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 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.

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. 2010–30726 Filed 12–7–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DOD–2010–OS–0161]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice to alter a system of records.

SUMMARY: The Defense Information Systems Agency is altering a system of records notices in its existing inventory of record systems 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 January 7, 2011 unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and/ or 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, or 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 December 1, 2010 to the House Committee on 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," February 20, 1996, 61 FR 6427.

Dated: December 2, 2010.

Morgan F. Park,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

K890.14 DoD

SYSTEM NAME:

Identity Synchronization Service (IdSS) (November 15, 2010, 7 FR 69645).

CHANGES:

*   *   *   *   *

CATEGORIES OF RECORDS IN THE SYSTEM:

Delete entry and replace with "These include 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 UPN, Signature Thumbprint, Signature Issuer, Signature serial number, Signature CN, Encryption (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, Country of Citizenship, US Citizenship Status Indicator Code, Cadency of name (*e.g.* Sr, Jr, III), Identity Certificate Serial Number, Persona E–Mail Address, Administrative Organization Code, DoD component, DoD sub-component, Non-DoD agency, Directory publishing restrictions, Reserve component code, Billet code and Pay grade.''

* * * * *

K890.14 DoD

SYSTEM NAME:

Identity Synchronization Service (IdSS).

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:

These include individual's name (last name, first name, middle initial); unique identifiers including Electronic Data Interchange Person Identifier (EDI PI), other unique identifier (not SSN), 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, 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 PKI certificate information, including FASN–C, 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, ID certificate issuer, ID certificate serial number, ID certificate principal name, ID Thumbprint, ID CN, signature certificate e-mail address, Signature Subject Alternative Name UPN, Signature Thumbprint, Signature Issuer, Signature serial number, Signature CN, Encryption (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, Country Of Citizenship, US Citizenship Status Indicator Code, Cadency of name (*e.g.* Sr, Jr, III), Identity Certificate Serial Number, Persona E–Mail Address, Administrative Organization Code, DoD component, DoD sub-component, Non-DoD agency, Directory publishing restrictions, Reserve component code, Billet code and Pay grade.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

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

PURPOSE(S):

The IdSS will populate and maintain persona-based user objects in DoD enterprise-level Domain Controllers, such as the Active Directory Enterprise Application and Services Forest (AD EASF) being implemented by DISA to provide DoD Enterprise E-Mail, workspace and collaboration tools, file storage, and office applications. In addition, DISA may use the IdSS to populate and maintain personal data elements in DoD Component networks and systems, such as directory services and account provisioning systems.

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 '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 IdSS 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 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 to determine whether information about themselves is contained in this system of records should address written inquiries to 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.

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 system.

RECORD SOURCE CATEGORIES:

DoD Component directories (such as Army Enterprise Directory Service-Lite (EDS–Lite) and the Air Force Directory Service (AFDS)), the Defense Eligibility Enrollment Reporting System (DEERS), and the DISA DoD PKI Global Directory Service (GDS).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 2010–30725 Filed 12–7–10; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DOD–2010–OS–0159]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to alter a system of records.

SUMMARY: The Office of the Secretary of Defense proposes to alter a system of records in its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: This proposed action would be effective without further notice on January 7, 2011 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: Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301–1155, or Ms. Cindy Allard at (703) 588–6830.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records 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 29, 2010, to the House Committee on Oversight and Government Reform, the Senate Committee on 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 30, 2010.

Morgan F. Park,
Alternate OSD Federal Register Liaison Officer, Department of Defense.

DWHS P37

* * * * *

SYSTEM LOCATION:

Delete entry and replace with "Washington Headquarters Services (WHS), Human Resources Directorate (HRD), Labor and Management Employee Relations, Human Resources Directorate, Washington Headquarters Services, Department of Defense, 1155 Defense Pentagon, Washington, DC 20301–1155."

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Delete entry and replace with "Employees of the Office of the Secretary of Defense, Joint Staff, Washington Headquarters Services, and Department of Defense (DoD) Agencies and Field Activities serviced by Washington Headquarters Services Human Resources Directorate who have submitted grievances covered by a negotiated grievance procedure or unfair labor practice charges."

CATEGORIES OF RECORDS IN THE SYSTEM:

Delete entry and replace with "Case file contains individual's name, case number, subject of grievance, background papers, and details pertaining to the case or issue. Case files may also contain the following information that is not solicited from individuals: Work and/or home addresses and telephone numbers and Social Security Numbers (SSN)."

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Delete entry and replace with "5 U.S.C. 7121, Grievance Procedures; DoD 1400.25–M (Subchapter 771), DoD Civilian Personnel Manual (Administrative Grievance System); Washington Headquarters Services Administrative Instruction 37, Employee Grievances, and E.O. 9397 (SSN), as amended."