



Department of Defense **INSTRUCTION**

NUMBER 5525.16

August 29, 2013

Incorporating Change 3, Effective October 30, 2020

USD(I&S)

SUBJECT: Law Enforcement Defense Data Exchange (LE D-DEx)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. 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)), this instruction establishes policy and assigns responsibilities for law enforcement criminal justice information (CJI) sharing through the LE D-DEx, by the law enforcement agencies (LEAs) of DoD in accordance with the authority in DoD Directive 5525.21 (Reference (c)) and Secretary of Defense Correspondence Action Report (Reference (d)).

b. Designates the LE D-DEx as the authorized DoD integrated CJI sharing system in accordance with the authority in Secretary of Defense Memorandum (Reference (e)).

c. Identifies the duties of the Secretary of the Navy as the DoD Lead Component Head for the LE D-DEx in accordance with the authority in Under Secretary of Defense for (Intelligence) Memorandum (Reference (f)).

d. Establishes the LE D-DEx Board of Governance (BoG) pursuant to DoD Instruction (DoDI) 5105.18 (Reference (g)).

2. APPLICABILITY. This instruction 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, 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").

3. POLICY. It is DoD policy that:

a. DoD LEAs share CJ I across organizational boundaries to enhance the Department's crime prevention and investigative lead sharing.

b. CJ I sharing within DoD must be accomplished through the LE D-DEx.

c. DoD LEAs share complete, accurate, and timely CJ I with counterpart civil LEA to enhance public safety for all jurisdictions concerned.

d. LE D-DEx is DoD's CJ I portal to externally share CJ I with the Federal Bureau of Investigation's (FBI) Law Enforcement National Data Exchange (N-DEx), under the provisions of the Memorandum of Understanding among the Federal Bureau of Investigation and Participating State, Local, Tribal, and Federal Agencies for an Information Sharing Initiative and its Addendum (Reference (h)).

e. As an N-DEx client, LE D-DEx and its participating LEAs will be governed by CJ I collection and sharing rules as defined in section 534 of Title 28, United States Code (U.S.C.) (Reference (i)); part 20 of Title 28, Code of Federal Regulations (Reference (j)); and the FBI's Criminal Justice Information Services (CJIS) Security Policy for N-DEx as defined in CJIS Security Policy (Reference (k)).

f. CJ I sharing with civilian counterpart LEAs must be accomplished through the LE D-DEx linkage with N-DEx.

g. Personally identifiable information (PII) concerning U.S. persons must be handled in strict compliance with section 552a of Title 5, U.S.C., also known and referred to in this instruction as "The Privacy Act of 1974," as amended (Reference (l)), and implemented in the DoD in accordance with DoDI 5400.11 (Reference (m)), DoD 5400.11-R (Reference (n)), and DoDI 5505.17 (Reference (o)).

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/>.

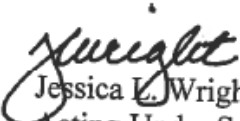
7. INFORMATION COLLECTIONS. The Law Enforcement Defense Data Exchange, referred to throughout this issuance, does not require licensing with a report control symbol or OMB Control Number in accordance with Paragraph 1 of Volume 1 of DoD Manual 8910.01 (Reference (z)) and Paragraph 1 of Volume 2 of DoD Manual 8910.01 (Reference (aa)).

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

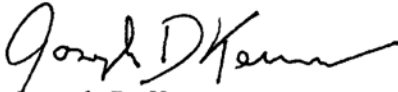
a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92 (Reference (ab)).

