whether to retain it based on the reasonable belief of foreign connection, including but not limited to international terrorism, counterintelligence, counternarcotics, personnel security, physical security, and safety.

(2) DoD non-CJA use of LE CRIMINT will conform to the regulations cited in this paragraph and all other intelligence oversight regulations, and all necessary steps will be taken to protect the security and integrity of the information.

(3) All DoD non-CJAs will coordinate with the appropriate DoD LEA to determine further dissemination requirements to protect criminal and non-criminal investigations and potential criminal prosecution.

(4) Based on their use and analysis of the LE CRIMINT, DoD non-CJAs will also provide investigative support or leads and analytic feedback to originating LEAs as appropriate.

g. CRIMINT may be shared with local, State, tribal, federal, regional, and international civilian CJAs and CRIMINT sharing systems under terms of reciprocity established by the DoD LEA and counterpart civilian LEA or CRIMINT sharing system.

8. DISSEMINATION CONTROL MARKINGS OF LE CRIMINT

a. CRIMINT files will be restricted to protect sources, investigations, and individuals' rights to privacy, as well as to provide a structure that will enable agencies to control access to CRIMINT.

b. Unless otherwise stated, CRIMINT will be marked with "LAW ENFORCEMENT SENSITIVE (LES)" including an LES distribution limitation statement detailed in accordance with DoDI 5200.48 (Reference (u)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CJA	criminal justice agency
CRIMINT	criminal intelligence
DoDI	DoD instruction
E.O.	Executive Order
GS	General Schedule
HRP	high risk personnel
LE	law enforcement
LEA	law enforcement agency
LEO	law enforcement officer
LES	law enforcement sensitive
PI	protective intelligence
USNORTHCOM	United States Northern Command

PART II. DEFINITIONS

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

CRIMINT. Defined in Reference (d).

criminal justice agency. The courts, a governmental agency, or any subunit of a governmental agency that performs the administration of criminal justice pursuant to a statute or E.O. and that allocates a substantial part of its annual budget to the administration of criminal justice. Includes State and federal inspectors general offices.

Defense criminal investigative organizations. The four criminal investigative organizations of DoD are the Defense Criminal Investigative Service, U.S. Army Criminal Investigations Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.

DoD LEAs. Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the Office of the Inspector General of the Department of Defense that perform a law enforcement function for those departments and agencies and are staffed by DoD LEOs.

DoD LEO. Military police (Army and Marine Corps), security forces (Air Force), and Masters-at-Arms (Navy) who wear a military uniform with police identification while on duty; and DoD Component civilian police (GS 0083 series or equivalent, consistent with the definitions of "law enforcement officer" in Reference (e)) when credentialed to perform those duties.

Military and civilian (GS 1811, consistent with the definitions of "law enforcement officer" in Reference (e)) criminal investigators (special agents).

Correctional officers (military or civilian employees in job series 0007 or equivalent of Reference (e)).

intelligence-led policing. Executive implementation of the intelligence cycle to support proactive decision making for resource allocation and crime prevention.

military criminal investigative organizations. The three military criminal investigative organizations within the DoD are U.S. Army Criminal Investigations Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.

originating LEA. The LEA that owns the CRIMINT system and the CRIMINT within that system.

PI. CRIMINT used to identify, analyze, and provide leads for investigation into various direct and indirect threats to DoD personnel and property. It may provide further details about persons who may have the interest, motive, intention, and capability of mounting attacks against the DoD and its personnel. Additionally, it can aid DoD LEAs in gauging the potential threat to and vulnerability of a targeted individual or property and may be used in determining or preventing violence.

strategic CRIMINT. Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for short- and long-term investigative goals.

tactical CRIMINT. Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.