SYSTEM NAME AND NUMBER: Computer/Electronic Accommodations Program, DHRA 15. (September 23, 2020; 85 FR 59762)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Computer/Electronic Accommodations Program (CAP), Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771.

SYSTEM MANAGER(S): Deputy Director, Computer/Electronic Accommodations Program, 4800 Mark Center Drive, Suite 05E22, Alexandria, VA 22350-3100, cap@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 1582, Assistive Technology, Assistive Technology Devices, and Assistive Technology Services; 29 U.S.C. 794d, Electronic and Information Technology; 42 U.S.C. Ch.126, Equal Opportunity For Individuals With Disabilities; and Department of Defense (DoD) Instruction 6025.22, Assistive Technology (AT) for Wounded, Ill, and Injured Service Members.

PURPOSE(S) OF THE SYSTEM: To administer a centrally funded program to provide assistive (computer/electronic) technology solutions to individuals with hearing, vision, dexterity, cognitive, and/or communications impairments in the form of an accessible work environment. The system documents and tracks provided computer/electronic accommodations and performs operational duties to accomplish mission objectives. It is also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Federal civilian employees in the DoD and CAP partnering agencies, and employees of other federal entities with disabilities, and wounded, ill and injured Service Members on Active Duty that can be accommodated with assistive technology solutions.

CATEGORIES OF RECORDS IN THE SYSTEM: Name(s), position/title, mailing/home/work address, work email address, disability information, official duty telephone number, worker compensation claims number, CAP request number, employment information, agency/organization, verification of disability, prior assistive technology solutions provided to the individual, CAP order number, and history of accommodations being sought. Product and vendor contact information including vendor name and address, vendor alias, phone number, fax number, email address, web address, order submission preference, orders, invoices, declination, and cancellation data for the product and identification of vendors, vendor products used, and product costs.

RECORD SOURCE CATEGORIES: Individual, the DoD Workforce Recruitment Program database, partnering agencies/organizations, and vendors.

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, these 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:

a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

b. To Federal agencies/entities participating in the CAP for purposes of providing information as necessary to permit the agency to carry out its responsibilities under the program.

c. To commercial vendors for purposes of providing information to permit the vendor to identify and provide assistive technology solutions for individuals with disabilities.

d. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

e. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

f. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

g. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

h. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

i. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

j. To another Federal agency or Federal entity, when the DoD determines information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper and electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Name, agency/organization, CAP request number, work address, and work telephone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: General files. Destroy three years after end of fiscal year in which a record is superseded or when no longer needed for reference, whichever is later.

Individual employee files that are created, received, and maintained by EEO reasonable accommodation or diversity/disability program or employee relations coordinators, immediate supervisors, CAP administrator, or HR specialists containing records of requests for reasonable accommodation and/or assistive technology devices and services through the agency or CAP that have been requested for or by an employee: Destroy three years after end of fiscal year of employee separation from the agency or conclusion of all appeals, whichever is later.

Records created, received, and maintained by EEO reasonable accommodation or diversity/disability program or employee relation coordinators, while advising on, implementing or appealing requests for or from an individual employee for reasonable accommodation: Destroy three years after end of fiscal year in which accommodation is decided or all appeals are concluded, whichever is later.

Records and data created, received, and maintained for purposes of tracking agency compliance with Executive Order 13164 and Equal Employment Opportunity Commission (EEOC) guidance: Delete/destroy three years after end of fiscal year in which compliance report is filed or when no longer needed for reference.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Multifactor log-in authentication including CAC authentication and password. Access controls enforce need-to-know policies so only authorized users have access to PII. Additionally, security audit and accountability policies and procedures directly support privacy and accountability procedures. Network encryption protects data transmitted over the network while disk encryption secures the disks storing data. Key management services safeguards encryption keys. Sensitive data is identified and masked as practicable. All individuals granted access to this system of records must complete requisite training to include Information Assurance and Privacy Act training.

Sensitive data will be identified, properly marked with access by only those with a need to know, and safeguarded as appropriate.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed, written requests should contain individual's full name, agency/organization, CAP request number, work address, work telephone number, and the name and number of this system of records notice (SORN). 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 DoD rules for accessing records, contesting contents, and for appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Program Manager, Computer/Electronic Accommodations Program, 4800 Mark Center Drive, Suite 05E22, Alexandria, VA 22350-1200. Signed, written requests should include the individual's full name and the name and number of this SORN. 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: None.

HISTORY: August 11, 2011, 76 FR 49753; October 20, 2014, 79 FR 62602.