DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2024–OS–0111]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of the Secretary is establishing a new system of records titled, ''Catch a Serial Offender (CATCH) Program Records,'' DoD–0024. This system of records covers DoD's maintenance of records used to collect and compare adult sexual assault reports for the purpose of identifying alleged serial sexual assault offenders. Additionally, DoD is issuing a notice of proposed rulemaking, which proposes to 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 upon publication; however, comments on the Routine Uses will be accepted on or before November 29, 2024. The Routine Uses listed in this document 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 Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 05F16, 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. Rahwa Keleta, Privacy and Civil Liberties Directorate, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 05F16, Alexandria, VA 22350–1700; *OSD.DPCLTD@mail.mil*; (703) 256–1408.

SUPPLEMENTARY INFORMATION:

I. Background

Section 543 of the Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2015 (Pub. L. 113–291) required the Secretary of Defense to develop a plan that would allow a restricted reporting adult victim of sexual assault to disclose suspect or incident information for the purpose of identifying serial offenders. In response to this requirement, the Naval Criminal Investigative Service (NCIS) developed a database to catalogue and centralize all victim entries into the CATCH program. The eligibility for the CATCH was later extended beyond just Restricted Reporters. The details in submitted CATCH entries are compared against reported subjects in adult sexual assault investigations and other CATCH Program entries. The sexual assault investigation records used for comparison include investigative reports prepared by DoD law enforcement, or other Federal, State, local, Tribal, or foreign law enforcement or investigative bodies, if such records exist. Entries in the CATCH system will consist of information voluntarily submitted into the CATCH system by eligible victims without identifying such victims, through established CATCH processes. At the present time, the CATCH Program gives adult sexual assault victims who filed (1) Restricted Reports, (2) certain Unrestricted Reports where the name of the suspect is not reported to or uncovered by law enforcement, or (3) no official report with the Sexual Assault Prevention and Response (SAPR) program, an opportunity to submit suspect information (without identifying the victim) into the CATCH system after receiving a user name and password from a Sexual Assault Response Coordinator (SARC) or Family Advocacy Program (FAP) representative. There is no self-service feature for CATCH entries; victims must go through a SARC or FAP representative, so they are apprised of their victim's rights and the CATCH Program is fully explained. The Military Criminal Investigative Organizations (MCIOs) specially assigned to CATCH Headquarters, not at the victim's installation, analyze suspect information in victim entries submitted into the CATCH Program. If a match is identified, the investigators will notify SAPR or FAP personnel of the match; the CATCH system protects the identity of the victim by not maintaining information that identifies the victim. The victim's contact information is stored in a separate database, the Defense Sexual Assault Incident Database (DSAID) File Locker or FAP case management system, which is only accessible to certain SAPR and FAP personnel, not MCIOs. Moreover, section 550 of Public Law 116–92 (National Defense Authorization Act for Fiscal Year 2020) contained additional protections specifically for Restricted Reporters to safeguard the restricted nature of their reports, notwithstanding a victim disclosure made pursuant to the CATCH program. More information about the CATCH Program may be found at the U.S. Department of Defense Sexual Assault Prevention and Response Organization website at *https://www.sapr.mil/catch*. Additionally, DoD is issuing a notice of proposed rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in this issue of the **Federal Register**. DoD system of records notices (SORNs) have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or on the Privacy and Civil Liberties Directorate 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: October 23, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

Catch a Serial Offender (CATCH) Program Records, DoD–0024.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301–1000, and other Department installations, offices, or mission locations. 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):

Director, Naval Criminal Investigative Service (NCIS), 27130 Telegraph Road, Quantico, VA 22134–2253, *CATCH@NCIS.NAVY.MIL.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 932, Art. 132 Retaliation; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1044e, Special Victim's Counsel For Victims Sex-Related Offenses; 10 U.S.C. 1561, Complaints of Sexual Harassment: Investigation by Commanding Officers; 10 U.S.C. 1565b, Victims Of Sexual Assault: Access To Legal Assistance and Services of Sexual Assault Response Coordinators and Sexual Assault Victim Advocates; section 543 of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113–291) DoD Instruction 5505.18, Investigation of Adult Sexual Assault in the Department of Defense; DoD Directive 6495.01, ''Sexual Assault Prevention and Response (SAPR) Program; section 550 of Public Law 116–92 (National Defense Authorization Act for Fiscal Year 2020); and E.O. 9397 (Social Security number), as amended.

