

SYSTEM NAME AND NUMBER: DoD Patron Authorization, Retail, Services, and MWR
Recreational Activities DoD-000x

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 are as follows:

Director/Chief Executive Officer, Army and Air Force Exchange Service, 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598; 800-527-6790.

Policy Official Commander, Navy Exchange Service Command, 3280 Virginia Beach Boulevard, Virginia Beach, VA 23452-5724.

Deputy Director/Chief Operating Officer, Defense Commissary Agency, 1300 E. Avenue, Fort Lee, VA 23801-1800.

Policy Official Commander, Navy Installations (Finance Department) Millington Detachment, 5720 Integrity Drive, Millington, TN 38055-6500

Director, Financial Management and Comptroller, Headquarters Air Force Services Agency (HQ AFSVA/SVF), 10100 Reunion Place, Suite 400, San Antonio, TX 78216-4138.

Director, Engineering and Services, Deputy Chief of Staff, Programs and Resources, Headquarters United States Air Force, Washington, DC 20330

Deputy Chief of Staff, G-1, 300 Army Pentagon, Washington, DC 20310-0300.

Chief of Community Programs, Community Programs Division, Services Directorate,
Headquarters Air Force Personnel Center, 2261 Hughes Avenue Suite 156, Joint Base San
Antonio (JBSA) Lackland AFB, TX 78236-9854.

Commander, Family and Morale, Welfare and Recreation Command, 4700 King Street,
Alexandria, VA 22302-4414.

Associate Director for Installations and Logistics, National Security Agency/Central
Security Service, 9800 Savage Road, Ft. George G. Meade, MD 20755-6000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Federal Claims Collection Act of 1966 (Pub.L. 89-508, as amended) and Debt Collection Act of 1982 (P.L. 97-365, as amended), as amended by the Debt Collection Improvement Act of 1996 (P.L. 104-134, section 31001) as codified in 31 U.S.C. 3711, Collection and Compromise; 10 U.S.C. 2481, Defense Commissary and Exchange Systems: Existence and Purpose; 10 U.S.C. 1146, Commissary and Exchange Benefits; 10 U.S.C. 2488, Combined Exchange and Commissary Stores; 14 U.S.C. 152, Nonappropriated Fund Instrumentalities; DoD Directive 5124.02, Paragraph 4.1.7, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); DoD Instruction (DoDI) 1330.21, Armed Services Exchange Regulation; DoDI 1330.17, DoD Commissary Program; DoDI 1015.10, Military Morale, Welfare, and Recreation (MWR) Programs; DoDI 1015.08, DoD Civilian Employee Morale, Welfare and Recreation (MWR) Activities and Supporting Nonappropriated Fund Instrumentalities (NAFI); DoDI 1330.09, Armed Services Exchange Policy; DoDI 1330.21, Armed Services Exchange Regulations; DoD 7000.14-R, Department of Defense Financial Management Regulation Volume 13: “Nonappropriated Funds Policy” and Volume 16: “Department of Defense Debt Management”; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

A. To identify and authenticate individuals who are authorized to obtain DoD privileges for goods and/or services as authorized by Congress and applicable service regulations

B. To create individual market and demographic profiles to better understand the patron base, in order to provide better services and enhance the quality of life for authorized patrons

C. To manage and oversee transactional records associated with DoD-provided goods or services.

D. To interact with financial institutions for the processing of payments received.

E. To monitor restricted items or services purchased overseas, prevent issues of black marketing, and to comply with rules concerning age-restricted services or purchases to minors or those under an allowable age.

F. To process applications for credit; administer and monitor account information; and perform required reports as regulated by statutes or regulations.

G. To detect and prevent criminal activity; identify potential abuse of privileges; and collect debts due to the United States.

H. To address and respond to individual's comments or complaints concerning the DoD military exchanges above and other vendors located on military installations.

I. To administer DoD programs devoted to mental and physical well-being.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Individuals who are authorized to receive privileges or benefits at any DoD location. This may include current and former military members (Active, Reserve, Guard, cadets, retirees, veterans), current and retired non-appropriated fund and appropriated fund DoD civilian employees, sponsored family members or other dependents of authorized patrons including

children, and individuals commissioned or contracted with the Federal government who are authorized to obtain privileges or benefits.

