PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Enterprise Workflow Support Capability (EWSC) - Directorate of Intelligence (DI)

2. DOD COMPONENT NAME:

Defense Logistics Agency

3. PIA APPROVAL DATE:

3/26/2018

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [x] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

EWSC is an Information System (I.S.) that provides DLA an Enterprise-Wide multi-tenant business process work-flow solution. EWSC is built upon a Commercial Off-The Shelf (COTS) product provided by RSA, LLC known as "RSA Archer." EWSC is comprised of two production instances housed in DLA's Ohio and California data-centers.

The purpose of the Directorate of Intelligence (DI) solution within EWSC (EWSC-DI) is to support DI Security Specialists in determining an individual's suitability, eligibility, or qualifications for federal civilian employment, federal contracts, or access to classified information. It will also assist with tracking insider threat information, security violations / infractions, employee foreign contact, and foreign travel.

In order to perform its mission, the EWSC-DI collects a variety of different types of PII (identified in Section 2), but only to the extent necessary to fulfill authorized activities. EWSC-DI is a stand-alone application within a multi-tenant environment with role based access controls managed through the Account Management Provisioning System (AMPS). All information input into the solution is done manually by authorized users and there is no information sharing, i.e., no data push or pull, between EWSC-DI and any other I.S.

*NOTE: While EWSC is an existing I.S., EWSC-DI represents a significant modification to the EWSC functionality. When EWSC-DI is fully operational, two existing GOTS applications (which contain PII) will be decommissioned: 1) Contractor Online Tracking System (COTS); and 2) Personnel Security (PERSEC).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

• Identification: Records are collected and maintained for the purpose of determining an individual's suitability, eligibility, or qualifications for federal civilian employment, federal contracts, or access to classified information.

• Mission-Related Use: Records are created and retained for mission-essential insider threat risk mitigation.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII data manually input by DI Security Specialists into the EWSC-DI originates from two (or more) sources, including:

1. DLA specific forms to process hiring actions such as DLA 1474 and DLAH 1728 which are provided directly from individual subjects.
2. From responses to official questionnaires, e.g., Standard Forms (SF) SF-85, SF-85PS, SF-86, SF-86A, and SF-86C. Responses to these official questionnaires are manually copied by DI Security Specialists into EWSC-DI.

The aforementioned questionnaires and forms contain Privacy Act Statements, allowing the individual to make an informed decision about providing the data. Individuals may elect not to provide the information requested, but the individual's suitability determination may be delayed or may not be completed. An individual may also contact the system managers specified in the applicable Privacy Act system of records notices (SORNs).

f. 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.

Once the individual completes the questionnaires or personal history statements, they have consented to the use of their information pursuant to the purposes specified in each of the applicable SORNs. No additional consent is requested for specific uses.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

The specific Privacy Act Warning and Privacy Act Statement within EWSC - DI is as follows:

"Privacy Act Warning
Information contained within this system is subject to the Privacy Act of 1974 (5 U.S.C. 552a, as amended). Only authorized personnel in the conduct of official business may use personal information contained within this system. Any unauthorized disclosure or misuse of personal information may result in criminal and/or civil penalties as well as administrative sanctions.

Any official or employee may be found guilty of a misdemeanor and fined not more than $5,000.00 if he or she willfully discloses personal information to anyone not authorized to receive the information.

Under the Privacy Act, an individual has a private right of action and Any individual may file a civil action against the Agency or its employees if the individual feels that certain provisions of the Privacy Act have not been complied with.

Would you like to proceed?"

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	PII data EWSC-DI may be shared with DI Security Specialists and as necessary, the DLA Anti-Terrorism (AT) Office and the DLA Counter-Intelligence (CI) Office. Whenever PII is shared by DI Security Specialists with another internal component (AT or CI), the information is limited to the subject individual and truncated / redacted to contain only the data necessary for the specific mission Function.
☒ Other DoD Components	Specify.	DoD Insider Threat Management and Analysis Center, DoD CAF
☒ Other Federal Agencies	Specify.	OPM or DoJ
☒ State and Local Agencies	Specify.	State, Local, Tribal Law Enforcement Agencies
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Peart-Hannon Consulting Group, LLC (3MCB0) 52.239-1 Privacy or Security Safeguards, 52.224-1 Privacy Act Notification, & 52.224-2 Privacy Act are included in the contract. Additionally contractor employees providing services are also required to sign Non-Disclosure Agreements (NDAs) outlining the non-release of information contained within the I.S.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☒ Other Federal Information Systems

PII data manually input by DI Security Specialists into the EWSC-DI originates from two (or more) sources, including:

1. DLA specific forms to process hiring actions such as DLA 1474 and DLAH 1728 which are provided directly from individual subjects.
2. From responses to official questionnaires, e.g., Standard Forms (SF) SF-85, SF-85PS, SF-86, SF-86A, and SF-86C. Responses to these official questionnaires are manually copied by DI Security Specialists into EWSC-DI.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [ ] Information Sharing - System to System
- [x] Other *(If Other, enter the information in the box below)*
- [x] Official Form *(Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [x] Website/E-Form

PII data manually input by DI Security Specialists into the EWSC-DI originates from two (or more) sources, including:

1. DLA specific forms to process hiring actions such as DLA 1474 and DLAH 1728 which are provided directly from individual subjects.
2. From responses to official questionnaires, e.g., Standard Forms (SF) SF-85, SF-85PS, SF-86, SF-86A, and SF-86C. Responses to these official questionnaires are manually copied by DI Security Specialists into EWSC-DI.

k. 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 must be consistent.

[x] Yes [ ] No

If "Yes," enter SORN System Identifier DLA S500.10, "Personnel Security Files,"

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 4.2, Item 30 (DAA-GRS-2016-0002-00002) & N1-361-91-7

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

• Record Series 5240.3: Personnel Security Clearance files are required to be destroyed two (2) years after last form entry, reply or submission; or when associated documents are declassified or destroyed; or when authorization expires, whichever is appropriate.

• Record Series 5240.19: Personnel Security Clearance files are required to be placed into an inactive status and retained for 2 years following subject employment and / or affiliation termination, after which they are to be destroyed.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; 44 U.S.C. 3554, Federal agency responsibilities; 44 U.S.C. 3557, National security systems; E.O. 10450, Security Requirements for Government Employment; Public Law 112-81, Section 922, National Defense Authorization Act for Fiscal Year 2012 (NDAA for FY12), Insider Threat Detection (10 U.S.C. 2224 note); Public Law 113-66, Section 907(c)(4)(H), (NDAA for FY14), Personnel security (10 U.S.C. 1564 note); Public Law 114-92, Section 1086 (NDAA for FY16), Reform and improvement of personnel security, insider threat detection and prevention, and physical security (10 U.S.C. 1564 note); E.O. 9397, as amended, Numbering System for Federal Accounts Relating to Individual Persons; E.O. 12829, as amended, National Industrial Security Program; E.O. 12958, Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; DoD Regulation 5200.2, DoD Personnel Security Program; and DoD Directive (DoDD) 5205.16, The DoD Insider Threat Program.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

- SF 86, SF 86C, and SF 86A: OMB No. 3206-0005
- SF 85: OMB No. 3206-0261
- SF 85PS: OMB No. 3206-0191