SYSTEM NAME AND NUMBER: Defense Central Index of Investigations (DCII), DMDC 13 DoD (September 18, 2019; 84 FR 49101).

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

SYSTEM MANAGER(S): Director, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000. Email: dodhra.dodcmb.dmdc.mbx.webmaster@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: E.O. 12829, National Industrial Security Program; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; DoD Instruction 1320.04, Military Officer Actions Requiring Presidential, Secretary of Defense, or Under Secretary of Defense for Personnel and Readiness Approval or Senate Confirmation; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDI 5505.07, Titling and Indexing Subjects of Criminal Investigations in the Department of Defense; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The DCII is a central database of DoD conducted or sponsored investigations used by DoD law enforcement activities, personnel security adjudicators, and in the Continuous Evaluation program. It also aggregates the results of National Agency Check (NAC) information prior to February 2005 (NAC information after this period is maintained by OPM as well as other Federal investigative agencies). Records document investigations on file with DoD agencies and the United States Coast Guard.

The database also provides data query, data management and reporting capabilities on data pertaining to the existence and physical location of criminal and personnel security investigative files.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All Armed Forces personnel, DoD and U.S. Coast Guard civilian employees, federal contractor employees, and applicants, "affiliated" personnel (such as Non-Appropriated Fund employees, Red Cross volunteers and staff; USO personnel, and congressional staff members) who are the subject of an investigation completed by or for a DoD investigative organization or the United States Coast Guard when that investigation is retained by the organization and the name is submitted for central indexing.

CATEGORIES OF RECORDS IN THE SYSTEM: Records contain names, known alias, Social Security Number (SSN), date of birth, state of birth, country of birth, date investigation completed, employing agencies/companies, type of incident, type of record, and investigation information to include custodian of the file, year indexed, number used by the repository to locate the file location of the investigation, and file number.

RECORD SOURCE CATEGORIES: Air Force Office of Special Investigations, Army Crime Records Directorate, Army Investigation Record Repository, Defense Contract Management Agency, Defense Intelligence Agency, Defense Logistics Agency, Department of Defense

Consolidated Adjudications Facility, Department of Defense Office of Inspector General, National Security Agency, Naval Criminal Investigative Service, Pentagon Force Protection Agency, United States Coast Guard and other DoD agencies performing criminal investigation or personnel security activities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the White House to obtain approval of the President of the United States regarding certain military personnel officer actions.

To the U.S. Senate for appointments and promotions which require Senate confirmation.

To Federal agencies for use in the performance of criminal investigation and personnel security activities to determine the security clearance status of an individual and to determine the existence or physical location of criminal and personnel security investigative files.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: SSN, name, combination of another data element with date of birth and/or place of birth; and/or by employing agencies/companies, type of incident, type of record, or file number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are deleted in accordance with DoD Component authorized disposition schedules or 15 years after completion date of the last update for that file, whichever is sooner.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are accessible only to authorized persons with a valid need-to-know, who are appropriately screened, investigated, and determined eligible for access. Physical safeguards include guards, the use of identification badges, and closed circuit TV. Technical safeguards include Personally Identifiable Verification (PIV) card login, Intrusion Detection System, encryption, firewall, and virtual private network. Administrative safeguards include security audits, monitoring of users' security practices, and encrypting backups of sensitive data offsite.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system must send written signed inquiries to Department of the Army, Defense Manpower Data Center, 1600 Spearhead Division Avenue, Department 548, AHRC-PSI-DMD, Fort Knox, KY 40122-5504.

Signed written requests must contain the subject's full name, SSN, date and place of birth, a description of the records sought, and a current return address.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting contents, and appealing initial agency determinations are published in OSD Administrative Instruction 81, 32 CFR part 311; or may be obtained directly from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine if information about themselves is contained in this system should address written inquiries to: Department of the Army, Defense Manpower Data Center, 1600 Spearhead Division Avenue, Department 548, AHRC-PSI-DMD, Fort Knox, KY 40122-5504.

Signed, written requests should contain the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

An exemption rule for this record system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 321. For additional information contact the system manager.

HISTORY: February 13, 2015, 80 FR 8074. Aug 17, 1999, 64 FR 44704.