PRIVACY IMPACT ASSESSMENT (PIA)

For the

VCE - VIRTUAL CONTRACTING ENTERPRISE
AMC - Army Contracting Command (AMC-ACC)

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: 10470 DA184945
- ☐ **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: Per APMS, this system stores PII but does "NOT" retrieve the PII

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.

10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance; and E.O. 9397 (SSN).

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 Virtual Contracting Enterprise (VCE) provides a standardized suite of Electronic and Web based tools utilized by Army Contracting Command's (ACC) employees and customers in acquiring goods and services for the Army. Only names, citizenship, clearance information, and job functions will be used to authenticate, authorize, and add users to processes entering into the Virtual Contracting Enterprise E-tool and Application tool suite. No information is released outside of the parent DoD component which is Army Contracting Command.

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

The risks are limited due to the limited nature of data collected. Data transmitted from system to system is encrypted and data at rest is also encrypted. Access to this data is limited to authorized personnel.

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. This information will only be utilized for Authentication, Authorization, and process management purposes within Army Contracting Command (ACC).

☐ **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. The Contractor is:
DATA SYSTEMS ANALYSTS, INC.
10300 EATON PL STE 500
FAIRFAX, VA 22030-2208

The following clauses are written in the contract to ensure safeguards are in place to

protect sensitive information:
6.1.1 Access to Government Data - The Contractor shall have access to procurement sensitive information to include contractors price and cost data, proprietary information related to Government contracting and source selections. As such, the contractor shall sign the Non Disclosure Agreement (NDA) to ensure this or any related information is not improperly disclosed. In addition each onsite employee and/ or those employees requiring access to ACC VCE applications shall sign the NDA.

6.1.3 Access to Sensitive Information - The contractor must abide by all personnel security requirements per AR 25-2, Para. 4-10, 4-14 and 4-15. Requirements vary depending on contractor role.

6.1.3.3 Roles/Privileges - The Contractor shall ensure that role/privileges assigned to Contractor employees on the Government platform and applications are limited to the role/privileges essential to that individuals performance of his/her assignment.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

In order to complete mission objectives users enter VCE portals to participate in work related acquisition processes.

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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

As part of the CAC authentication process users entering VCE portals need to do so in carrying out acquisition duties.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:
The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.