PRIVACY IMPACT ASSESSMENT (PIA)

For the

Alternative Personnel System (APS)/Government Employee Management System (GEMS)
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

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 DoD

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.

SORN Authorities: 5 U.S.C. 301, Department Regulations; 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, 5 U.S.C. 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; and E.O. 9397 (SSN), as amended.

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 purpose of the system is to allow civilian employees and supervisors to create and maintain performance plans. The performance plan includes yearly objectives/performance goals entered by the employee and supervisor which is then used to determine the rating for salaries/bonuses at the end of the fiscal year. These plans are then used for rating and payout information at the end of the appraisal cycle. APS will get PII information (birth date, SSN, performance evaluation and performance objectives) from a Defense Civilian Personnel Data System (DCPDS) file, use that information to validate and match the user with their DCPDS information, and then use the SSN field (required by DCPDS) to send payout information back to DCPDS at the end of the appraisal cycle. The birth date is deleted once user validation occurs.

Personal information received from DCPDS and uploaded into the APS Performance Plan Tool:

a. PERSON_ID - [DCPDS] Employee ID
b. NAME - DCPDS Name; NAME_LAST - Last Name
c. NAME_FIRST - First Name
d. NAME_MIDDLE - Middle Name
e. TITLE - Position Title
f. UIC - UIC
g. ORG_CODE - specifies the full five alphanumeric characters of organization codes of SPAWARSYSCOM and associated PEOs.
h. SSN - 9 characters numeric; loads all 9 characters and is encrypted in the database
i. DATE_BIRTH - Birth Date; format: "yyyymmdd"; this field is deleted after the user connects to their record
j. DUTY_STATION - Geographic Locator Code
k. PAY_PLAN - Pay Plan
l. SERIES - Series
m. GRADE - Grade
n. SUPV_LEVEL - Supervisor Code; a value of "2" or "4" identifies the employee as a supervisor
o. PAYPOOL_ID - Pay Pool ID; format: 10 alphanumeric Pay Pool characters + "-" + up to 10 alphanumeric Sub Pay Pool characters)
p. APS ENTRY DATE - gives the date the employee started a job that is under the APS. If an employee transfers to another job that is covered under APS, this date will not change.
q. APS EXIT DATE - date (may be blank)
r. BASE PAY - current salary base pay
s. ADJUSTED BASE PAY - current salary adjusted base pay
t. LOCALITY PAY - current salary locality pay (may have a 0 value)
u. OTHER PAY - current salary other pay
v. TOTAL PAY - current salary total pay (sum of other pay values)
w. EMPLOYEE NUMBER - not used (NSPS identifier)
x. REGIONAL SERVICE CENTER - two characters (e.g., "SW", "NE")
y. LOCALITY AREA - three characters
z. PAY RATE DETERMINANT - one alphanumeric characters (e.g., "0", "J", "Y")
aa. DUTY STATUS - two characters (e.g., "00", "30")
bb. WORK SCHEDULE - one characters (e.g., "F")
cc. DATE PERSON ASSIGNED TO POSITION - not used
dd. DATE TEMP PROMOTION EXPIRES - date (may be blank)
ee. DATE LWOP EXPIRES - date (may be blank)
ff. DATE TEMP REASSIGN EXPIRES - date (may be blank)
gg. PERM PAY PLAN - not used
hh. PERM GRADE - not used

The DCPDS Continuing Payout File created in the Rating Payout Tool of APS includes the following data and is exported to DCPDS:
DCPDS EMP ID
Employee Name

UIC
Continuing Points
Continuing Point Value
Roll-over Amount
Effective Date
Salary Increase Amount
New Basic Salary
New Locality
New Adjusted Pay
New Other Pay
New Total Salary
Date Last Equivalent
SF 50 Remarks 1
SF50 Remarks 2
SF50 Remarks 3
SF50 Remarks 4
SF50 Remarks 5
SF50 Remarks 6 <Note to Developers: Must ensure PAY RATE DETERMINATE (Y,J,K) or Top of Band includes this Remark>
SF50 Remarks 7
SF50 Remarks <Note to Developers: Must ensure Successful with 1 Continuing Within Midpoint Results in this Remark Field Being Included>

DCPDS Bonus Payout File exported from the APS Rating Payout Tool input to DCPDS:

DCPDS Emp ID
Employee Name
UIC
Bonus Points*
Bonus Point Value
Bonus Amount
Effective Date
Rating of Record
Date Effective
Date Appr Period Ends
Org Struct ID
Pay Plan
Grade
SF50 Remarks 1
SF50 Remarks 2
SF50 Remarks 3

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

The DCPDS file will contain PII data, and this file will be uploaded for processing by an administrator. The uploaded file will be loaded directly into the database, so that it is never sitting in a server directory. Once processed, the file will be deleted.

The birth date and SSN will only be loaded into the database for employees who are new to APS. Once a new user is verified and matched to their DCPDS record, the birth date will be deleted from the database. The SSN field will be encrypted in the database. This PII data is NEVER displayed to any users on any screens but just resides in the database.

The administrator will generate the final payout file to send to DCPDS. This file will be encrypted when sent for processing into DCPDS.

The privacy risks need to be addressed here This is a standard statement that can be used
All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that SPAWAR APS, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.**

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. Human Resources Departments within SPAWAR

☒ **Other DoD Components.**

Specify. DoD and DON HR organizations

☐ **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.

The information is obtained from DCPDS. PII is not generated or collected for the first time by the use of this system.

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.

APS/GEMS information is not collected 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.

APS/GEMS information is not collected 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.