SYSTEM NAME AND NUMBER: Exchange Non-appropriated Personnel Systems; AAFES 0401.04

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Headquarters, Army and Air Force Exchange Service, 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598; National Personnel Records Center (NPRC), 1411 Boulevard, Valmeyer, IL 62295; Army and Air Force Exchange Service-Europe Region, Building Sembach Kaserne Geb 201, 67681 Sembach, Heuberg, Germany; Exchange Regions and Area Exchanges at posts, bases, and satellites world-wide.

SYSTEM MANAGER(S): Director/Chief Executive Officer, Army and Air Force Exchange Service (Exchange), 3911 S. Walton Walker Blvd., Dallas, TX 75236-1598; 800-527-67903.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; 42 U.S.C. 659, Consent by United States to Income Withholding, Garnishment, and Similar Proceedings for Enforcement of Child Support and Alimony Obligations; 31 CFR 285.11, Administrative Wage Garnishment; DoD Directive 7000.14-R, DoD Financial Management Regulation; DoD Instruction 1400.25, Volume 1408, DoD Civilian Personnel Management System: Insurance and Annuities for Nonappropriated Fund (NAF) Employees; Army Regulation 215-8/AFI 34-211(I), Army and Air Force Exchange Service Operations; and E.O. 9397 (SSN), as amended.

PURPOSE FOR THE SYSTEM:

A. To populate and maintain a repository of documentation of the history and status of an individual's employment relationship with the Exchange .

B. To provide a basic source of factual data of a person's Federal employment while as an active Exchange associate and after his or her separation for the purpose of administer, compute, monitor, and report employee personnel actions such as pay entitlements and transactions, grade increases, length of service and incentive/honor awards and recognitions, performance ratings, disciplinary actions, training, compensation, benefit enrollment and payouts, annuities and retirement, bonds due and issued, taxes paid, employee debts, leave accrued and usage, and employment separation and outsourcing.

C. To determine an employee's qualification and eligibility for promotion and/or transfer.

D. To capture and maintain individual job applicants' essential job skills and aptitudes for consideration and hiring determinations for open Exchange positions worldwide.

D. To administer proper health care, medical treatment, and processing of claims for employees who become ill or are injured during working hours.

E. To process official travel requests for Exchange civilian employees including data to determine eligibility of associates' dependents for travel, obtain necessary clearance where foreign travel is required, assisting employees in applying for passports and visas, and counseling here proposed travel incudes visiting or transiting to communist counties and danger zones.

F. To provide locator and emergency notification data.

G. To maintain information on participates in the Exchange tuition assistance program.

H. To obtain data to verify employment and wages.

I. To provide data in support of Equal Employment Opportunity Program requirements.

J. To answer inquiries, process claims, administer and investigate complaints, grievances, and appeals.

K. To respond and process payments to Court and Regulatory Bodies requests for information or garnishment orders such as Qualifying Domestic Relations Orders (QDRO) or compliance with Child Support, Alimony obligations, Federal and Commercial (civil) debts, or tax levies.

L. To produce managerial report and statistical analysis of Exchange work force strength trends and composition in support of established manhours, projected staffing requirements, and budgetary programs and procedures.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Individuals who are potential, current, of former employees of the Exchange.

B. Individuals who are dependents, family members, emergency contacts, survivors, or legal representatives of current or former employees of the Exchange.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal and Biographical Information, such as individual full name, date of birth, Social Security Number (SSN); age; gender; marital status; race, hair color, color of eyes, height, and weight; sex; citizenship and place of birth; disability; contact information such as mailing/physical address, e-mail address, phone numbers; emergency contact information; legal representative name and contact data; Drivers' License data and personal automobile license plate number.

B. Employment Information, such as past employer's name and contact information; application for employment and academic transcripts; previous and current position/grade/rank; past and present salary/wages; Department of Defense Identification Number (DoD ID Number); Military history to include branch of service; mobility plans; travel orders; time records; supervisory approvals and delegations; leave requests; personnel actions such as transfers, pay increases/decreases; awards; disciplinary actions and reprimands, and like documents; time records; training; change of duty documents; security and clearance documents.

C. Financial Information, such as bank name, bank account number, routing number, check numbers; Exchange pay documents such as paystubs; tax documents such as W2, W4; Garnishment Orders and payments; unemployment data requests; indebtedness papers.

D. Benefit and Retirement Information, such as benefit enrollment information, 401K balances, retirement estimates, annuities, and like documents.

