

BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-XXXX]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is establishing a new Department-wide system of records titled, “Pentagon Athletic Programs”

DWHS E07. This system of records covers DoD’s maintenance of records used to manage the athletic memberships of military members (active duty, reservist, retired), civilian employees, contractors and their family members in the National Capital Region with access to the

Pentagon. **DATES:** This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for

this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, DC 20301-1155, or by phone at (571) 372-0478. **SUPPLEMENTARY INFORMATION:**

I. Background

DoD is establishing the “Pentagon Athletic, Programs” DWHS E07. The PAC provides physical fitness facilities and fellowship for Department of Defense military and civilian employees. The information collected under this system of records is used to determine eligibility, establish and maintain athletic memberships of military members (active duty, reservist, retired), civilian employees, contractors, their family members and guests who have access to the Pentagon and its annex fitness facilities located in the National Capital Region. DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.defense.gov>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and OMB Circular No. A-108, DoD has provided a report of this system of records to the Office of Management and Budget and to Congress.

Dated:

Aaron T. Siegel,
Alternate OSD Federal Register
Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Pentagon Athletic, Programs, DWHS E07

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): The system managers is the Director, Executive Service Directorate, Washington Headquarters Services (WHS), 1155 Defense Pentagon, Washington, DC 20301-1155, whsmc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. Chapter 79, "Services to Employees; 5 U.S.C. 7901, Health Service Programs; 10 U.S.C. 113, Secretary of Defense; DoD Directive 5105.53, Director of Administration and Management; DoD Directive 5110.4, Washington Headquarters Services, and DoD Instruction 1010.10, Health Promotion and Disease Prevention.

PURPOSE(S) OF THE SYSTEM:

A. To determine eligibility and register individuals for athletic memberships, track usage; make fee determinations, register applicants for classes, reserve various events and workout sessions.

B. To generate statistical reports that keep track of the number of members; activities utilized, place members on/off hold status and terminate membership or facility use for noncompliance with rules.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Active, Reserve and Retired Military members, civilian employees, contractors, family members and guests of individuals who apply for membership and are authorized to use the Pentagon athletic facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: Records covered by this SORN includes information regarding individuals applying for access to the Pentagon athletic facilities. Records include: name, DoD ID number, membership number, gender, branch, military status, official duty and home address, phone (home and/or cell), official duty and home e-mail address, official duty telephone number, rank/grade, family member name and date of birth.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individual and membership application.

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, all or a portion of the records or information 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 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.

C. 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.

D. 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 that 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.

E. 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.

F. 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.

G. 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.

H. To another Federal agency or Federal entity, when the DoD determines that 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.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, DoD CAC ID number, member number, work and personal email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Temporary. Cut off and destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use..

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures,

including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities. The computer files are CAC card enabled with access restricted to authorized users

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the

individual. 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 appropriate 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: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None

HISTORY: None.