SYSTEM NAME AND NUMBER: Electronic Security System (ESS), K890.28. (February 1, 2019; 84 FR 1079)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Information Systems Agency (DISA), 6910 Cooper Ave., Ft. Meade, MD 20755–7090.

SYSTEM MANAGER(S): Chief, Security Division, Workforce Services Directorate (WSD)/MP61, Defense Information Systems Agency, 6910 Cooper Ave., Ft. Meade, MD 20755–7090, (301) 225–1235.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 193 and 10 U.S.C. 142; Department of Defense Directive 5105.19, Defense Information Systems Agency (DISA); Department of Defense Directive 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) and HSPD–12, Policy for a Common Identification Standard for Federal Employees and Contractors.

PURPOSE(S) OF THE SYSTEM: The purpose of the system is to control physical access to DISA Headquarters controlled information. DISA's security responsibilities include identifying or verifying individuals through the use of matching PKI (Public Key Infrastructure) information on the CAC to the information registered into the ESS (from the CAC). For entry into building guards also have ability to match picture on CAC to person holding CAC and the picture on file in system.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DISA military and civilian employees and contractors, and others with issued common access card and authorized (regular or frequent) entry to DISA facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, DoD ID Number or credential barcode, photograph of person, information that reflects time of entry/ exit from facility or secure location, and identification expiration dates.

RECORD SOURCE CATEGORIES: Individuals; Defense Enrollment Eligibility Reporting Systems, Department of Defense, other Federal Departments and Agencies, Department of Army, Department of the Air Force, Department of Navy, and U.S. Marine Corps security offices; system managers; computer facility managers; commercial businesses whose employees require access to the facilities or locations; and automated interfaces for user codes on file at Department of Defense sites.

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, the records 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 44 U.S.C. 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: These electronic records are stored on secure servers with access controlled, access restricted by the use of logon, password, and/or card swipe protocols.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Information is retrieved by name and DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Data elements housed in the agency identity management system are destroyed 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal Government personnel. Data is protected by 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 e-App system integrity and the data confidentiality. Access to computerized data is restricted by Common Access Card (CAC).

Access is provided on a need-to-know basis only. The office space in which the servers are located is locked outside of official working hours. Computer terminals are located in supervised areas. The electronic security system utilized to safeguard is password protected. Computerized records maintained in a controlled area are accessible only to authorized personnel. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, the access control system, and is accessible only to authorized personnel. Physical and electronic access is restricted to designated individuals having a need therefore in the performance of official duties and who are properly screened and cleared for need-to-know. Access is restricted to only authorized persons who are properly screened.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves should address written inquiries to the Defense Information Systems Agency (DISA), Workforce Services Directorate (WSD)/ MP61, 6910 Cooper Ave., Ft. Meade, MD 20755–7090.

Signed, written requests should include the individual's full name, current address, telephone number, and the name and number of this System of Records. 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 following 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 Defense Information Systems Agency (DISA) rules for contesting contents and appealing initial agency determinations are published in DISA Instruction 210–225–2; 32 CFR part 316; 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 Defense Information Systems Agency (DISA), Workforce Services Directorate (WSD)/ MP61, 6910 Cooper Ave., Ft. Meade, MD 20755–7090.

Signed, written requests should include the individual's full name, current address, telephone number, and the name and number of this system of records notice. 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 following 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.