



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Customer Relationship Management (CRM) Sales
and Business Objects (BO) -- Disposition Services

Defense Logistics Agency

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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

OMB NO: 0704-0382

Enter Expiration Date

January 31, 2016

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.

10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; 40 U.S.C. 101 et seq., Federal Property and Administrative Services Act of 1949, as amended; 50 U.S.C. App. 2401 et seq., Export Control; 41 CFR Part 101-45, Cross-Reference To The Federal Management Regulation (FMR) (41 CFR Chapter 102, Parts 102-1 Through 102-220); 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.

Information is collected and maintained for the purpose of registering bidders for DLA Disposition Services surplus sales. The information is also used to award contracts with successful bidders, perform Trade Security Control Clearance Assessments (using the DLA Form 1822, "End Use Certificate") and process financial transactions, such as payments and refunds. Information is imported into the Customer Relationship Management (CRM) Sales and Business Objects data base for the purpose of contract management and includes any or all of the following: Bidder Registration Number; Bidder Identification Number; Bidder Last Name; First Name; Middle Name; Company Name; Attention Line; Street Address; City; State; Zip; Province; Country; Mailing Address; Mailing City; Mailing State; Zip; Mailing Province; Mailing Country; Commercial Phone; Fax Number. The encrypted SSNs of the high bidders are stored in the CRM data base.

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

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 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 cipher and/or combination locks.

Records are maintained in secure, limited access, and monitored work area accessible only to authorized personnel. Central Processing Units are located in a physically controlled access area requiring either a badge or card swipe for entry. Passwords are tested for strength at the time of selection. Users are warned of the consequences of improperly accessing restricted databases and data misuse at each login, during staff meetings, and during separate Information Assurance and Privacy Act training. After hours, records are stored in locked file cabinets, locked rooms, or areas controlled by personnel screening. All file cabinets containing information subject to the Privacy Act of 1974 must have DLA Form 1461 affixed to the outside of the storage compartment. This form reads: The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable systems of records notice and 32 CFR part 323.

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.

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.

The DLA Disposition Services E-sales web form used to collect data contains a Privacy Act Statement as required by 5 U.S.C. 522a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection.

(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.

The DLA Disposition Services E-sales web form used to collect data contains a Privacy Act Statement as required by 5 U.S.C. 522a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection.

(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.

DLA Disposition Services E-sales website provides a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an Informed decision about providing the data or participating in the program.

When the high bidders are determined, they will complete a DLA Form (currently being developed) asking for their name and social security number. This DLA form also contains a Privacy Act Statement.

Information about high bidders is retained indefinitely in the system for the purposes of providing a cradle-to-grave record of the contracts and property purchases. Information is used routinely for investigative purposes (criminal, IG, GAO, compliance with Trade Security Control, etc), determining government indebtedness, hazardous material third party clean-up liability, and other litigation/legal matters that often occur years after the contract is closed out.

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.