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

9. EFFECTIVE DATE. This instruction is effective August 29, 2013


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

Change #2 Approved by:


Joseph D. Kernan
Under Secretary of Defense for Intelligence

Joseph D. Kernan
Under Secretary of Defense for Intelligence

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....7

 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
 (USD(I&S)).....7

 DoD COMPONENT HEADS THAT HAVE LEAs ACTING AS CRIMINAL JUSTICE
 AGENCIES (CJAs) AND PERFORMING ADMINISTRATION OF CRIMINAL
 JUSTICE.....7

 SECRETARY OF THE NAVY.....7

ENCLOSURE 3: PROCEDURES.....9

 OPERATIONAL FRAMEWORK.....9

 SYSTEM DESCRIPTION.....10

 POLICY MANAGEMENT.....11

 DATA USE.....11

 SYSTEM SECURITY.....12

 RESPONSIBILITY FOR RECORDS.....12

 AUDIT.....13

 TRAINING.....13

 LE D-DEx SYSTEM MAINTENANCE.....13

GLOSSARY.....14

 PART I. ABBREVIATIONS AND ACRONYMS.....14

 PART II. DEFINITIONS.....14

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, 2018¹
- (c) DoD Directive 5525.21, “Protection of Buildings, Grounds, Property, and Persons and Implementation of Section 2672 of Title 10, United States Code.” July 9 2018, as amended
- (d) Secretary of Defense Correspondence Action Report, “Lead for Integrating DoD Crime Databases into a Federal System,” August 2, 2005²
- (e) Secretary of Defense Memorandum, “Final Recommendations of the Ft. Hood Follow-on Review,” August 18, 2010
- (f) Under Secretary of Defense for Personnel and Readiness Memorandum, “Designation of the Navy as the DoD Lead Component for the Law Enforcement Defense Data Exchange (LE D-DEx),” August 12, 2008¹
- (g) DoD Instruction 5105.18, “DoD Intergovernmental and Intragovernmental Committee Management Program,” July 10, 2009, as amended
- (h) Memorandum of Understanding among the Federal Bureau of Investigation and Participating State, Local, Tribal, and Federal Agencies for an Information Sharing Initiative, January 30, 2008, and Addendum to the January 30, 2008 Memorandum of Understanding Between the Federal Bureau of Investigation and Department of Defense Regarding an Information Sharing Initiative, January 30, 2008¹
- (i) Section 534 of Title 28, United States Code
- (j) Title 28, Code of Federal Regulations
- (k) Federal Bureau of Investigation, “Criminal Justice Information Services Security Policy,” current edition
- (l) Section 552a of Title 5, United States Code (also known as “The Privacy Act of 1974,” as amended)
- (m) DoD Instruction 5400.11, “DoD Privacy and Civil Liberties Programs,” January 29, 2019
- (n) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (o) 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
- (p) DoD Instruction 5025.01, “DoD Issuances Program,” August 1, 2016, as amended
- (q) Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010
- (r) DoD Instruction 5240.26, “Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat,” May 4, 2012, as amended
- (s) DoD Instruction 2000.12, “DoD Antiterrorism (AT) Program,” March 1, 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 (OUSD(I&S))

² Available from the Chief, Office of Law Enforcement, OUSD (I&S)

- (t) Section 9101(a)(2) of Title 5, United States Code
- (u) Executive Order 13526, "Classified National Security Information," as amended
- (v) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended
- (w) DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020
- (x) DoD Instruction 7600.02, "Audit Policies," October 16, 2014, as amended
- (y) DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program,"
January 25, 2017
- (z) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for
DoD Internal Information Collections," June 30, 2014, as amended
- (aa) DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for
DoD Public Information Collections," June 30, 2014, as amended
- (ab) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020,"
December 20, 2019

ENCLOSURE 2
RESPONSIBILITIES

1. USD(I&S). The USD(I&S):

- a. Develops and maintains policy for criminal data and information sharing through the LE D-DEx.
- b. Monitors compliance with this instruction.
- c. Oversees the activities of the DoD Lead Component and assesses DoD Component compliance periodically as required by Reference (f).
- d. Ensure there is a Chief, Law Enforcement.
- e. Develops and oversees DoD information security policy, which includes policy for controlled unclassified information (CUI).
- f. Provides guidance for the control and safeguarding of CUI.

