



DEPARTMENT OF DEFENSE

[Docket ID: DoD-2021-OS-0003]

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 DoD is establishing a new system of records covering all DoD components titled, “Military Justice and Civilian Criminal Case Records,” DoD 0006. This system of records describes DoD’s collection, use, and maintenance of records for the administration of the Uniform Code of Military Justice (UCMJ) and disciplinary cases under the authority of the DoD. These records include legal information and filings used to facilitate public access to the Department’s court docket. This system of records also includes records created when DoD legal practitioners in support of the U.S. Department of Justice, prosecute in U.S. District Courts crimes that occurred on military installations or property. This system of records will apply enterprise-wide for the furtherance of good order and discipline. Individuals covered by this system of records includes armed forces members and others as identified in Article 2 of the UCMJ, as well as civilians who are alleged to have engaged in criminal acts on DoD installations and properties. Additionally, the 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 today’s issue of the *Federal Register*.

DATES: This new system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT 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: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

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. Lyn Kirby, Defense Privacy, Civil Liberties, and Transparency Division, Directorate for Oversight and Compliance, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

The “Military Justice and Civilian Criminal Case Records” system of records is being established as a DoD-wide Privacy Act system of records for use by all DoD offices and components. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

In Section 5504 of the National Defense Authorization Act of 2017, Congress mandated the Secretary of Defense prescribe and implement uniform standards and criteria for the conduct of each of the following functions at all stages of the military justice system, including pretrial, trial, post-trial, and appellate processes: (1) collection and analysis of data concerning substantive offenses and procedural matters in a manner that facilitates case management and decision making within the military justice system, and that enhances the quality of periodic reviews; (2) case processing and management; (3) timely, efficient, and accurate production and distribution of records of trial within the military justice system; and (4) facilitation of access to docket information, filings, and records, taking into consideration restrictions appropriate to judicial proceedings and military records. In response, the DoD has been modifying its information systems to implement uniform standards and criteria to allow for improved management and analysis of these military justice records and activities across the DoD. In association with this effort, this DoD-wide SORN also is being published to unify and standardize the management of this data in accordance with the Privacy Act of 1974.

The purpose of this system of records is to support the collection, maintenance, use, and dissemination of records compiled by the DoD for the adjudication and litigation of cases under the UCMJ, as well as criminal proceedings brought in U.S. District Courts for offenses occurring on DoD installations or property. This system will contain the information, records, and filings publicly accessible on the Department's court docket. It also supports the compilation of internal statistics and reports related to these activities.

The DoD is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the *Federal Register*.

The DoD SORNs have been published in the *Federal Register* and are available from the address in the FOR FURTHER INFORMATION CONTACT section or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.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, the DoD has provided a report of this system of records to the OMB and to Congress.

Dated: May 12, 2021.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: “Military Justice and Civilian Criminal Case Records,” DoD 0006.

SECURITY CLASSIFICATION: Unclassified; Classified

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, D.C. 20301-6000.

SYSTEM MANAGER(S): The system managers are the Judge Advocates General of the Army, Navy, Air Force and the Staff Judge Advocate General to the Commandant of the U.S. Marine Corps. Their addresses will vary according to the location where the actions described in this notice are conducted. The Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records have been delegated to the DoD components. DoD components include the Military Departments of the Army, Air Force (including the U.S. Space Force), and Navy (including the U.S. Marine Corps), field operating agencies, major commands, field commands, installations, and activities. To contact the system manager at the DoD component with oversight of the records, go to www.FOIA.gov to locate the contact information for each component’s Freedom of Information Act (FOIA) office.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. Chapter 47, §§ 801-946a, Uniform Code of Military Justice (UCMJ); 10 U.S.C. § 2683, Relinquishment of Legislative jurisdiction- minimum drinking age on military installations; 10 U.S.C. § 7037, Judge Advocate General, Deputy Judge Advocate General, and general officers of Judge Advocate General’s Corps: appointment; duties; 10 U.S.C § 8046, Staff Judge Advocate to the Commandant of the Marine Corps; 10 U.S.C. § 8088, Judge Advocate General’s Corps: Office of the Judge Advocate General; Judge Advocate General; appointment, term, emoluments, duties; 10 U.S.C. § 9037, Judge Advocate General, Deputy Judge Advocate General: Appointment and duties; 18 U.S.C. §

