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:

Contract Support System

2. DOD COMPONENT NAME:

3. PIA APPROVAL DATE:

Defense Information Systems Agency

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
- ☒ 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
- ☐ 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.

CSS uses Vendor and Mission Partner Point of Contact (POC) information to support contract actions. The Contracting Officers (KO) and Contract Specialists (CS) routinely reach out to vendors and mission partners during the development and execution of contract actions. The personal information includes names, titles, phone numbers, official mailing addresses and email addresses.

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)*

All data is for administrative use in order to contact individuals associated with the contract actions.
Vendor Business/Office and Mission Partner POC information, including email address and phone numbers, are used by KO/CS staff to contact vendors or mission partners for initiating, updating and completing contracting actions. Names, address and phone numbers are routinely included on official correspondence including letters, contracts, Request for Information, Request for Quotation and other contracting actions.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ 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.

Vendor POC data originates from the Central Contractor Registration (CCR), also known as SAM.gov. The vendors can object or refuse to provide the information in SAM.gov. The CCR data is manually inputted by PLD/DITCO into CSS because there is no interface between these systems. Data entered on federal customer POCs is gathered directly from the customer, and the CS manually enters the data into CSS. Federal customers can object and or refuse to provide information that is requested by the CS.

Additionally, vendors who register for access to the DITCO Solicitations and uploads site, enter their contact information on the registration page. Users can object to the collection of their data by not entering the requested information.

Vendor Business/Office Point of Contact (POC) information is intended for contracting purposes.
Federal Employee Business/Office Point of Contact (POC) information is intended for contracting purposes.

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.

Only occasionally, when a KO or CS is telephonically communicating with a vendor, can these individuals object to use of their data in this specific way. DITCO manually enters data found originally within the CCR into CSS. While vendors have self-entered information into CSS (via SAM.gov), they cannot consent to this particular use of their data (pulled from CRR and placed into CSS). However, in some cases, Federal customers can consent to provide information that is requested by the CS, or withhold consent when communicating with the CS.

Additionally, vendors who register for access to the DITCO Solicitations and uploads site, enter their contact information on the registration page. While users can consent to the collection of their data by entering the requested information or withhold consent by not entering the data; there is no opportunity to consent to this data being used/placed into CSS.

Vendor Business/Office Point of Contact (POC) information is intended for contracting purposes.
Federal Employee Business/Office Point of Contact (POC) information is intended for contracting purposes.

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

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.	Only within DISA
☐ Other DoD Components	Specify.	
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☐ 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.	
☐ 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

Central Contractor Registration (CCR) also known as SAM.gov (GSA system - hosted externally)
https://www.ditco.disa.mil/vendors/register.asp (DISA system - hosted at OKC)

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

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

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier K890.18

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 6.5, Item 20

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

(3) Retention Instructions.

Customer/client records. Temporary. Delete when superseded, obsolete, or when customer requests the agency to remove the records. (DAA-GRS2017-0002-0002)

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; Pub. L. 106-229, Electronic Signatures in Global and National Commerce Act,; Presidential Directive on Electronic Commerce, July 1, 1997; OASD(C3I) Policy Memorandum dated August 12, 2000, subject: Department of Defense (DoD) Public Key Infrastructure (PKI) and, OASD(C3I) Memorandum dated Jan 2001, subject: Common Access Card (CAC), and Government Paperwork Elimination Act.

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.

☐ 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.

OMB approval is not required in accordance with section 8.b.11 of Enclosure 3 of DoD Manual 8910.01.