



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Range Facility Management Support System (RFMSS)

Department of the Army Program Executive Office Enterprise Information Systems

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

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      3827 (DA00249)
- 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.

The authority for the Range Facility Management Support System to collect information is derived from:  
10 U.S.C. 3013, Secretary of the Army;  
Army Regulation 190-40, Serious Incident Report  
Army Regulation 95-2, Air Traffic Control, Airspace, Airfields, Flight Activities and Navigational Aids  
FAA Federal Aviation Regulation (FARS) – Part 73

**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.

The Range Facility Management Support System application assists Army Unit Training managers in scheduling firing range and land training areas; and enhances Range Control management personnel ability to manage firing ranges and training areas. It includes a scheduling capability; unit and range control approval process for ranges and training areas; live training asset allocation; automation of range firing desk operations; resolution of safety, scheduling and environmental conflicts; and utilization reporting.

The following PII data is collected by the RFMSS system user personnel from the individual: personal and work-related information.

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

Due to the level of safeguarding of data in RFMSS, the risk to individuals' privacy is minimal. There is no risk in providing an individual the opportunity to object or consent.

**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.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

also required notification of affected individuals within 10 working days of an incident. Contractor shall ensure that no PII is stored on contractor equipment, nor at contractor facilities. Contractor shall ensure that all personnel are trained on proper handling of PII to include reporting requirements".

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

Specify.

**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.

Since the PII information in RFMSS is provided by the individual involved, the opportunity to object is provided when the information is initially collected.

(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.

Since the PII information in RFMSS is provided by the individual involved, the opportunity to consent is provided when the information is initially collected.

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



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

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

**PRIVACY ACT STATEMENT**  
Range Facility Management Support System  
**AUTHORITY:** The legal authority for recording Personal Identifiable Information in the Range Facility Management Support System is 10 USC 3013 in the overall Secretary of the Army authority.

**PRINCIPAL PURPOSE:** Personal Identifiable Information is used by the Range Facility Management Support System application to record information about an individual who has gained access to the system to perform a task or mission for the Army, or performs selected tasks within the application pertaining to range safety, serious incident reporting, and/or transmission of official documentation.

**ROUTINE USE(S):** The Personal Identifiable Information will be used to record names of system users; Range Safety Officers and Officers-in-Charge; personnel involved with a serious incident, and/or officials transmitting official historical information/reports. The Personal Identifiable Information will be released only to Department of Defense personnel or other US Government personnel who have a need to know and will not be released or disclosed to anyone outside of the US Government.

**DISCLOSURE:** Disclosure of Personal Identifiable Information is voluntary; however, failure to provide required information will result in disapproval of your request to utilize the Range Facility Management Support System.

**THIS PRIVACY ACT STATEMENT WILL BE PROMAENTLY DISPLAYED ON A BANNER ON THE OPENING SCREEN OF THE SYSTEM. ACKNOWLEDGEMENT AND APPROVAL IS REQUIRED PRIOR TO BEING GRANTED PERMISSION TO ACCESS THE 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.**