13, Laws of States adopted for areas within Federal jurisdiction; 18 U.S.C. § 3401, Misdemeanors; application of probation laws; 28 U.S.C. Chapter 43, United States Magistrate Judges; 28 U.S.C. § 515, Authority for legal proceedings; commission, oath, and salary for special attorneys; 28 U.S.C. § 543, Special attorneys; 28 U.S.C. § 636, Jurisdiction, powers, and temporary assignment; 28 U.S.C. § 3008, Proceedings before United States magistrate judges; 40 U.S.C. § 3112, Federal jurisdiction; 32 CFR § 634.32, Traffic violation reports; 32 CFR § 634.25, Installation traffic codes; Executive Order (E.O.) 11835, Prescribing Amendments to the Manual for Courts-Martial, United States, 1969 (Revised Edition); E.O. 12473, Manual for Courts-Martial, United States, 1984; E.O. 13825, 2018 Amendments to the Manual for Courts-Martial, United States; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

- a. To support adjudication and litigation by military judges, convening authorities, prosecutors, and defense counsel of disciplinary cases, hearings, courts-martial and adverse administrative actions under the UCMJ.
- b. To support litigation of civilian criminal cases before Federal magistrate judges for offenses conducted on DoD installations and property.
- c. To manage disciplinary case processes, reviews and appeals, from the complaint filing through adjudication, review, and when applicable, appeals; including tracking, managing, and storing case-related information and documents; facilitating case research and reporting; and creating statistics on key business functions and metrics.
- d. To facilitate the public access to docket information, filings, and hearings appropriate to UCMJ judicial proceedings as authorized by law and policy.
- e. To share information that supports the enforcement and administration of laws for individuals within the jurisdiction of the DoD, including violations of law occurring on and off military installations.

f. To verify, validate, and report professional activities for attorneys, legal service professionals, and other professionals associated with legal proceedings, to licensing organizations as required, and to support the administration of background checks in support of employment and licensing of such personnel as authorized by law.

g. To provide appropriate notification to victims in accordance with Federal victim protection laws.

h. To identify and address conduct by DoD Service members that may warrant criminal or disciplinary action, and conduct by civilians on DoD military property; to uphold and enforce the law; and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals within the DoD's jurisdiction who are the subjects of current or previous law enforcement actions; adverse administrative actions under the UCMJ or Federal criminal code; investigations, and/or prosecutions. Victims, witnesses, informants, and third parties who may have knowledge of offenses under the UCMJ or other criminal activities. Attorneys, military judges, legal personnel, and DoD personnel involved in UCMJ and Federal criminal court functions (to include investigations and legal prosecutions).

NOTE: DoD jurisdiction applies to individuals subject to the UCMJ (*see* 10 U.S.C. § 802, Article 2, UCMJ). This system also extends to civilians who are alleged to have engaged in criminal acts on military installations or military property.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of Records within this system support prosecutors, defense counsel, military judges and legal personnel in the administration of the Uniform Code of Military Justice and in the prosecution of civilian criminal offenses, within the DoD's jurisdiction, litigated in coordination with the Department of Justice.

a. Personal Information such as: name and aliases; DoD ID number; Social Security Number; date of birth; physical, mailing, and e-mail addresses; phone numbers; place of birth; citizenship/immigration status; race/ethnicity; medical information/medical records; biometric

data; driver's license number; vehicle registration information; marital status; gender/gender identification; biographical data; property information.

b. Employment Information such as: position/title, rank/grade, duty station; work address, e-mail address, supervisor's name and contact information; military records, personnel records, financial information, education and training records.

