BILLING C

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2024-OS-0048]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new system of records titled, "All-domain Anomaly Resolution and Anomalous Phenomena (AARO) Program Records," AARO-0001. This system of records describes the AARO's collection, use, and maintenance of correspondence and reports submitted from current or former U.S. government employees, service members, or contractors with direct knowledge of U.S. Government programs or activities related to Unidentified Anomalous Phenomenon (UAP) dating back to 1945. This system also includes correspondence and reports submitted from members of the general public and government-affiliated personnel on reported events related to UAP. The submitted information will be used to carry out AARO's mission, including to inform AARO's congressionally directed Historical Record Report. Additionally, DoD is issuing a direct final rulemaking, which will exempt this system of records from certain provisions of the Privacy Act, elsewhere in this issue of the Federal Register.

DATES: This system of records is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]; 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 take effect 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 Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: 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: Paul Plescow, Chief of Staff, All-domain Anomaly Resolution Office, Office of the Deputy Secretary of Defense, 5000 Defense Pentagon, 3C949, Washington, DC 20301-5000, ATTN: AARO; osd.pentagon.ousd-intel-sec.mesg.contact-aaro-mbx@mail.mil; phone 703-693-6081.

SUPPLEMENTARY INFORMATION:

I. Background

The All-domain Anomalous Resolution Office is an office within the Office of the Secretary of Defense charged with the mission to synchronize efforts across the DoD, and with other U.S. Federal departments and agencies, to detect, identify and attribute objects of interest in, on or near military installations, operating areas, training areas, special use airspace and other areas of interest, and, as necessary, to mitigate any associated threats to safety of operations and national security. This includes anomalous, unidentified space, airborne, submerged and transmedium objects. In furtherance of this mission, the AARO Report System covers the AARO's maintenance of correspondence and reports received from current or former U.S. government employees, service members, or contractor personnel with direct knowledge of U.S. Government programs or activities related to UAP dating back to 1945. This system also includes correspondence and reports received from members of the general public and

government-affiliated personnel on events related to UAP. The records include contact information and any other reported information voluntarily provided by submitters.

Additionally, DoD is issuing a direct final rule to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the Federal Register. DoD SORNs 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.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: April 29, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register
Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: All-domain Anomaly Resolution and Anomalous Phenomena Program Records," AARO-0001.

SECURITY CLASSIFICATION: Unclassified; Classified.

SYSTEM LOCATION: All-domain Anomaly Resolution Office, Office of the Deputy Secretary of Defense, 5000 Defense Pentagon, 3C949, Washington, DC 20301-5000. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): The system manager for this system of records is the Chief of Staff, All-domain Anomaly Resolution Office, Office of the Deputy Secretary of Defense, 5000 Defense Pentagon, 3C949, Washington, DC 20301-5000, ATTN: AARO; osd.pentagon.ousd-intel-sec.mesg.contact-aaro-mbx@mail.mil; phone 703-693-6081.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 44 U.S.C. 2107, Acceptance of Records for Historical Preservation; Section 1673 of the National Defense Authorization Act for Fiscal Year 2023 (Pub. Law 117-263).

PURPOSE(S) OF THE SYSTEM:

A. To manage records maintained in furtherance of AARO's mission, including to synchronize efforts across the DoD and with other U.S. Federal departments and agencies to detect, identify, and attribute objects of interest in, on or near military installations, operating areas, training areas, special use airspace and other areas of interest, and, as necessary, to mitigate any associated threats to safety of operations and national security. This includes anomalous, unidentified space, airborne, submerged and transmedium objects.

B. To document, manage, track, and oversee correspondence and reports from current or former U.S. government employees, service members, or contractor personnel with direct knowledge of U.S. Government programs or activities related to UAP dating back to 1945.

C. To document, manage, track, and oversee correspondence and reports from the general public and Government-affiliated personnel concerning events related to UAP.

D. To track and report data, conduct research and statistical analysis, and evaluate program effectiveness.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Current or former U.S. Government employees, uniformed service members, and contractor personnel with direct knowledge of U.S. Government programs or activities related to UAP dating back to 1945 or who report any event related to UAP;

B. Members of the general public and Government-affiliated personnel who provide correspondence or reports concerning events related to UAP.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal information including: Name, DoD ID number, home and email addresses, phone numbers, U.S. Government or contractor employment status, driver's license ID information, security clearance information.

B. Information related to UAPs including: correspondence and reports of events related to UAP, event description or narrative, location relative to the observer, any reported health implications related to UAP, metadata, night vision camera footage, characteristics, including physical state (e.g., size shape, color), observer's assessment of the UAP, including the nature of the phenomenon and whether it was benign, hazard, or a threat, imagery and metadata from photography or recording devices, including mobile phones, and analytical products related to submitted correspondence and reports. The specific types of data in these records may vary widely depending on the nature of the individual's report or correspondence.

RECORD SOURCE CATEGORIES: Records and information maintained in this system of records are obtained from the individuals; some records may also be obtained from other systems or databases maintained by other DoD or OSD components or other agencies.

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, all or a portion of the records or information 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 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 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.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act of 1978, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute, treaty, or other international agreement.

K. To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee.

L. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of scientific study or counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the

national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name and case number, or combination of both.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Disposition pending; until the National Archives and Records Administration has approved the retention and disposition schedule, treat as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification,

marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, DC 20301–1155. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the individual. 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 appropriate 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: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1), (2), (3), and (4); (e)(1); (e)(4)(G), (H), and (I); and (f) pursuant to 5 U.S.C. 552a(k)(1). In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same

exemptions for those records that are claimed for the prior system(s) of records of which they were a part, and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and published in 32 CFR part 310.

HISTORY: None.

[FR Doc. 2024-09608 Filed: 5/3/2024 8:45 am; Publication Date: 5/6/2024]