



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Deficiency Reporting System (JDRS)
--

Department of the Navy - NAVAIR

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

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

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR** Enter DITPR System Identification Number
- Yes, SIPRNET** Enter SIPRNET Identification Number
- No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes**
- No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes**
- No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

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

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

OPNAVINST 4790.2, Naval Aviation Maintenance Program (NAMP)
OPNAVINST 4790.15, Aircraft Launch and Recovery Equipment Maintenance Program (ALREMP)
USAF TO# 0035D-54, USAF Deficiency Reporting and Investigation System
AR 702-7-1, Reporting of Product Quality Deficiencies Within the U.S. Army
USCG CDMTINST 13020.1, USCG Aeronautical Engineering Maintenance Management Manual
E. O. 9397 (SSN), as amended
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN) as amended
5 U.S.C. 301, Departmental Regulations
5 U.S.C. 7311; 10 U.S.C. 5013
E.O. 9397 (SSN) as amended
E.O. 10450, Security Requirements for Government Employees, in particular sections 2 - 9, and 14
E.O. 12958, Classified National Security Information
E.O. 12968, Access to Classified Information
DoD Regulation 5200.2-R, Personnel Security Program Regulation
SECNAVINST 5510.30A, Department of Navy Personnel Security Program

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

PURPOSE OF SYSTEM: The JDRS system is designed for the joint warfighter to submit deficiencies in material and processes and allows for the engineering, quality and logistics support teams to investigate and report resolution. The system is a workflow system that identifies who submits and approves the deficiency reports and resolution responses. The users PII is not displayed to users. PII is only used for authenticating users for access to the system.
PRINCIPLE PURPOSES OF PII COLLECTION: To record names(Full), last 4 digits of Social Security Number and citizenship for validating the individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: Used by developers and administrators
DISCLOSURE: Disclosure of this information is voluntary, however, failure to provide the requested information may impede, delay or prevent further processing of this request and result in denial of access to this computer application.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that the JDRS system, with the limited collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. In addition, all systems are vulnerable to "insider threats". JDRS managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. These individuals have gone through extensive background and employment investigations.
Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Only a person granted a Service Enrollment Administrator account could access the PII data at the presentation layer. System Administrators and Developers could access the raw data as it is stored in the database. Service Enrollment Administrators, System Administrators and developers are authorized access to this information based on their approved roles and privileges within JDRS by the Program Manager. Access to this information is strictly enforced and controlled by the JDRS Program Manager.
Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

N/A

Other DoD Components.

Specify.

N/A

Other Federal Agencies.

Specify.

N/A

State and Local Agencies.

Specify.

N/A

- Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

N/A

- Other** (e.g., commercial providers, colleges).

Specify.

N/A

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

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

Disclosure is voluntary; however, failure to provide the requested information may prevent access to this computer application.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Information is required for user authentication.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The following Privacy Act Statement is presented to the user with a checkbox that the user must acknowledge.

Privacy Act Statement

PRINCIPLE PURPOSES: To record names (Full), last 4 digits of Social Security Numbers and citizenship for the purpose of authentication and/or identification of an individual for access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: Used by developers and administrators.

DISCLOSURE: Disclosure of this information is voluntary, however, failure to provide the requested information may impede, delay or prevent further processing of this request and result in denial of access to this computer application.

(checkbox) I acknowledge disclosure of Privacy Act information within the JDRS system.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.