B. Visitors to DoD facilities who are offered limited-time purchase privileges. These individuals may be special guests of eligible patrons, or members of the public who are invited to a DoD location for special events such as air shows, retirement ceremonies, or military graduations.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal and Account Information, such as individual's full name, date of birth, Social Security Number (SSN); age; gender; marital status; contact information, such as mailing/physical address, e-mail address, phone numbers; Website log-in information; personal automobile license plate number; username for Internet and/or mobile ordering; social media (e.g., Facebook, Twitter, Flickr, YouTube) username; household size.

B. Employment Information, such as current/past employer's name and contact information; position/grade/rank; salary/wages; Department of Defense Identification Number (DoD ID Number); branch of service; projected future station of assignment.

C. Financial Information, such as bank name, bank account number, routing number, check number; credit and debit card numbers; benefit transfer cards (Women, Infants and Children Programs (WIC) and Supplemental Nutritional Assistance Program (SNAP)); credit bureau reports.

D. Transaction/Account Information, such as charges or refunds associated with receipt or the collection of debts for goods or services; claim data for returns or damages of goods/services; copies of returned checks; debt statements and communication; garnishment orders; video/audio recordings; registrations and registry logs.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individual, contractors, vendors, the Defense Enrollment Eligibility Reporting System (DEERS), and other Federal organizations.

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, 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 has confirmed that there has been a breach of the system of records; (2) the DoD has determined that 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 such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or

homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

K. To consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)), or in accordance with 3(d)(4)(A)(ii) of the Federal Claims Collection Act of 1966 as amended (31 U.S.C. 3701(a)(3)), for the purpose of encouraging the repayment of an overdue debt, the amount, status and history of overdue debts, the name and address, taxpayer identification (SSN), and other information necessary to establish the identity of a debtor, the agency and program under which the claim arose, may be disclosed pursuant to 5 U.S.C. 552a(b) (12).

L. To credit card processors, banks, and other financial institutions to process payments or refunds made by credit or debit cards, by check, or other payment methods.

M. To the U.S. Department of the Treasury (Treasury) for centralized administrative or salary offset, including the offset of Federal income tax refunds, for the purpose of collecting debts owed to the U.S. government,

N. To Treasury-contracted private collection agencies for the purpose of obtaining collection services, including administrative wage garnishment (AWG), to recover debts owed to the U.S. Government.

O. To a loyalty card, rewards card, points card, advantage card or club card or digital coupon program coupon contractor to verify individual's enrollment in a loyalty, rewards, points, advantage, club or digital coupon program, and to provide discounts, digital coupons, or other incentives to be applied to individual's purchases.

POLICIES AND PRACTICES FOR STORING 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 individual's name; DoD ID Number; SSN; or other personal identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A. Contact information, dependent data, military information for all individuals within this system is maintained in electronic format until obsolete or superseded when they are erased from the database.

B. Layaway transactions are maintained for six-months after completed or cancelled then destroyed by shredding or erasing from the database.

C. Service work orders, remote patron signature cards, charge/credit vouchers for merchandise returned to the vendor, and Moral, Welfare and Recreation (MWR) membership for golf privileges are maintained for one year after service or goods are provided then destroyed by shredding.

D. Diamond trade-ups, refunds/repairs to fine jewelry, purchase of critical items (firearms, jewelry, cameras), lodging registration, golf fee registers, and theater transaction data are maintained for two years after service is provided and then destroyed by shredding.

E. Correspondence from patrons and outdoor game life records are maintained for three years after issue resolved and then destroyed by shredding or erasing from the database.

F. Executive restaurant data is maintained for four years and then destroyed by shredding or erasing from the database.

G. Order transactions, order related documentation, and general MWR data is maintained for six years and then destroyed by shredding or erasing from the database.

H. Bingo records are maintained for seven years and destroyed by shredding or deletion from the database.

I. Debt files are maintained while the account is active and destroyed six years after all debts have been paid and then either shredded or erased from the database.

J. Theater schedules of activities are maintained for thirty years after event and destroyed by shredding or erasing from database.

K. Library registration forms, video, audios, cash checking privilege documentation are retained until the account is deactivated or superseded then destroyed by burning or shredding or erasing from the database.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL 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 CAC authentication and password; 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.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the DoD office with oversight of the records. The public may identify 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, identifier (i.e., DoD ID Number or Defense Benefits Number), date of birth, current address, and telephone number 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: The DoD rules for accessing records, contesting contents, and 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 appropriate system managers(s). Signed written requests should contain the full name, identifier (i.e., DoD ID Number or DoD Benefits Number), date of birth, and current address and telephone number 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).”

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.