PURPOSE(S) OF THE SYSTEM:

The system will collect adult sexual assault victims' CATCH entries about alleged perpetrators, without identifying victims, for the purpose of comparison against other CATCH entries and against law enforcement investigative records of adult sexual assaults to identify serial sexual assault offenders. Pursuant to section 550 of Public Law 116–92 (National Defense Authorization Act for Fiscal Year 2020), a victim's disclosure made pursuant to the CATCH program will not operate to terminate a restricted report's status as restricted. Unless a victim expressly decides to participate in an investigation after being notified of a match, the information in a victim's entry in the CATCH system will not be used to initiate an investigation, regardless of the type of victim report (Restricted Reporters, certain Unrestricted Reporters, and victims who filed no report of sexual assault.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals named as alleged sexual assault perpetrators by victims eligible to provide information for the CATCH program (''eligible victims''). Such alleged perpetrators include current, former, and retired Active Duty and Reserve military personnel, DoD civilian personnel, contractors, and members of the public accused of sexual assault by an eligible victim.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system include:

A. Personal Information about individuals named as alleged perpetrators in sexual assault incidents by eligible victims, such as: name and aliases, Social Security number (SSN), date of birth, physical, mailing, and email addresses, phone numbers, place of birth, race/ethnicity, biometric data including photographs, vehicle information, marital status, gender/gender identification, other biographical data, and other information about alleged perpetrators provided by eligible victims.

B. Employment Information such as: position/title, rank/grade, duty station, branch of service, work address, and email address.

C. Case numbers of other investigations associated with alleged perpetrators for purposes of reference.

D. Information about alleged perpetrators obtained by MCIOs from other sources (such as DoD databases; other Federal, State, local, Tribal, or foreign law enforcement databases; or open-source databases) for purposes of validating or confirming information about alleged perpetrators provided by eligible victims or further identifying such alleged perpetrators.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: the victim, DoD systems of records/databases maintaining personnel information, investigative reports, public records and other publicly available sources, commercial data aggregators, subjects of investigation, witnesses, and law enforcement entities.

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.

* Note 1. Given the sensitive nature of records in this system, appropriate discretion and care must be exercised in the extent of disclosure of information under this routine use.

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.

* Note 2. Given the sensitive nature of records in this system, appropriate discretion and care must be exercised in the extent of disclosure of information under this routine use.

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 some other review as authorized by the Inspector General Act of 1987, as amended.

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

K. When an originating record is maintained by the U.S. Department of Defense, records may be disclosed, as authorized, to the U.S. Department of Homeland Security, including the U.S. Coast Guard, for purposes of investigation, verification, or notification by the CATCH investigative program when a reported sexual assault incident allegedly involves a current or former Service member of, or civilian employed by or affiliated with the U.S. Coast Guard.

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 about alleged perpetrators may be retrieved by a unique victim reference number (VRN) maintained in the CATCH system apart from any other identifying victim information or by Defense Sexual Assault Incident Database (DSAID) control number maintained in the CATCH system apart from any other identifying victim information. The CATCH entries do not identify the victim and CATCH system information may not be aggregated to identify a victim. Victim identity and victim contact information is found in DSAID, a separate system maintained and operated by the DoD Sexual Assault Prevention and Response Office.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

CATCH Program records are maintained in this system for a period of 10 years and destroyed.

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 may follow the procedures in 32 CFR part 310. Individuals may address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: *www.FOIA.gov.* 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).''

Requesters should be aware that DoD has claimed an exemption from first-party access pursuant to (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2) and that Congress has provided for an exemption from disclosure under the Freedom of Information Act pursuant to section 550 of Public Law 116–92 (National Defense Authorization Act for Fiscal Year 2020).

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) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f), and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), as applicable. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310. 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 from which they are a part and claims any additional exemptions set forth here.

HISTORY:

None.

[FR Doc. 2024–25034 Filed 10–28–24; 8:45 am]

BILLING CODE 6001–FR–P