2. DoD COMPONENT HEADS THAT HAVE LEAs ACTING AS CRIMINAL JUSTICE AGENCIES (CJAs) AND PERFORMING ADMINISTRATION OF CRIMINAL JUSTICE. The DoD Component heads that have LEAs acting as CJAs and performing administration of criminal justice:

- a. Ensure compliance with this instruction.
- b. Establish and implement automated means to share criminal data and information through the LE D-DEx from internal law enforcement record management systems.
- c. Participate in the LE D-DEx system within their own Component's resources in accordance with the authority in Reference (f).
- d. Ensure timeliness, accuracy, and completeness of records made available to the LE D-DEx system.
- e. Designate an LE D-DEx point of contact (POC) for their Component's matters relating to LELE D-DEx.
- f. Participate in BoG management meetings.

3. SECRETARY OF THE NAVY. In addition to the duties in section 4 of this enclosure and as the DoD Lead Component Head for LE D-DEx, the Secretary of the Navy:

- a. Develops LE D-DEx based on existing Law Enforcement Information Exchange (LInX) technology.
- b. Manages the LE D-DEx system.
- c. Establishes and manages the LE D-DEx Program Management Office (PMO).
- d. Establishes, maintains, and manages the LE D-DEx Operational Rules and User Agreement (ORUA).
- e. Ensures that LE D-DEx participating agencies have procedures to comply with the policies in this instruction and those of the LE D-DEx ORUA.
- f. Manages Information Exchange Packages Documentation (IEPD) for LE D-DEx.
- g. Develops LE D-DEx operational and security training.
- h. Designates a representative to serve as the LE D-DEx BoG Vice Chair.
- i. Publishes system compliance audit standards and conducts periodic compliance audits.

ENCLOSURE 3

PROCEDURES

1. OPERATIONAL FRAMEWORK

a. The LE D-DEx system is restricted to documented CJJ obtained by DoD LEAs in connection with their official law enforcement duties.

b. The LE D-DEx system is an on-line real-time CJJ data sharing system to assist in crime prevention and investigative lead sharing. Records are constantly being updated; therefore, record information can change at any time.

c. Participating agencies control what CJJ is shared within the LE D-DEx system. To the maximum extent possible, agencies will share all CJJ, recognizing that some CJJ may not be sharable due to the sensitivity of the information, as defined in Executive Order 13556 (Reference (q)).

d. The criminal and investigative records in the record-owning agency record or case management system are considered the source records.

e. LE D-DEx will not contain criminal intelligence information as defined by part 23 of Reference (j).

f. In accordance with the authority in part 20, subpart A of Reference (j), LE D-DEx system access is restricted to DoD LEAs acting as a CJA and performing administration of criminal justice.

g. The LE D-DEx program is a cooperative endeavor of DoD LEA, in which each entity is participating under its own legal status, jurisdiction, and authorities. All LE D-DEx operations will be based on the legal status, jurisdiction, and authorities of individual participants. LE D-DEx is not intended, and will not be deemed, to have any independent legal status.

h. LE D-DEx participants will contribute or allow access to information via LE D-DEx, and agree to permit the access, distribution, and use of such information by other parties pursuant to the provisions of this instruction. The record-owning agency has the sole responsibility and accountability for ensuring that it is not constrained from permitting this access by any laws, regulations, policies, or procedures.

i. CJJ Sharing:

(1) Sharing With CJA. CJJ contained in LE D-DEx must be shared with DoD CJAs whose mission includes prosecution of criminal offenders, and incarceration and parole of criminal offenders.

(2) Sharing With DoD Non-CJAs. CJI contained in LE D-DEx must be shared with DoD non-CJAs whose missions include responsibilities for DoD insider terrorist threats, foreign terrorist threats, and Anti-Terrorism and Force Protection measures as defined by DoDI 5420.26 (Reference (q)) and DoDI 2000.12 (Reference (s)). Originating LEAs retain responsibility for CJI shared from LE D-DEx to a DoD non-CJA or organization.

(a) DoD non-CJAs are authorized, under regulations described in paragraph 1i(2) of this enclosure, to review the provided CJI 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.

