BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Department of the Air Force

[Docket ID: USAF-2020-HQ-0003]

Privacy Act of 1974; System of Records

AGENCY: Department of the Air Force (AF), Department of Defense (DoD).

ACTION: Notice of a new System of Records.

SUMMARY: The Air Force Deputy Chief Information Officer is adding a new System of Records titled, Bring Your Own Approved Device (BYOAD), F017 SAF CN A. The BYOAD program provides authorized AF users the ability to voluntarily use their authorized personal mobile devices to conduct government business. This system safeguards government records by providing secured communication mechanisms on personal mobile devices with secured containers and AF Public Key Infrastructure (PKI) certificates for conducting government business.

DATES: This new System of Records is effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The Routine Uses are effective at the close of the comment period.

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

* Federal Rulemaking Portal: https://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 https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Anh Trinh, Department of the Air Force, Air Force Privacy Office, Office of Warfighting Integration and Chief Information Officer, ATTN: SAF/CN, 1800 Air Force Pentagon, Washington, DC 20330-1800, or by phone at (703) 614-8500.

SUPPLEMENTARY INFORMATION: The BYOAD program provides authorized AF military members and civilian employees the ability to use approved personal devices (i.e., smartphone or tablet) to access unclassified government information and applications by installing a Managed Mobile Service (MMS) on their personal devices. Similar federal and private industry programs have shown to increase employee productivity, convenience, and user job satisfaction.

The DoD notices for Systems of Records subject to the Privacy Act of 1974, 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://dpcld.defense.gov.

The proposed system reports, as required by of the Privacy Act, as amended, were

submitted on March 26, 2020, to the House Committee on Oversight and Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 of 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: April 6, 2020.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Bring Your Own Approved Device (BYOAD), F017 SAF CN A.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Amazon Web Services - 9105B Owens Drive, Unit 202, Manassas Park, VA 20111.

SYSTEM MANAGER(S): Program Management Office, Headquarters Cyberspace Capabilities Center Service Transition Division, 203 West Losey Street, Scott Air Force Base, IL 62225, 618-229-6717, AFNIC.NTS.SystemsEngineering@us.af.mil.

Air Force Deputy Chief Information Officer, 1800 Pentagon Air Force, Washington, DC 20330-1800, 703-695-6829, usaf.pentagon.saf-cn.mbx.cns-workflow.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 9013, Secretary of the Air Force: powers and duties; DoD Directive (DoDD) 8100.02, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG); DoD Instruction (DoDI) 8420.01, Commercial Wireless Local-Area Network

(WLAN) Devices, Systems, And Technologies; DoDI 8170.01, Online Information Management And Electronic Messaging; DoDI 5000.76, Accountability and Management of Internal Use Software; AFMAN17-1301, Computer Security (COMPUSEC).

PURPOSE(S) OF THE SYSTEM: The BYOAD program provides authorized AF users a mechanism to voluntarily receive AF approved software on their own authorized personal mobile devices for the purpose of conducting government business. This system enables optimum efficiency by providing authorized AF personnel the convenience of using authorized personal mobile devices equipped with secured communication components which robustly safeguard government information and resources as required by federal standards. User participation for this System of Records is based upon informed, explicit consent.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: AF Active Duty, Reserve, and Air National Guard service members; and civilian employees.

CATEGORIES OF RECORDS IN THE SYSTEM: Individual name, personal cell phone number and other mobile specific numbers for network and device identification.

RECORD SOURCE CATEGORIES: Individuals.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE 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 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 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: The records are maintained in electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Individual's full name and personal cell phone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Destroy 5 years after fiscal year for audit control and planning.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Role-based access control restricts the system access to authorized users with a need-to-know. The system is common access card-enabled and has a firewall with security rules implemented. Records are encrypted during transmission to protect session information and at rest. Access to personally identifiable information is role/attribute based and restricted to those who require the data in the performance of their official duties and have completed annual information assurance and privacy training.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address inquiries to the Deputy Chief

Information Officer, 1800 Pentagon Air Force, Washington, DC 20330. Signed, written requests should include the individual's full name, DoD ID number, current address, and telephone number and this System of Records Notice number. 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 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 if information about themselves is contained in this system of records should address inquiries to the Deputy Chief Information Officer, 1800 Pentagon Air Force, Washington, DC 20330. Signed, written requests should include the individual's full name, DoD ID number, current address, and telephone number. 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. 2020-07507 Filed: 4/8/2020 8:45 am; Publication Date: 4/9/2020]