test equipment, range and test programs, support equipment, prime movers, generators, publications and technical documentation, training equipment, spare and repair parts, personnel training, Technical Assistance Field Team (TAFT), U.S. Government and contractor technical, engineering, and logistics support services, Systems Integration and Checkout (SICO), field office support, and other related elements of logistics and program support.

(iv) *Military Department:* Army

(v) *Prior Related Cases, if any:* None

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid:* None

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold:* See Attached Annex.

(viii) *Date Report Delivered to Congress:* December 18, 2018

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Turkey—Patriot Missile System and Related Support and Equipment

Turkey has requested the possible sale of four (4) AN/MPQ–65 Radar Sets, four (4) Engagement Control Stations, ten (10) Antenna Mast Groups (AMGs), twenty (20) M903 Launching Stations, eighty (80) Patriot MIM–104E Guidance Enhanced Missiles (GEM–T) missiles with canisters, sixty (60) PAC–3 Missile Segment Enhancement (MSE) missiles, and five (5) Electrical Power Plant (EPP) III. Also included with this request are communications equipment, tools and test equipment, range and test programs, support equipment, prime movers, generators, publications and technical documentation, training equipment, spare and repair parts, personnel training, Technical Assistance Field Team (TAFT), U.S. Government and contractor technical, engineering, and logistics support services, Systems Integration and Checkout (SICO), field office support, and other related elements of logistics and program support. The total estimated program cost is $3.5 billion.

This proposed sale will contribute to the foreign policy and national security of the United States by improving the security of a key NATO Ally on the front lines of the fight against terrorism. Turkey is a member of and critical enabling platform for the Defeat-ISIS campaign and continues to be an essential element of our National Security Strategy and National Defense Strategy efforts to compete against great powers in both Europe and the Middle East. The TPY–2 radar site that Turkey hosts is important to the European Phased Adaptive Approach and to efforts to protect Allies and partners against growing Iranian ballistic missile threats. This sale is consistent with U.S. initiatives to provide key allies with modern systems capable of being networked to defend against regional instability. The proposed sale will enhance Turkey's interoperability with the United States and NATO, making it a more valuable partner in an increasingly important area of the world.

Turkey will use Patriot to improve its missile defense capability, defend its territorial integrity, and deter regional threats. The proposed sale will increase the defensive capabilities of the Turkey military to guard against hostile aggression and shield NATO Allies who might train and operate within Turkey's borders. Turkey should have no difficulty absorbing this system into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The prime contractors will be Raytheon Corporation in Andover, Massachusetts, and Lockheed-Martin in Dallas, Texas. The purchaser requested offsets. At this time offset agreements are undetermined and will be defined in negotiations between the purchaser and contractors.

Implementation of this proposed sale will require approximately 25 U.S. Government and 40 contractor representatives to travel to Turkey for an extended period for equipment de-processing/fielding, system checkout, training, and technical and logistics support.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

Transmittal No. 18–17

Notice of Proposed Issuance of Letter of Offer Pursuant to Section 36(b)(1) of the Arms Export Control Act

Annex

Item No. vii

(vii) *Sensitivity of Technology:*

1. The Patriot Air Defense System contains classified CONFIDENTIAL hardware components, SECRET tactical software and CRITICAL/SENSITIVE technology. Patriot ground support equipment and Patriot missile hardware contain CONFIDENTIAL components and the associated launcher hardware is UNCLASSIFIED. The items requested represent significant technological advances for Sweden Patriot. The Patriot Air Defense System continues to hold a significant technology lead over other surface-to-air missile systems in the world.

2. The Patriot sensitive/critical technology is primarily in the area of design and production know-how and primarily inherent in the design, development and/or manufacturing data related to certain components. The list of components is classified CONFIDENTIAL.

3. Information on system performance capabilities, effectiveness, survivability, missile seeker capabilities, select software/software documentation and test data are classified up to and including SECRET.

4. If a technologically advanced adversary were to obtain knowledge of the hardware and software elements, the information could be used to develop countermeasures or equivalent systems which might reduce system effectiveness or be used in the development of a system with similar or advanced capabilities.

5. A determination has been made that Turkey can provide substantially the same degree of protection for the sensitive technology being released as the U.S. Government. This sale is necessary in furtherance of the U.S. foreign policy and national security objectives outlined in the Policy Justification.

6. All defense articles and services listed in this transmittal have been authorized for release and export to Turkey.

[FR Doc. 2019–00609 Filed 1–31–19; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2019–OS–0003]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency, DoD.

ACTION: Notice of a New System of Records.

SUMMARY: The Defense Information Systems Agency (DISA) proposes to establish a new system of records entitled ''Electronic Security System (ESS), K890.28'' to control physical access to DISA Headquarters. DISA, as a classified collateral open storage area, has security responsibilities mandated by DoD Manual 5200.01, volume 3, DoD Information Security Program: Protection of Classified Information. This includes the use of an integrated electronic access control system. The system identifies and verifies

individuals through the use of data registered into the access control system from an individual's Common Access Card (CAC). The system tracks the entry/exit times of personnel who enter/exit the DISA Headquarters Complex and some rooms within the complex.

DATES: Comments will be accepted on or before March 4, 2019. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* *Federal Rulemaking Portal: http://www.regulations.gov.*

Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number 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: Mrs. Jeanette M. Weathers-Jenkins, DISA Privacy Officer, 6914 Cooper Ave., Fort Meade, MD 20755–7090, or by phone at (301) 225–8158.

SUPPLEMENTARY 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), to retrieve CACs upon separation, to maintain visitor statistics, collect information to adjudicate access to facility, and track the entry/exit times of personnel for purposes of verifying times of entry and exit. For entry into building, the guards have the ability to match picture on CAC to person holding CAC and the picture on file in system.

The DISA 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 address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy, Civil Liberties, and Transparency Division website at *https://defense.gov/privacy.*

The proposed system reports, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on November 5, 2018, 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 Section 6 to OMB Circular No. A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,'' revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated: January 28, 2019.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER

Electronic Security System (ESS), K890.28

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.

[FR Doc. 2019–00608 Filed 1–31–19; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Department of the Army, Corps of Engineers

Notice of Availability of The Great Lakes and Mississippi River Interbasin Study—Brandon Road Integrated Feasibility Study and Environmental Impact Statement—Will County, Illinois

AGENCY: Department of the Army, U.S. Army Corps of Engineers, DoD.

ACTION: Extension of public comment period.

SUMMARY: The U.S. Army Corps of Engineers (USACE), Rock Island and Chicago Districts, are extending the comment period for the report ''The Great Lakes and Mississippi River