POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic storage media.

RETRIEVABILITY:

Name and/or Social Security Number (SSN).

SAFEGUARDS:

Records are accessed and/or maintained in areas accessible only to authorized personnel who are properly screened, cleared, and trained. User names and passwords and/or Common Access Cards (CACs) are employed to ensure access is limited to authorized personnel only. Employees are able to access and view only their records and update certain personal information to them via user name and password. Security systems and/or security guards protect buildings where records are accessed or maintained. A risk assessment has been performed and will be made available on request.

RETENTION AND DISPOSAL:

Records are retained for 25 years after an individual separates from the government and then the records are purged.

SYSTEM MANAGERS AND ADDRESS:

Civilian Personnel Management Service, 1400 Key Boulevard, Suite B200, Arlington, VA 22209–5144.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to: Civilian Personnel Management Service, 1400 Key Boulevard, Suite B200, Arlington, VA 22209–5144.

Written requests should contain individual's name and Social Security Number (SSN).

RECORD ACCESS PROCEDURES:

Individuals seeking access to information 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, 1155 Defense Pentagon, Washington, DC 20301–1155.

Written requests should contain the name and number of this system of records notice along with the individual's name and Social Security Number (SSN).

CONTESTING RECORD PROCEDURES:

The Office of the Secretary of Defense rules for accessing records, for contesting contents and appealing initial agency determinations are contained in Office of the Secretary of Defense Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

RECORD SOURCE CATEGORIES:

Prospective employee generated resume, Standard Form 171, or Optional Form 612; employee or supervisor generated training requests; human resources generated records; employee generated data recorded as self certified; and other employee or supervisor generated records. Data is also received from various interfaces; Defense Manpower Data Center; Defense Civilian Payroll System; Joint Personnel Adjudication System; Air Force Manpower Interface; National Guard Bureau Military Data Upload; NAF Payroll; Resumix; and training.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 2010–28755 Filed 11–12–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2010–OS–0154]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice to add a System of Records.

SUMMARY: The Defense Information Systems Agency is proposing to add a system of records to its inventory of records system subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice on December 15, 2010 unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and/ Regulatory Information Number (RIN) and title, by any of the following methods:

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

* *Mail:* Federal Docket Management System Office, Room 3C843, 1160 Defense Pentagon, Washington, DC 20301–1160.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) 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 *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Defense Information Systems Agency, 5600 Columbia Pike, Room 933–I, Falls Church, VA 22041–2705, Ms. Jeanette M. Weathers-Jenkins at (703) 681–2409.

SUPPLEMENTARY INFORMATION: The Defense Information Systems Agency system of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the **Federal Register** and are available from the **FOR FURTHER INFORMATION CONTACT** address above.

The proposed system report, as required by 5 U.S.C. 552a(r), of the Privacy Act of 1974, as amended, was submitted on November 3, 2010, to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: November 9, 2010.

Morgan F. Park,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

K890.15 DoD

SYSTEM NAME:

Active Directory Enterprise Application and Services Forest (AD EASF).

SYSTEM LOCATION:

System locations may be obtained from the systems manager at the Defense Information Systems Agency (DISA), Computing Services Division (CSD), 5600 Columbia Pike, Falls Church, VA 22204–4502.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Department of Defense (DoD) personnel who have been issued DoD Common Access Cards (CAC) or a DoD Class 3 Public Key Infrastructure (PKI) certificate to include civilian employees, military personnel, contractors and other individuals detailed or assigned to DoD Components.

CATEGORIES OF RECORDS IN THE SYSTEM:

Individual's name (last name, first name, middle initial); unique identifiers including Electronic Data Interchange Person Identifier (EDI PI), other unique identifier (not Social Security Number), Federal Agency Smart Credential Number (FASC–N), login name, legacy login name, and persona username; object class; rank; title; job title; persona type code (PTC); primary and other work e-mail addresses; persona display name (PDN); work contact information, including administrative organization, duty organization, department, company (derived), building, address, mailing address, country, organization, phone, fax, mobile, pager, Defense Switched Network (DSN) phone, other fax, other mobile, other pager, city, zip code, post office box, street address, state, room number, assigned unit name, code and location, attached unit name, code and location, major geographical location, major command, assigned major command, and base, post, camp, or station; US government agency code; service code; personnel category code; non-US government agency object common name; user account control; information technology service entitlements; and Public Key Infrastructure (PKI) certificate information, including Personal Identity Verification Authentication (PIV Auth) certificate issuer, PIV Auth certificate serial number, PIV Auth certificate principal name, PIV Auth Subject Alternative Name, PIV Auth Thumbprint, PIV Auth Issuer, PIV Auth Common name, Identity (ID) certificate issuer, ID certificate serial number, ID certificate principal name, ID Thumbprint, ID Common Name (CN), signature certificate e-mail address, Signature Subject Alternative Name User Principal Name (UPN), Signature Thumbprint, Signature Issuer, Signature serial number, Signature CN, Public Binary Certificate, Encryption Thumbprint, Certificate Issuer, Encryption Serial Number, Encryption CN, distinguished name, PKI login identity, e-mail encryption certificate, and other certificate information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulation; and DoD Directive 5105.19, Defense Information Systems Agency (DISA).

PURPOSE(S):

The AD EASF will control access and provide contact information for users of DoD Enterprise E–Mail, workspace and collaboration tools, file storage, and office applications.

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, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: The DoD 'Blanket Routine Uses' set forth at the beginning of the DISA's compilation of systems of records notices apply to this system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic storage media.

RETRIEVABILITY:

By individual's name.

SAFEGUARDS:

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Defense-in-Depth methodology is used to protect the repository and interfaces, including (but not limited to) multi-layered firewalls, Secure Sockets Layer/Transport Layer Security (SSL/TLS) connections, access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the AD EASF system integrity and the data confidentiality.

RETENTION AND DISPOSAL:

Disposition pending (until the National Archives and Records Administration approves retention and disposal schedule, records will be treated as permanent).

SYSTEM MANAGER(S) AND ADDRESS:

Defense Information Systems Agency (DISA), Computing Services Division (CSD), 5600 Columbia Pike, Falls Church, VA 22204–4502.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the systems manager at the Defense Information Systems Agency (DISA), Computing Services Division (CSD), 5600 Columbia Pike, Falls Church, VA 22204–4502.

Requests must include the individual's full name, rank, grade or title, component affiliation, work e-mail address, telephone number, assigned office or unit, and complete mailing address.

RECORD ACCESS PROCEDURES:

Individuals seeking access to get information about themselves contained in this system of records should address written inquiries to the systems manager at the Defense Information Systems Agency (DISA), Computing Services Division (CSD), 5600 Columbia Pike, Falls Church, VA 22204–4502.

Requests must include the individual's full name, rank, grade or title, component affiliation, work email address, telephone number, assigned office or unit, and complete mailing address.

CONTESTING RECORD PROCEDURES:

DISA's rules for accessing records, for contesting content and appealing initial agency determinations are published in DISA Instruction 210–225–2; 32 CFR part 316; or may be obtained from the systems manager at the Defense Information Systems Agency (DISA), Computing Services Division (CSD), 5600 Columbia Pike, Falls Church, VA 22204–4502.

RECORD SOURCE CATEGORIES:

The DoD Identity Synchronization Service (IdSS).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 2010–28754 Filed 11–12–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2010–OS–0153]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice to add a System of Records.

SUMMARY: The Defense Information Systems Agency is proposing to add a system of records to its inventory of records system subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective without further notice on December 15, 2010 unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and/