PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Document Access (EDA) System
Business Transformation Agency/DBSAE/PEO Sourcing

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: 418
- ☐ 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: 007-97-01-29-02-6576-00

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: T-1300

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.

31 U.S.C. Section 3325; DoD Financial Management Regulation, 7000.14-R, Vol. 5 Chapter 33 and Vol. 10 Chapter 17; E.O. 9397 (SSN) as amended 18 NOV 2008 by E.O. 13478.

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 Electronic Document Access (EDA) program is one of the Business Transformation Agency (BTA) Sourcing Environment programs. EDA supports the goals of the BTA to simplify and standardize the methods that DoD uses to interact with commercial and government suppliers in the acquisition of catalog, stock, as well as made-to-order and engineer-to-order goods and services initiatives to increase the application of Electronic Business/Electronic Commerce (EB/EC) across the Department of Defense (DoD). The EDA is a web-based system that provides secure online access, storage, and retrieval of contracts, contract modifications, Government Bills of Lading (GBLs), DFAS Transactions for Others (E110), vouchers, DD Forms 577, and Contract Deficiency Reports to authorized users throughout the DoD.
The Appointment/Termination Record, Authorized Signature, DD Form 577 information is used to determine whether an individual has held an accountable position in the past. To obtain data for the appointment or termination of deputies and the appointment or termination of other than finance officers as accountable officers.

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

The risk is identity theft. For EDA access is based on an authorized user account: granted by EDA POC approval and submission of 2875. For approved user account - role based access granted to user for access to DD577's by EDA POC based on job requirements. Data is transferred to EDA via Secure FTP and displayed within EDA using SSL and an encrypted token.

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.

☒ **Other DoD Components.**

Specify. All users with authorized EDA accounts whose EDA POC has granted them the DD577 role based on their job requirement needs. Authorized users can include all DoD Services and Agencies.

☐ **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.

Per the Privacy Act Statement appearing on the top of the DD577 form. Appointment as a certifying authority or accountable official is voluntary. An individual can decline the appointment by not signing the form.

(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.

Per the Privacy Act Statement appearing on the top for the DD577 form. The PII is collected to determine whether an individual has held a position as a certifying authority or accountable position in the past. The individual may decline the appointment by not signing the form DD577.

(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 Privacy Act Statement is printed at the top of the Appointment/Termination Record - Authorized Signature (DD577) Form:

PRIVACY ACT STATEMENT
AUTHORITY: E.O. 9397, 31 U.S.C. 3325, 3528, DoD Financial Management Regulation, Vol. 5, Chapter 33, and DoDD 7000.15, DoD
Accountable Officials and Certifying Officers.
PRINCIPAL PURPOSE(S): To maintain a record of certifying and accountable officers' appointments, and termination of those appointments.
The information will also be used for identification purposes associated with certification of documents and/or liability of public records and
funds.
ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U. S.C. 552a(b) of the Privacy Act of 1974,
as amended. It may also be disclosed outside of the Department of Defense (DoD) to the the Federal Reserve banks to verify authority of the
accountable individual to issue Treasury checks. In addition, other Federal, State and local government agencies, which have identified a need
to know, may obtain this information for the purpose(s) identified in the DoD Blanket Routine Uses published in the Federal Register.
DISCLOSURE: Voluntary; however, failure to provide the requested information may preclude appointment.

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.