(b) DoD non-CJA use of LE D-DEx CJI will conform to the aforementioned and all other intelligence oversight regulations, and all necessary steps will be taken to ensure the security and integrity of the CJI.

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

(d) Based on their use and analysis of the LE D-DEx CJI, DoD non-CJAs must also provide investigative support, leads and analytic feedback to originating LEAs as appropriate.

j. LE D-DEx is not created pursuant to a single federal statute; rather, LE D-DEx is the DoD's response to its law enforcement community's request to answer the challenge of CJI sharing.

2. SYSTEM DESCRIPTION

a. Full system participants are LEAs of the DoD.

b. Data contributed to the LE D-DEx system must meet the criteria established for the particular type of record involved, as identified in the LE D-DEx IEPD and ORUA.

c. Data contributed and exchanged via LE D-DEx is CJI, and may contain PII (e.g., names, social security numbers) and non-identifying descriptive information (e.g., offense location, weapon involved). It may also contain criminal history record information, as defined in section 9101(a)(2) of Title 5, U.S.C. (Reference (t)). The collection, storage, and distribution of CJI must comply with all applicable laws and regulations.

d. Pursuant to Executive Order 13526 (Reference (u)), LE D-DEx is designated as an unclassified system. Record-owning agencies must ensure that data contributed to and exchanged by LE D-DEx is unclassified. Information contributed to LE D-DEx resides on a server located in Naval Criminal Investigative Service (NCIS)-controlled space, containing CUI from contributing DoD LEAs with established formal agreements.

3. POLICY MANAGEMENT

a. The LE D-DEx BoG manages general policy with respect to the philosophy, concept, and operational principles of the LE D-DEx system. The LE D-DEx BoG places particular emphasis on system security and rules, regulations, and procedures to maintain the integrity of the system and CJI.

b. The Chair of the LE D-DEx BoG conducts board meetings.

c. The Chief, Law Enforcement, serves as the BoG Chair.

d. The LE D-DEx BoG will meet twice a year and at the call of the Chair to provide oversight to development, operation, and maintenance of the LE D-DEx system.

e. The LE D-DEx BoG consists of participating DoD LEA and cognizant OSD law enforcement staff.

f. Under the authority of the Secretary of the Navy as the DoD Lead Component Head and at the direction of the Director, NCIS, the LE D-DEx PMO will manage the LE D-DEx system and implement policy decisions of the LE D-DEx BoG.

g. Participating DoD LEAs will execute the LE D-DEx memorandum of understanding (MOU), maintained by the Chief, Law Enforcement, governing the use of and their participation in the shared LE D-DEx system.

h. LE D-DEx POCs administer their agencies' systems programs and oversee their agencies' compliance with LE D-DEx system policies.

4. DATA USE

a. System Use. The LE D-DEx system will be used in accordance with the policies in this instruction and those of the LE D-DEx ORUA.

b. System Access. LE D-DEx contains CJI obtained by DoD LEA in connection with their official law enforcement duties and access is restricted to DoD LEAs.

c. Pre-Authorization Use. LE D-DEx information may be viewed, output, or discussed without advance authorization of the record-owning agency, within the record-requesting LEA or another LEA, if the other LEA meets the requirements for LE D-DEx access and is serviced by the record-requesting LEA.

d. Authorized Use. The use of LE D-DEx information for external actionable purposes (e.g., arrest or search warrant) requires permission of the information record-owning LEA.

e. Exigent Circumstances Use

(1) As an exception, LE D-DEx information can be used immediately without the advance permission of the record-owning agency if there is an exigent circumstance— an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect or destruction of evidence.

(2) The record-owning agency must be immediately notified of any distribution made as a result of exigent circumstances.

f. Verification Requirement

(1) LE D-DEx information must be verified with the record-owning agency for completeness, timeliness, accuracy, and relevancy prior to reliance upon, action (e.g., preparation of documents related to the judicial process such as affidavits, warrants, or subpoenas), or secondary dissemination to another LEA.

