PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Warehouse Business Intelligence System (DWBIS)
Department of the Navy - SPAWAR (SSC Atlantic)

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: DITPR ID: 14950 DITPR DON ID: 22430
- ☐ **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 UII: 007-000004010

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 N05220-1

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 N05220-1 authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. Chapter 87, Defense Acquisition Workforce
DoD 5200.2-R, Department of Defense Personnel Security Program
DoDD 8570.1-M, Information Assurance Workforce Improvement Program
SECNAV M-5510.30, 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.

The Data Warehouse Business Intelligence System (DWBIS) is used to combine information from several different official sources to help the Command prioritize the staffing plans and assignments of almost 10,000 employees against the needs of the Navy and DoD to design, install and deploy Information Warfare systems. DWBIS is also used to manage available funds to ensure that certifications for Defense Acquisition Workforce and Cyber Security Workforce are kept at the level needed to support assigned missions.

PII in DWBIS will be shared with Government Supervisors and Managers (or their deputy authorized by the local Human Resources organization with a signed Nondisclosure Agreement), Command Training Officers and Personnel Officers responsible to supervise, manage or track employee qualifications and credentials such as: Contracting Officer's Representatives, Cyber Security Workforce, Defense Acquisition Workforce, Employees eligible for tuition reimbursement, and Billet Managers.

Integrated Product Team leaders receive a report listing the names of employees who have submitted charges to their project(s).

Supervisors or Managers can only view information related to the employees they are responsible for. SPAWAR Contractors, including those persons charged to maintain the system or who load the data and prepare management reports, must first sign a Nondisclosure Agreement before being given access to DWBIS.

PII collected: name, other names used, other id number, security clearance,
Employment information: Person's name, billet number, work mailing address, military rank or employee series and grade, clearance, date reported to command, work location, organizational code, organizational group,supervisor and their contact numbers, position title and pay plan, overseas tour begin and end date, number of years at current position or current tour end; Education information: Education information includes college degrees held and institutions attended, professional certifications held, plus college or professional courses applied for if under tuition reimbursement.
Job specific education includes:
Cyber Security Workforce membership and status including related credentials, certifications held, and expiration date of their certification; Contracting Officer's Representative status, training and certifications achieved, Defense Acquisition Workforce coursework planned or completed, position level and continuous learning points required to remain a member of that workforce; The following unique identifiers come from the source system(s) and are needed for computer matching:

- Navy ERP Unique Identifier Personnel Number (PERNR) for civilians,military and contractors, including names.
- Total Workforce Management Services (TWMS) System Unique Identifier for civilians, military and contractors, including names.
- Defense Civilian Personnel Data System (DCPDS) System Unique Identifier,Navy Position or Sequence Number and Billet Identification Number (BIN) for each civilian, including name.
- Total Force Manpower Management System (TFMMS) unique identifier and BIN for each civilian, including name.
- DoD Common Access Card Electronic Data Interchange Personal Identifier (DoD ID) Unique Identifier, including name.
- SPAWAR Directory Services (LDAP) Unique Identifier as a crosswalk to for the above, including name.

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

Risks:

Privacy risks to the individual associated with the collected PII are unauthorized access to the data or possible misuse of the data.

Safeguards:
The privacy risks associated with the PII collected by DWBIS include: computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., earthquake, fire, flood, etc.).

DWBIS data is strictly limited to support personnel who are legally authorized to receive that information (need to know). Access to the system is further limited to those individuals who have a defined need to access the information in the performance of their duties, and each individual access is controlled by role based privileges limiting their access to only that necessary for their job requirements.

All DWBIS users go through extensive background and employment investigations. System administrators are subject to more rigorous checks and must be certified members of the Cyber Security Workforce. Once these requirements and the need to know are met, the individual still needs a DoD issued Common Access Card to access the system.

All DWBIS users must complete training annually on the authorized use and proper handling of PII data.

DWBIS is an accredited system operating within a secure military facility. Physical access to the system is controlled by security personnel and access cards.

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 (see Section 2, question g. for specifics)

☐ **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. Cameron Bell Corporation (dba Government Solutions Group (GovSG)), Product Data Integration Technologies, Inc (dba Modulant), ATLAS Executive Consulting, LLC.

Support contractors must comply with all privacy protections under the Privacy Act when accessing PII. The following contract clauses are incorporated into the base contract or task order in accordance with DoN CIO Privacy Tip "Rules for Handling PII by DON Contractor Support Personnel" by the DON Privacy Team - Published, March 10, 2011: 52.224 - 1 - Privacy Act Notification, 52.224 - 2 - Privacy Act

☐ **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.

PII is not collected 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.

PII 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.	PII 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.