PRIVACY IMPACT ASSESSMENT (PIA)

For the

SYSTOC
DLA Installation Support

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 OPM/GOVT-10

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.

Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 33, and 63.

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.

SYSTOC is an electronic medical records system for use by the DLA Installation Support at Richmond Occupational Health Clinic. It is primarily used as for development and storage of electronic medical records, medical history and tracking to ensure compliance with annual medical surveillance requirements. Typical information contained in this system includes employee medical information related to occupational exposures and required occupational testing. The system will also store civilian information related to fitness for duty, workers' compensation examinations and treatment and physical exam findings related to the American's with Disabilities Act. On rare occasions, military service members may visit this clinic, and are referred to their appropriate treatment facility.

Personal Information collected include: Name, truncated social security number, date of birth, gender, military record information (if applicable).

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

Some privacy risks associated with PII collection were identified for SYSTOC: (1) unauthorized access (compromise of data resulting in identity theft would be critical as it would be a release of personal medical information, (2) unauthorized disclosure can result in identity theft or embarrassment.

Risk exposure of individual's private and personal information. The risks are minimized by physical, technical, and administrative controls. Data is available to only those whose job performances require access and is trained in privacy protection. System access is physically located in locked offices, controlled by use of smart cards, passwords, timed computer screen locks and role-based security which ensures access to the information in the system is limited by job requirement and authorization to view the data. Physical access to the system is restricted by the use of security guards and door locks and laptop locks.

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. DLA Installation Support Occupational Health Physician, Nurse and Medical Assistant.

☐ **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. Federal Staffing Resources contract (SP4703-08-C-0010) Section 7.1 Maintenance of

Medical Records: The contractor shall maintain all records under this contract in accordance with the Privacy act of 1974 and DLAR 5400.21. All records produced under this contract will remain the property of the Government.

☐ **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.

Individuals may object to the collection of their PII, however their objection would lead to the inability to perform the required work-related medical examinations. Typical medical examination required by law include the following: annual audiogram testing under 29 CFR 1910.95, Asbestos medical Surveillance under 29 CFR 1910.1101 and medical evaluation for respirator use under 29 CFR 1910.134.

(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.

Individuals may object to the collection of their PII, however their objection would lead to the inability to perform the required work-related medical examinations. Typical medical examination required by law include the following: annual audiogram testing under 29 CFR 1910.95, Asbestos medical Surveillance under 29 CFR 1910.1101 and medical evaluation for respirator use under 29 CFR 1910.134.

(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.	The individuals are provided a DD Form 2005 (Health Care Records), which contains a privacy act statement which states that the information collection is voluntary and the consequences of choosing not to participate in the information collection. The form is publicly posted at the DLA Installation Support Richmond Occupational Health Clinic and a signed form is kept with each individual's permanent medical file.

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.