E. Medical Information, such as physical examination documents, Workers' Compensation Claims; medical diagnosis and treatment plan; prescription documentation; adjuster notes and legal advice; payments for medical services and claims; copies of DOL reports; and regulated documents/reports.

F. Travel Information, such as requests and approvals, Temporary Duty Changes and Official Change of Duty Station documents to include authorized leave in-route, shipment of household and personal goods, travel expense vouchers, Visa, and passports information.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individual, educational institutions, officials and other individuals of the Exchange such as security and supervisors, the Defense Enrollment Eligibility Reporting System (DEERS), previous employers, medical providers; law enforcement organizations, dependents, administrative and regulatory offices of the court, third party organizations and individuals, 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:

Note: This system of records contains Personal Identifiable Information. The DoD Health Information Privacy Regulation (DoD 6025.18, March 13, 2019) issued pursuant to Health Insurance Portability and Accountability Act of 1996, applies to most such health information. DoD 6025.18 may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974, as amended, or mentioned in this system of records.

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

J. To the Department of Labor, Department of Veterans Affairs, Social Security Administration, Federal agencies that have special civilian employee retirement programs, or a national, state, county, municipal, or other publicly recognizable charitable or income security administrative agency (e.g. State unemployment compensation agencies), where necessary to adjudicate a claim under the retirement, insurance or health benefits programs or to an agency to conduct studies or audits of benefits being paid under such programs.

K. To designated officers and employees of Federal, State, local, territorial, or tribal, international, or foreign agencies maintaining civil, criminal, enforcement, or other pertinent information, such as current licenses, if necessary to obtain information relevant and necessary to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

L. To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies in connection with the hiring or retention of an employee, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a

license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter and the Department deems appropriate.

M. To contractors whose employees require suitability determinations, security clearances, and/or access to classified national security information, for the purpose of ensuring that the employer is appropriately informed about information that relates to and/or may impact a particular employee or employee applicant's suitability or eligibility to be granted a security clearance and/or access to classified national security information.

N. To a former DoD employee for the purpose of responding to an official inquiry by a Federal, State, local, territorial or tribal entity or professional licensing authority, in accordance with applicable DoD regulations; or for the purpose of facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the DoD requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

O. To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

P. To unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. §§ 7111 and 7114, the Merit Systems Protection Board, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective actions, or grievances, or conducting administrative hearings or appeals.

Q. To the Merit Systems Protection Board and the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems; review of Office of Personnel Management or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

R. To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

S. To State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. §§ 5516, 5517, or 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax, regardless of whether tax is or was withheld. The information to be disclosed is information normally contained in Internal Revenue Service (IRS) Form W-2.

T. 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.

U. To any person, organization, or governmental entity (e.g., local governments, first responders, American Red Cross, etc.), in order to notify them of or respond to a serious and

imminent terrorist or homeland security threat or natural or manmade disaster as is necessary and relevant for the purpose of guarding against or responding to such threat or disaster.

V. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or of which they were a victim.

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. The records may be stored locally on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP) and/or applicable security regulations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual's name; SSN; or another personal identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A. Official Personnel Folders (OPF) are maintained for 129 years after separation from Federal Service and then destroyed by cross shredding or removal from electronic database.

B. Personnel files for aliens, foreign nationals or local nationals employed outside the U.S. are held temporary and destroyed five years after the end of the fiscal year of separation of employment. Longer retention may be required, if host government agreements require longer retention, or if OPFs are used to certify Federal employment for

admitting refugees into the United States. In such cases, OPFs will be offered to the Department of State at the end of the retention period.

C. Convenience personnel folders at regions are retained if employee is assigned under the jurisdiction of the U.S. Region (USR) and destroyed by cross shredding or deletion from electronic system when no longer needed for reference, update, revisions, or dissemination.

D. Supervisor personnel records and communication logs are maintained while the employee is active, reviewed annually, and destroyed by cross shredding or removal from database when superseded or obsolete or one year after the employee separates, retires, or transfers.

E. Employee identification files and credentials, including related applications is destroyed three months after return to the issuing authority. Associated identification card control is maintained for five years past the date of completion and destroyed by cross shredding and removal from database.