c. Legal Information such as: trial transcripts, records of trial, charge sheets, exhibits (e.g. documents and recordings attached to records of trial), evidentiary data in any form (including papers, photographs, electronic recordings, electronic data, or video records that were obtained, seized, or otherwise lawfully acquired from any source,) pleadings, sentencing reports, court motions, correspondence, filings, and supporting documents; forms, evidentiary data, supporting documents, investigatory data associated with non-judicial punishment under Article 15 of the UCMJ and adverse actions or administrative actions; victim and witness statements; notifications, recordings, and elections of victim rights and investigative data (including investigative findings and reports); criminal history; information received from other governmental agencies, confidential sources and other sources pertaining to an investigation, as well as investigatory referrals from other agencies, tips, and leads pertaining to potential criminal activities.

RECORD SOURCE CATEGORIES: The DoD may receive information in the course of the law enforcement activities described in this system of records from nearly any source. Sources of information include: courts and tribunals, domestic and foreign governmental and quasi-governmental agencies and data systems, public records and other publicly available sources, commercial data aggregators, subjects of investigation, victims, witnesses, confidential sources, attorneys and other legal personnel, DoD employees participating in disciplinary functions, investigators, 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 United States, 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 Department of Justice (including Offices of the United States Attorneys) or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when necessary to assist in the development of the DoD or such agency's legal and/or policy position.
- f. 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.
- g. 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.

h. 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.

i. 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.

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

k. To a Federal, state, local, tribal, foreign, or international agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit, or if necessary to obtain information relevant to a DoD decision concerning the hiring or retention of an individual, the issuance of a security clearance, license, contract, grant, or other benefit.

l. To a public or professional licensing authority, organization, board, agency or society (to include a medical or legal professional society, organization, or licensing authority), if such information is needed to perform functions related to licensing or professional standards monitoring or compliance, or when the information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral,

educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

m. To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

n. To the Department of State when it requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about a pending legal action or prosecution with transnational implications.

o. To unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. §§ 7111 and 7114, the Merit Systems Protection Board, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective actions, or grievances, or conducting administrative hearings or appeals.

p. To the Merit Systems Protection Board and the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems; review of Office of Personnel Management or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

q. To state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. §§ 5516, 5517, or 5520 and only to those state and local taxing authorities for which an employee or Service member is or was subject to tax, regardless of whether tax is or was withheld. The information to be disclosed is information normally contained in Internal Revenue Service (IRS) Form W-27.

- r. To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.
- s. To the general public in order to provide access to docket information, filings, and records in compliance with Article 140a, UCMJ or other Federal statutes, and corresponding DoD or Service implementing guidance, regulations, or policies.
- t. To a confinement facility or prison, if confinement is adjudged, and the facility is outside the jurisdiction of the DoD.
- u. To the U.S. Department of Veterans Affairs (VA) to assist the Department in determining the individual's entitlement to benefits administered by the VA.
- v. To other Federal, State, tribal, and local government law enforcement and regulatory agencies and foreign governments, individuals and organizations during the course of an investigation or the processing of a matter, or during a proceeding within the purview of the local, state, federal or host-country specific laws, to elicit information required by the Department to carry out its functions and statutory mandates.

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: Individual's name, DoD ID number and/or SSN, or aliases.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained and disposed in accordance with National Archives and Records Administration Schedules. The Military Departments retain records in accordance with their

individual Records and Information Management retention schedules. The retention period may be obtained by contacting the system manager for the Military Department.

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, the DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including CAC authentication and password; SIPR 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 address written inquiries to the DoD office with oversight of the records. The public may identify 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, identifier (i.e., DoD ID Number or Defense Benefits Number), date of birth, current address, and telephone number 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: 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 appropriate system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the appropriate system managers(s). Signed written requests should contain the full name, identifier (i.e. DoD ID Number or DoD Benefits Number), date of birth, and current address and telephone number 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).”

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)-(I), (5), and (8); and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and

(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 systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: None.

[FR Doc. 2021-10367 Filed: 5/24/2021 8:45 am; Publication Date: 5/25/2021]