BILLIN

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-0137]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is modifying, renumbering, and renaming a Department-wide system of records titled DoD DPR-39, "DoD Personnel Accountability and Assessment System." This system of records is being modified to support additional information systems being established within the DoD using the same categories of data for the same purposes. The system number is changing from DPR-39 to DoD-0012, to reflect its status as a DoD-wide system of records, and the name is changing from "DoD Personnel Accountability and Assessment System" to "Defense Accountability and Assessment Records." The DoD is also modifying numerous sections of the notice, including the system location, system managers, authority for maintenance of the system, purpose of the system, individuals covered by the system, record source categories, routine uses, and notification procedures. This system of records covers DoD's maintenance of records about accountability for and status of DoD-affiliated individuals, including Military Service members, civilian employees, dependents and family members, contractors, and other DoD-affiliated personnel (including individuals in other uniformed services performing DoD-related assignments) in a natural or man-made disaster, public health emergency, similar crisis, or when directed by the Secretary of Defense. This system may also apply to DoD's maintenance of records about DoD-affiliated individuals that are necessary to respond to anomalous health incidents (AHIs), such as AHIs contemplated by two sections of the National Defense Authorization Act of Fiscal Year 2022, when such records are not covered by another system, such as EDHA 07, Military Health

Information System (June 15, 2020). Additionally, DoD is issuing a direct final rule, which is exempting this system of records from certain provisions of the Privacy Act, elsewhere in today's 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 [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 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: Ms. Rahwa Keleta, Defense Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, 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 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is modifying an existing DoD-wide Privacy Act system of records titled DPR-39, DoD Personnel Accountability and Assessment System, March 26, 2020 (85 FR 17047) and renaming it DoD-0012, Defense Accountability and Assessment Records. 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.

This system of records contains personnel accountability and assessment records created and maintained by all component parts of DoD, wherever they are maintained. The system consists of both electronic and paper records and will be used by DoD components and offices to maintain records about accountability for and status of DoD-affiliated individuals, including Military Service members, civilian employees, dependents and family members, contractors, and other DoD-affiliated individuals, in preparation for, response to, or recovery from a natural or man-made disaster or public health emergency, or when directed by the Secretary of Defense. Such events could include severe weather events, acts of terrorism or severe destruction, pandemics or major outbreaks, and similar crises. This system may also apply to DoD's maintenance of records about DoD-affiliated individuals that are necessary to respond to anomalous health incidents (AHIs), such as AHIs contemplated by sections 910 or 6603 of the National Defense Authorization Act of Fiscal Year 2022, when such records are not covered by another system, such as EDHA 07, Military Health Information System, 85 FR 36190 (June 15, 2020).

The DoD is updating this SORN to add the standard DoD routine uses (routine uses A through J) and three other routine uses. Additionally, the following sections of this SORN are being modified as follows: (1) the Authority for Maintenance of the System section to add additional authorities; (2) the Security Classification section to add "Classified"; (3) the Categories of Individuals Covered by the System section to expand the individuals covered and Categories of Records to clarify how the records relate to the revised Category of Individuals; (4) the Administrative, Technical, and Physical Safeguards to update the individual safeguards protecting the personal information; (5) the Contesting Records Procedures section to update the appropriate citation for contesting records; (6) the System Manager and System Location sections to update the addresses and office names; (7) the Purpose(s) of the System section to clarify the collection of why this system is needed; (8) the Policies and Practice for Storage of Records, to list different ways records may be kept; (9) the Record Source Categories to add additional sources where information can be acquired; (10) the Policies and Practices For Retrieval Of Records: to include "other unique identifier"; (11) the Record Access Procedures section to reflect the need for individuals to provide a notarized statement or an unsworn declaration and to identify the appropriate DoD office or component to which their request should be directed; and (12) the Exemptions Promulgated for the System, to add an exemption from certain provisions of the Privacy Act.

