would require participating vessels to retain and land all catch of allocated groundfish, including undersized fish that they would normally be required to discard. All other species would be handled per normal commercial fishing operations. An EM service provider would review 100 percent of the video footage to verify that the vessels did not discard allocated groundfish. Northeast Fisheries Science Center (Center) staff would conduct a secondary review of the video footage on a subset of trips.

All catch would be assessed shoreside via an accompanying DSM program. Dockside monitors would: (1) Collect biological information for undersized catch, including length-frequency data and age structures on a subset of fish in this market category; (2) verify dealer-reported weights for all species and market categories; and (3) inspect fish holds. Vessels would be authorized to sell catch, including undersized fish, to a limited number of dealers. The vessel and dealer would work collaboratively with the Center to ensure that a dockside monitor is present to observe 100 percent of offloads for this project. Participating dealers would be required to accommodate monitors' sampling protocols and all totes containing undersized fish would be accompanied by a tag identifying the program and the vessel trip report (VTR) number.

Because vessels would be fully monitored, GMRI also requested exemptions to incentivize participation in the project and increase fishing opportunities for healthy stocks. The EFP would allow vessels to use the codend configuration used in the Canadian haddock fishery (5.1-inch (13.0-cm) square mesh codend with modifier haddock separator device or Ruhle trawl) and/or the codend configuration tested in the REDNET project (4.5-inch (11.4-cm) diamond mesh codend). The latter mesh size would be restricted to the Redfish Exemption Area and all standard sector exemption requirements would still apply. These exemptions are intended to improve size selectivity and increase catch of target species, while avoiding groundfish species of concern.

The applicant also requested access to portions of Closed Area II. Vessels would be allowed to fish in the non-essential fish habitat portions of Closed Area II from April 16 through January 31. Vessels would not be allowed to fish in the area from February 1 through April 15 as fishing activity during this time may negatively affect Georges Bank cod and haddock spawning. The applicant states that, due to the distribution and movement of groundfish stocks, this exemption would improve vessels' ability to selectively target healthy groundfish stocks.

The applicant also requested an exemption from sector third-party ASM requirements. Under the current MREM program EFP, ASM data is used to build discard rates for unallocated groundfish stocks and non-groundfish species for MREM vessels. ASM data is not used to build discard rates for allocated groundfish stocks because the vessels are required to retain and land this catch. Therefore, we intend to reduce the ASM coverage target under this EFP to the level necessary to meet the coefficient of variation (CV30) precision standard for the unallocated groundfish stocks. For fishing year 2020, the ASM coverage target would be 9 percent, driven by ocean pout. Although the ASM coverage level should not be based solely on the results of the CV30 standard methodology for the fishery as a whole, we determined that the CV30 methodology is appropriate for this program because the same circumstances do not apply. MREM vessels are not allowed to discard allocated stocks and are fully monitored to ensure compliance. These vessels would only be discarding unallocated stocks, which do not present the same potential for bias. Northeast Fishery Observer Program (NEFOP) observers would not be deployed on these vessels because their fishing activity is not consistent with the Standardized Bycatch Reporting Methodology (SBRM) sampling design. Under an operational program, NMFS would build an SBRM stratum for MREM vessels and these data would be used to build discard rates for unallocated species. Participating vessels would use cameras in lieu of ASM and in additional to NEFOP observers. Because vessels participating in the EFP are not subject to NEFOP coverage, a limited amount of ASM is necessary.

This EFP would be effective for the 2020 and 2021 fishing years. NMFS would authorize a maximum of eight bottom-trawl vessels to participate. MREM vessels would take roughly 240–315 trips per year and would land an estimated 1–3 million pounds (454—1,361 mt) of fish annually. All catch of allocated groundfish stocks would be deducted from the appropriate sector's allocation. Because this is a maximized retention program, vessels would not be permitted to discard legal unmarketable fish for allocated groundfish stocks, regardless of whether the vessel holds a sector exemption to do so through its operations plan.

If approved, the applicant may request minor modifications and extensions to the EFP throughout the year. EFP modifications and extensions may be granted without further notice if they are deemed essential to facilitate completion of the proposed research and have minimal impacts that do not change the scope or impact of the initially approved EFP request. Any fishing activity conducted outside the scope of the exempted fishing activity would be prohibited.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: April 6, 2020.

Hélène M.N. Scalliet,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2020–07473 Filed 4–8–20; 8:45 am]

BILLING CODE 3510–22–P

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 May 11, 2020. 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 4–8–20; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Charter Renewal of Department of Defense Federal Advisory Committees

AGENCY: Department of Defense.

ACTION: Renewal of Federal Advisory Committee.

SUMMARY: The Department of Defense (DoD) is publishing this notice to announce that it is renewing the charter for the Defense Innovation Board (''the Board'').

FOR FURTHER INFORMATION CONTACT: Jim Freeman, Advisory Committee Management Officer for the Department of Defense, 703–692–5952.

SUPPLEMENTARY INFORMATION: The Board's charter is being renewed in accordance with the Federal Advisory Committee Act (FACA) (5 U.S.C., Appendix) and 41 CFR 102–3.50(d). The charter and contact information for the Board's Designated Federal Officer (DFO) are found at *https://www.facadatabase.gov/FACA/apex/FACAPublicAgencyNavigation.*

The Board, through the Under Secretary for Defense for Research and Engineering (USD(R&E)), shall provide the Secretary of Defense and the Deputy Secretary of Defense independent advice and recommendations using a focus on innovative means to address future challenges in terms of integrated change to organizational structure and process, business and functional concepts, technology applications, and any other topics raised by the Secretary of Defense, the Deputy Secretary of Defense, the Chief Management Officer of the Department of Defense or the USD(R&E). The Board shall be composed of no more than 20 members appointed in accordance with DoD policy and procedures. The members must possess some or all of the following: (a) Proven track record of sound judgment in leading or governing large, complex private sector corporations or organizations; (b) demonstrated performance in identifying and adopting new technology innovations into the operations of large organizations in either the public or private sector; (c) demonstrated performance in developing new technology concepts; and (d) proven track record as distinguished academic, professor or researcher at an accredited academic institution.

Board members who are not full-time or permanent part-time Federal civilian officers, employees, or active duty members of the Armed Forces will be appointed as experts or consultants, pursuant to 5 U.S.C. 3109, to serve as special government employee members. Board members who are full-time or permanent part-time Federal civilian officers, employees, or active duty members of the Armed Forces will be appointed pursuant to 41 CFR 102–3.130(a), to serve as regular government employee members.

All members of the Board are appointed to provide advice on the basis of their best judgment without representing any particular point of view and in a manner that is free from conflict of interest. Except for reimbursement of official Board-related travel and per diem, members serve without compensation.