F. Candidate information, including applications for employment and supportive documents is maintained within the system of collection for one year past the submission date, then destroyed by cross shredding or removal from electronic system. Candidate information for individuals selected for vacancies, and associated interview files, is destroyed two years after the hiring decision or the finalization of an appeals or litigation. Candidate information for hired individuals is transferred to the employees Official Personnel Folder and maintained for 129 years past the employee's separation from Federal Employment.

G. Employee incentive awards nominations is destroyed by cross shredding and removal from database two years after the award is approved or disapproved.

H. Administrative grievance, disciplinary, and adverse actions are maintained for seven years past the final action and then destroyed by cross shredding or removal from database.

I. Retirement assistance case files is destroyed by cross shredding or removal from database one year or when no longer needed.

J. Individual employment separation case files, not included in an employee's OPF, is destroyed by cross shredding or removal from electronic database one year after the date of the employee's separation or transfer.

K. An employee's acknowledgement for the Workplace Drug Testing Program is destroyed by cross shredding or removal from database when an employee separates from a testing designated position. Employee drug testing specimen records are destroyed three years after the date of last entry or when three years old, whichever is later. Positive drug test documents are destroyed when the employee separates from employment or when the record is three years old. Negative results are maintained for three year and then destroyed. Disciplinary action documents for cases associated with drug testing or related litigation or adverse action are destroyed seven years after the date the case is closed.

L. Employee's Individual Health Records is maintained for six years past separation or transfer and then destroyed by cross shredding or erasure from the database.

M. Individual Exchange training files are destroyed by cross shredding or removal from database when superseded, three years old, or one year after separation from employment.

N. Employee's Tuition Assistance case files is maintained for two years past the date of completion and destroyed by cross shredding and removal from the database.

O. Management Administrative Records such as general correspondence with travelers regarding official passport application procedures and documentation requirements are destroyed three years after approved/disapproved by cross shredding or deletion from electronic systems.

P. Employee Temporary Duty (TDY) travel requests, approvals/disapprovals, Military Airlift Command (MAC) authorizations, Ticketing Service Files, and supportive documentation is maintained for a period of three years past the end of travel and then destroyed by cross shredding or removal from database. Employee Permanent Change of Duty Station (PCS) requests, approvals/disapprovals, and supportive documentation is maintained for a period of eight years past completion of travel and then destroyed by cross shredding or removal from database. Personnel property shipment files are destroyed ten years after movement.

Q. Passport applications and renewal records are maintained for three years or when employee separates or is transferred. Official passports of transferred or separated employees are transferred to the new agency or returned to the Department of State. Official passport registers listing agency personnel who have official passports issued is maintained until superseded or obsolete and then destroyed by cross shredding or removal from database.

R. Overseas differential and allowance case files to affirm employee's eligibility for foreign post differential and allowances are destroyed by cross shredding or removal from database when employee separates from employment.

S. Employee pay records are maintained for fifty-six years and destroyed by cross shredding or removal from database.

T. Printouts of employees covered by group insurance is maintained for six years and then destroyed by cross shredding or removal from database.

U. Documents related to the administration of accidental death and dismemberment insurance program are maintained for three years and then destroyed by cross shredding and removal from database.

V. Exchange insurance claim files are destroyed thirty years past the date of incident or report of claim by cross shredding and removal from database.

W. Short-Term Disability file documents are maintained for two years after the employee returns to work and then destroyed by cross shredding and removal from database. Long-term Disability files are destroyed six years after the employee returns to work or retires.

X. Miscellaneous employee claim files accumulated on group insurance plans are maintained for three years after the clam is closed and then destroyed by cross shredding and removal from databases.

Y. Annuity eligibility case files of retired employees are destroyed six years after the Exchange involvement is terminated by cross shredding and removal from database.

Z. Documents accumulated on employees who have been disabled for more than nine months, whose hospitalization and life coverage premiums have been waived by the carriers, are destroyed by cross shredding and removal from database four years after the employee returns to work or is no longer eligible for coverage.

AA. Individual retirement files are destroyed six years after the Exchange terminates involvement.

AB. Histories of death benefit payments and associated documents are destroyed by cross shredding and removal from database six years after the date the benefits are paid.

AC. Employee withholding allowance certificates such as Internal Revenue Service (IRS) W-4 series forms, IRS W-2, IRS W-3, IRS 1099's, state equivalents, records of fringe benefits, and expense reimbursements provided to employees are terminated four years after superseded or when employee separates.

AD. German payroll reports are maintained for sixty years and destroyed by cross shredding or removal from 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; 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 mangers(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: 61 FR 41573, August 9, 1996.