This system also documents individuals' check-in data or other information that is self-reported or provided by third parties (e.g., supervisors or commanders) if necessary to maintain accountability or inform agency responses to emergencies, including to ensure the safety and protection of the workforce. The DoD Components may also collect information about DoD personnel and their dependents for needs and status assessments as a result of the natural or man-made disaster, public health emergency, similar crisis, AHIs, or when directed by the Secretary of Defense. The DoD Components may also use accountability data for accountability and assessment reporting exercises.

This system of records is being modified to reflect and affirm its status as a DoD-wide system of records. The remaining modifications principally change the SORN to reflect the broad intended use of this system of records to cover data stored in multiple information systems throughout the Department.

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.

Additionally, the 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 Freedom of Information 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: December 9, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Defense Accountability and Assessment Records, DoD-0012.

SECURITY CLASSIFICATION: Unclassified and 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, DC 20301-6000.

SYSTEM MANAGER(S): The system managers are as follows:

A. Senior Program Manager for Casualty and Mortuary Affairs, Office of the Under Secretary of Defense (Personnel & Readiness), Deputy Under Secretary of Defense for Military Community and Family Policy, 4000 Defense Pentagon, Washington DC 20301-4000.

B. Individuals in DoD components who have responsibilities for maintaining records for personnel accountability and assessment purposes. To obtain information on the system managers at the Military Departments, Combatant Commands, Defense Agencies, or other Field Activities with oversight of the records, please visit www.FOIA.gov to contact the component's Freedom of Information Act (FOIA) office. The Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system notice have been delegated to the employing DoD components.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 137, Under Secretary of Defense for Intelligence and Security; 10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 8013, Secretary of the Navy; 10 U.S.C. 9013, Secretary of the Air Force; 10 U.S.C. 2672, Protection of buildings, grounds, property, and persons; Public Law 117-82, National Defense Authorization Act for Fiscal Year 2022, including sections 910 (Cross-Functional Team for Emerging Threat Relating to Anomalous Health Incidents) and 6603

(Anomalous Health Incidents Interagency Coordinator); DoD Directive 5525.21, Protection of Buildings, Grounds, Property and Persons and Implementation of 2672 of Title 10, United States Code; DoD Instruction (DoDI) 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; DoDI 6200.03, Public Health Emergency Management (PHEM) Within the DoD; DoDI 6055.17, DoD Emergency Management (EM) Program; DoDI 1444.02, Volume 2, Data Submission Requirements for DoD Civilian Personnel: Nonappropriated Fund (NAF) Civilians; and E.O. 9397, as amended.

PURPOSE(S) OF THE SYSTEM:

A. To accomplish personnel accountability for and status assessment of DoD-affiliated individuals in preparation for, response to, or recovery from a natural or man-made disaster or public health emergency, similar events of concern, or when directed by the Secretary of Defense. Such events could include severe weather events, acts of terrorism or severe destruction, pandemics or major outbreaks, anomalous health incidents, and similar crises.

B. To document an individual's status reporting data or other information that is self-reported or provided by third parties (e.g. supervisors, commanders, or caretakers).

C. To maintain accountability or inform agency responses to emergencies and similar events of concern, including the safety and protection of the workforce.

D. To conduct needs and status assessments as a result of the natural or man-made disaster, public health emergency, similar crisis or event or concern, or when directed by the Secretary of Defense. This could include assessments and referrals that are necessary to respond to a reported suspected anomalous health incident, when such records are not covered by another system, such as EDHA 07, Military Health Information System, 85 FR 36190 (June 15, 2020).

E. To support accountability and assessment reporting exercises.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DoD-affiliated individuals such as: Military Service members (active duty, Guard/Reserve and the Coast Guard personnel when operating as a military service with the Navy), civilian employees (including

non-appropriated fund employees), dependents and family members of the above, contractors or other individuals working at or requiring access to DoD facilities; and other DoD-affiliated individuals that may require personnel accountability or assessment by DoD.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal and work-related information, such as name, Social Security Number (SSN), Department of Defense Identification Number (DoD ID Number), other unique identifier, DoD affiliation, date of birth, duty station address and telephone numbers, home and email addresses, and telephone numbers (to include cell number).

