

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Force Risk Reduction (FR2)

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

05/02/2025

Force Safety and Occupational Health (FSOH)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☒ From Federal employees
- ☐ from both members of the general public and Federal employees ☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Originally directed by the Secretary of Defense in 2001, the Force Risk Reduction (FR2) tool is a data warehouse that aggregates and displays event and hazard data from the Air Force, Army, Navy, Marine Corps, and DoD Agencies, as well as population data, military injury data, workers compensation data, and lost time data from other Fourth Estate systems. This data is used for trending and analysis in determining high risk behavior areas and in mitigating these risks to protect the strength of our force.

To support this mission information is maintained on individuals who suffer injuries or illness caused by a DoD mishap, or individuals otherwise involved in a DoD mishap, near miss, or hazard and/or related investigation/assessment. Specifically:

- Personal information including: first name, last name, Social Security Number (SSN), DoD ID number, date of birth, age, sex, ethnicity, email address, phone number, marital status, language(s) spoken and citizenship information.
- Employment and education information including: grade/rank, job title, pay and allowances, military unit destination, branch and location, educational status, deployment date, work schedule, and training and licensure information.
- Health information including: alcohol use, drug use, blood alcohol level, fatigue factors, type and location of injury or illness, date of injury or illness, evaluation and treatment summary, and disability information.
- Other information including: personal protective equipment use, reports and witness statements, and board findings and recommendations.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Verification; Identification; Mission-related use

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

FR2 is not the initial point of collection. Individuals may have the opportunity to object to the collection of their PII at the initial point of collection, however, once collected information may be shared with FR2 as authorized and stated within all applicable Privacy Act Statements and System of Records Notices.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

FR2 is not the initial point of collection. Individuals may have the opportunity to object to the specific uses of their PII at the initial point of

collection, however, once collected information may be shared with FR2 as authorized and stated within all applicable Privacy Act Statements and System of Records Notices.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? (Check all that apply)

☐ Within the DoD Component Specify.

☒ Other DoD Components (i.e. Army, Navy, Air Force) Specify.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) Specify.

☐ State and Local Agencies Specify.

☐ Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) Specify.

☐ Other (e.g., commercial providers, colleges). Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☐ Individuals ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

Defense Manpower Data Center Data Base, Defense Civilian Personnel Data System, Defense Enrollment Eligibility Reporting System (DEERS), Defense Casualty Information Processing System, Defense Civilian Personnel Data System (DCPDS), Army Safety Management Information System 2.0 (ASMIS), Air Force Safety Automated System (AFSAS), T Defense Injury and Unemployment Compensation System (DIUCS), Armed Forces Health Longitudinal Technology Application (AHLTA), and MHS Genesis.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

☐ E-mail ☐ Official Form (Enter Form Number(s) in the box below)

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☐ Website/E-Form

☐ Other (If Other, enter the information in the box below)

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

GRS 2.7, item 040 (DAA-GRS-2017-0010-0004)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cutoff annually after monitoring is conducted. Destroy 30 years after cut off.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.

(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

10 U.S.C. 113, Secretary of Defense; 5 U.S.C. 7902, Safety Programs; Executive Order (E.O.) 12196, Occupational Safety and Health Act of 1970; DoD Instruction (DoDI) 6055.01, DoD Safety and Occupational Health (SOH) Program; DoDI 6055.05, Occupational and Environmental Health (OEH); DoDI 6055.07, Mishap Notification, Investigation, Reporting, and Record Keeping; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.

(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."

(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

System does not collect information from members of the public.