

SYSTEM NAME AND NUMBER: Defense User Registration System (DURS) Records, DTIC 01. (February 21, 2017; 82 FR 11193)

SYSTEM CLASSIFICATION: Unclassified

SYSTEM LOCATION: Defense Technical Information Center (DTIC), Directorate of User Services, Communications and Customer Access Division, Attn: DTIC-UC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

SYSTEM MANAGER(S): Chief, Customer Access and Communications Division, DTICUC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: E.O. 13526, Classified National Security Information; DoD Directive (DoDD) 5105.73 Defense Technical Information Center (DTIC); DoD Instruction (DoDI) 3200.12 DoD Scientific and Technical Information Program (STIP); and DoD Manual (DoDM) 3200.14, Volume 1, Principles and Operational Parameters of the DoD Scientific and Technical Information Program (STIP): General Processes.

PURPOSE(S) OF THE SYSTEM: To collect registration requests, validate eligibility, and maintain an official registry that identifies individuals who apply for, and are granted access privileges to DTIC owned or controlled computers, databases, products, services, and electronic information systems.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Department of Defense (DoD) military and civilian personnel and other U.S. Federal Government personnel, their contractors and grantees, and other government officials according to agreements with DoD who request access privileges to DTIC products, services, and electronic information systems.

CATEGORIES OF RECORDS IN THE SYSTEM: Name; DoD Identification (ID) Number; citizenship; service type; personnel category; civilian pay grade; military rank; organization/company name; office mailing address/physical location; office email address; userid and password/reset questions; office telephone number(s); access eligibility; dissemination/distribution group codes; and personal and facility security clearance level(s).

Records also contain the government approving official's name, office phone number and email address; date of registration activation; and the projected date of expiration. Where applicable, the records contain contract number(s), contract expiration date(s), and the Militarily Critical Technical Data Agreement (MCTDA) Certification Number.

RECORD SOURCE CATEGORIES: Individuals, security personnel, the Defense Manpower Data Center Department of Defense Person Search (DMDC DPS), and the electronic Official Personnel Folder (eOPF).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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 552a(b)(3) as follows:

1. Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

2. 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.

3. 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.

4. 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.

5. 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.

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

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Individual name; DoD ID number; office email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Electronic records are to be deleted when DTIC determines they are no longer needed for administrative, audit, legal, or operational purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are maintained in secure, limited access, and monitored areas. Database is monitored, access is password protected, and common access card (CAC) enabled. Firewalls and intrusion detection

system are used. Physical entry by unauthorized persons is restricted through the use of locks, guards, passwords, and/or other security measures. Archived data is stored on compact discs, or magnetic tapes, which are kept in a locked, controlled access area. Access to personal information is limited to those individuals who require a need to know to perform their official assigned duties.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written requests to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, DC 20701-1155.

Signed, written requests should include 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 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, contesting contents, and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURE: Individuals seeking to determine if information about themselves is contained in this system should address written inquiries to Defense Technical Information Center; Attn: DTIC-UC, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218.

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 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: None.

HISTORY: October 04, 2010, 75 FR 61135; November 12, 2008, 73 FR 66852; April 25, 2005, 70 FR 21181.