B. Emergency information, such as spouse's and children's names, dates of birth, contact information and address; parents' names, addresses and contact information; or other emergency contact name and contact information.

C. Needs and status information of DoD-affiliated individuals, such as component-conducted needs and status assessment records identifying specific emergent needs, the date of the assessment, and the type of event and category classification.

D. Federal Emergency Management Agency (FEMA) number, if issued, and additional information about individuals if necessary to maintain personnel accountability or inform agency responses to emergencies, such as travel and health-related information covered under the Privacy Act. Personal information maintained will be the minimum necessary in order to accomplish the accountability and/or emergency response mission in accordance with the Privacy Act of 1974 and DoD Instruction 5400.11, consistent with applicable law.

E. Information reported about events of concern, including anomalous health incidents, such as date and description of event or incident, location, symptoms, actions taken, and other information requested by DoD to inform agency responses.

Note 1: Excluded from this system of records are employee occupational medical records covered by the U.S. Office of Personnel Management (OPM) regulation at 5 CFR part 293, subpart E, Employee Medical File System Records. The regulation requires agencies that are

subject to OPM's recordkeeping requirements to maintain employee occupational medical records in the agency's Employee Medical File System. Such records are covered exclusively by the OPM/GOVT-10, Employee Medical File System of Records.

Note 2: Excluded from this system of records are records gathered or created to assist DoD during a declared public health emergency in maintaining a safe and healthy DoD environment—including for contact tracing purposes--such as work and training environments, transportation facilities and vehicles, base housing, retail and recreation areas, hospitals, and other health care facilities which are maintained in the DoD-0013, DoD Declared Public Health Emergency Exposure Records system of records.

Note 3: Excluded from this system of records are records gathered or created for the delivery of health care to eligible personnel for the medical treatment of anomalous health incidents (such as those contemplated by sections 732, 910, and 6603 of the National Defense Authorization Act of Fiscal Year 2022) that are maintained in the EDHA 07, Military Health Information System, system of records.

RECORD SOURCE CATEGORIES:

A. Individuals and supervisors, commanders, and other third parties on behalf of individuals.

B. Federal Agencies, Public Health and Emergency Management authorities, and non-governmental organizations, such as the Red Cross.

C. The Defense Enrollment Eligibility Reporting System (DEERS database).

D. DoD Component program offices including DoD contractor databases, internal security databases and files, personnel security databases and files, DoD component human resources databases and files.

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 some 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 or treaty.

K. 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.

L. 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 military 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-2.

M. To any person, organization or governmental entity (e.g., other Federal, State, territorial, local, or foreign, or international governmental agencies or entities, first responders, American Red Cross, etc.), as is necessary and relevant to notify them of, respond to, evaluate, or

guard against a serious and imminent terrorist or homeland security threat, natural or manmade disaster, public health emergency, anomalous health incident, or other similar crisis or event of concern, including for the purpose of enabling emergency service personnel to locate an individual.

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 individual's name, DoD ID Number, Social Security Number, other unique identifier, date of birth, and/or date of occurrence.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are to be retained by the Office of the Secretary of Defense (OSD), the Joint Staff, the Military Departments, the Defense Agencies, and the Defense Field Activities in accordance with their NARA-approved records retention schedules.

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 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. Individuals should also provide any additional identifiers (i.e., DoD ID Number or Defense Benefits Number), date of birth, and telephone number. In addition, the individual 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 (e), and published in 32 CFR part 310.

HISTORY: March 26, 2020 (85 FR 17047).

[FR Doc. 2022-27145 Filed: 12/15/2022 8:45 am; Publication Date: 12/16/2022]