PRIVACY IMPACT ASSESSMENT (PIA)

For the

Remedy ARS - Rating Workbench
Department of the Navy - SPAWAR

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: _____
- ☐ 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 BIN 2690, UPI 007-17-01-04-02-2690-00

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 DPR 34, T7335, OPM/GOVT-2

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.

5 U.S.C. 301, Department Regulations;
5 U.S.C. Sections 1104, 3321, 4305, and 5405;
Executive order 12107.
5 U.S.C. Chapter 11, Office of Personnel Management;
5 U.S.C. Chapter 13, Special Authority;
5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports;
5 U.S.C. Chapter 31, Authority for Employment;
5 U.S.C. Chapter 33, Examination, Selection, and Placement;
5 U.S.C. Chapter 41, Training;
5 U.S.C. Chapter 43, Performance Appraisal;
5 U.S.C. Chapter 51, Classification;
5 U.S.C. Chapter 53, Pay Rates and Systems;
5 U.S.C. Chapter 55, Pay Administration;
5 U.S.C. Chapter 61, Hours of Work;
5 U.S.C. Chapter 63, Leave;
5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress;
5 U.S.C. Chapter 75, Adverse Actions;
5 U.S.C. Chapter 83, Retirement;
5 U.S.C. Chapter 99, Department of Defense National Security Personnel System;
5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program;

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness;
E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended;
29 CFR part 1614.601, EEO Group Statistics;

Section 1113 of the National Defense Authorization Act for FY 2010 (NDAA 2010), Public Law 111-84, effective October 28, 2009, repealed the statutory authority for NSPS. All employees and positions must be transitioned from NSPS by not later than January 1, 2012.

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 existing system (Remedy ARS) is being modified to include a personnel performance management and performance payout capability (Rating Workbench). To add this capability, a couple new forms that include several new data elements will be added to the data collected and stored on the Remedy server. The information includes: Individual's name; financial information (current base pay, proposed performance payout); employment information (supervisory assessment, performance rating, pay plan, pay band); Other ID number (a randomly generated personnel number for data matching and alignment on export). Most of the information within this form will be populated via an input file from DCPDS. Supervisors and Managers will then input employee ratings. Algorithms to properly implement performance business rules will be embedded within the form and will establish the employees new base pay and performance related bonus pay. The system will then export a data file that will be uploaded into DCPDS to affect base pay changes and performance payouts. This capability supports the implementation of the Alternative Personnel System (APS) at SPAWAR. This capability will not collect any information from the general public. The general public will not have access to this system.

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

Should this data be compromised, the risk is that SPAWAR employee Names, salaries, annual performance rating, and annual performance rating payouts would then also be compromised. This risk is considered low for the following reasons:
1. The system is currently protected and covered under an ATO.
2. System access is controlled both by CAC Sign-on and the assignment of roles by a system administrator. Access will only be provided to rating officials (Managers/Supervisors) and Managers' Administrative assistants
3. There are only 3 system administrators with overall access to data on the Remedy server.
4. The data is kept on the server in a secure area and will not be kept on removable media.
5. Compromise of the specific information collected/stored would only result in a low risk to employees.

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. SPAWAR echelon II & III personnel with an official need to know.

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service personnel and non-Navy military personnel with an official need to know.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

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

Remedy ARS - Rating Workbench does not collect personal information directly from the individual.

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.

Remedy ARS - Rating Workbench does not collect personal information directly from the individual.

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.	Remedy ARS - Rating Workbench does not collect personal information directly from the individual.

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.