(2) This requirement provides for the opportunity to validate the current status of the information as still being accurate and unchanged since the original submission to the LE D-DEx system and notification to the submitting agency of pending action upon that information.

5. SYSTEM SECURITY

a. The lead DoD Component uses hardware and software controls to ensure system security in accordance with DoDI 8500.01 (Reference (v)) and other applicable guidance.

b. The data stored in the LE D-DEx system is documented CJJ and must be protected to ensure authorized and legal distribution and use. Each LE D-DEx participating entity must implement mechanisms and procedures for user authentication and for verification of authorization to perform any actions involving LE D-DEx data.

6. RESPONSIBILITY FOR RECORDS

a. Each record-owning LEA controls what CJJ is submitted to the LE D-DEx system and how it is shared among LE D-DEx participating LEAs consistent with applicable federal laws and regulations governing access and safeguarding of that type of information.

b. Information contributed to the LE D-DEx system resides on a server located in NCIS controlled space, containing sensitive unclassified information from contributing LEAs party to the LE D-DEx MOU. In accordance with DoDI 5200.48 (Reference (w)) such sensitive unclassified information is referred to collectively as CUI.

7. AUDIT. The LE D-DEx PMO manages the system compliance audit standards and maintains the integrity of the system through a number of automated and manual checks, inspections, audits, and quality control checks in accordance with Reference (k) and DoDI 7600.02 (Reference (x)).

8. TRAINING

a. Before accessing the LE D-DEx, users must be trained on LE D-DEx policy and data use rules.

b. Basic security awareness training must be completed within 6 months of initial assignment and biennially thereafter for all personnel who have access to CJJ.

c. Basic security awareness training is a prerequisite for LE D-DEx account access.

d. All individuals with physical and logical access to LE D-DEx information must be trained on LE D-DEx data use.

e. Records of all training and proficiency affirmation must be maintained by LE D-DEx participating LEAs.

9. LE D-DEx SYSTEM MAINTENANCE. When scheduled maintenance is being conducted on the LE D-DEx system, or the system becomes unavailable outside of scheduled maintenance, the LE D-DEx PMO will notify participating LEAs by the most expeditious electronic means.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

BoG	Board of Governance
CJA	criminal justice agency
CJI	criminal justice information
CJIS	Criminal Justice Information Services
CUI	controlled unclassified information
DoDI	DoD instruction
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
IEPD	Information Exchange Packages Documentation
LEA	law enforcement agency
LE D-DEx	law enforcement Defense Data Exchange
MOU	memorandum of understanding
NCIS	Naval Criminal Investigative Service
N-DEx	National Data Exchange
ORUA	Operational Rules and User Agreement
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PII	personally identifiable information
PMO	program management office
POC	point of contact
U.S.C.	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence and Security

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this instruction.

administration of criminal justice. The detection, apprehension, detention, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and distribution of criminal history record information; criminal justice employment; and, crime prevention programs.

CJA. The courts, a governmental agency, or any subunit of a governmental agency that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General offices are included.

CJI. The term used to refer to data necessary for LEAs to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case or incident history data.

CUI. Designation within the U.S. Government for unclassified information that requires safeguarding or distribution controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. CUI is a broad category of information that includes material covered by designations such as For Official Use Only (FOUO), Law Enforcement Sensitive, Sensitive Homeland Security Information, Security Sensitive Information, and Critical Infrastructure Information. Sensitive but Unclassified is a term previously used for CUI.

DoD LEA. An organization, agency, entity, or office of the Military Departments and Defense Agencies and the DoD Inspector General that perform law enforcement function for those departments and agencies and is staffed by DoD law enforcement officers.

FOUO. A protective marking applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the FOIA as delineated in DoD Manual 5400.07 (Reference (y)). This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974.

N-DEx. A CJI sharing system that provides nationwide connectivity to disparate local, State, tribal, and federal systems for the exchange of information. N-DEx provides LEAs with an investigative tool to search, link, analyze, and share information (for example, incident and case reports) on a national basis.

originating LEAs. The LEA that owns the record management system and the CJI within that system.