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:

Vendor Vetting and Arming Authorization, FCENTCOM 05

2. DOD COMPONENT NAME:

Defense Logistics Agency

and U.S. Central Command (USCENTCOM)

3. PIA APPROVAL DATE:

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
- [x] 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.

The purpose of the Joint Contingency Contracting System (JCCS) is to register and investigate vendors to verify their information and to evaluate them for trustworthiness to conduct business with the U.S military or access military installations. The purpose for Civilian Armed Authorization Management System (CAAMS) is to investigate vendor personnel to verify their information and evaluate them for trustworthiness to be authorized to carry firearms while acting as a contractor during performance of official duties on behalf of USCENTCOM. Information is collected from Department of Defense (DoD) and Federal agency civilian employees and North Atlantic Treaty Organization (NATO) personnel for the purpose of granting access to the system. Joint Contingency and Expeditionary Services (JCXS) is the agile, responsive, and global provider of joint expeditionary acquisition business solutions for the DoD that fulfills mission-critical requirements while supporting inter-agency collaboration and is comprised of JCCS and CAAMS, among others.

The following types of information is collected:

a. Name, Phone number, email address (JCCS/CAAMS)
b. Amount Contributed, % of shares, (JCCS)
c. Passport photo and number/National ID photo and number (JCCS)
d. Driver's License number, Passport number, or other Government issued ID number (CAAMS)
e. Financial Information (JCCS)
f. Social Security Number (CAAMS)
g. Criminal Record (CAAMS)
h. Business, Commerce, or Industry License photocopies (JCCS)
i. Arming Eligibility and Status (CAAMS)
j. Service/Rank, Duty Location (CAAMS/JCCS)

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)*

Mission Use:
JCCS is collecting the selected PII to provide a secure vendor repository for U.S. Government contract awards. CAAMS is collecting the selected PII to provide a document verification and repository for Exception to Policy contractor arming requests. All data is owned by USCENTCOM. JCCS and CAAMS operate under ATO as part of the DLA JCXS platform that is hosted at the DISA DECC Ogden site.

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.

Disclosure of the PII and other requested information is voluntary to support the registration and vetting process; however, failure to provide the required information could cause delay or cause that individual denied access to do business with the U.S Government.

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.

Individuals can give or withhold information to which they choose to input in JCCS, knowing that the consequence of withholding information may result in the inability to conduct business with the U.S Government. Contractors in CAAMS can withhold sharing their information with the hiring company prior to it's input in the system; individuals without required documents/information may result in the inability to conduct business with the U.S Government.

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

Authority: Section 822 of Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020", December 20, 2020; Section 872 of Public Law 115-232, "National Defense Authorization Act for Fiscal Year 2019", August 13, 2018; Sections 841-843 of Public Law 113-291, "National Defense Authorization Act for Fiscal Year 2019", December 19, 2014; DoD DTM 18-003, "Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records", April 9, 2018; USCENTCOM EXORD on Designation of Vendor Vetting Responsibilities in the USCENTCOM Theater Area of Operation, November 3, 2017; USCENTCOM EXORD on Designation of Vendor Vetting Responsibilities in the USCENTCOM Theater Area of Operation, MOD 01, July 10, 2019.Sections 841 to 843 of Public Law 113-291, "National Defense Authorization Act for Fiscal Year 2015", December 19, 2014.

Purposes: The purpose of the Joint Contingency Contracting System (JCCS) is to register and investigate vendors to verify their information and to evaluate them for trustworthiness to conduct business with the U.S military or access military installations. The purpose for Civilian Armed Authorization Management System (CAAMS) is to investigate vendor personnel to verify their information and evaluate them for trustworthiness to be authorized to carry firearms while acting as a contractor during performance of official duties on behalf of USCENTCOM. Information is collected from Department of Defense (DoD) and Federal agency civilian employees and North Atlantic Treaty Organization (NATO) personnel for the purpose of granting access to the system.

Routine Uses: Federal Intelligence and Law Enforcement agencies and to NATO to determine when a contractor or subcontractor is suspected or confirmed to pose a security risk or to determine or confirmed to be affiliated with bad actors including, but not limited to individuals involved in other criminal or human rights violations.

Disclosure: failure to provide the requested information could result in a user not being allowed to use the application, which would prevent being considered for U.S. contracts or weapon support.

Rules of Use: Rules of Use: Information is safeguarded in accordance with applicable laws, rules, and policies. Access is limited to those officers and employees of the agency who have an official need for access in order to perform their duties. Full details are available in the CENTCOM System of Records Notice, FCENTCOM 05, "Vendor Vetting and Arming Authorization," (pending publication in the Federal Register). URL to be provided upon publication.

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.	The only persons with access to data are vetted JCXS Administrators, Government Contracting Officers, and Government Reviewers. Vendors can only see the data that they enter themselves (JCCS).
☒ Other DoD Components	Specify.	USCENTCOM
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	

[X] 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.	Per existing contract with Celerity Solutions LLC, Section 2.6, Performance Requirements, "Every Contractor employee (including those of sub-contracts) is required to obtain an identification card badge (ID Card) / Common Access Card (CAC)/ prior to starting work on this contract. The Contractor will submit a completed DLAH 1728 and DD FORM 2875." (The 2875 requires privacy training before a system can be accessed and thereafter annually.) FAR privacy clauses are being added to the contract 5/15/20.
[X] Other *(e.g., commercial providers, colleges)*.	Specify.	Vendors are able to see information on hired contractors that they added into the system themselves (CAAMS).

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

- [X] Individuals
- [ ] Databases
- [ ] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

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

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

For JCCS, information is collected from the vendor requesting to be vetted. For CAAMS, information is collected using the DD 2760.

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 FCENTCOM 05

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.

The SORN will be submitted for approval to DPCLTD June 29, 2020

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. CJCSM 5760.01a, Records Retention, vol 2

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

(3) Retention Instructions.

CJCSM 5760.01A, V. 2: 0600-03.A General Logistics Records for normal information maintained in the system. Destroy/delete no less than 7 years and no more than 10 years after cutoff of calendar year. 0400-06.F Correspondence, memorandums, and other records relating to codes of ethics and standards of conduct for information where vendors were denied access in JCCS or an Arming Authorization was revoked for a CAAMS contractor. Cut off on completion of final action, hold 50 years, then destroy/delete. Earlier destruction is

authorized for routine materials not needed for legal purposes.

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.

Authority: Section 822 of Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020", December 20, 2020; Section 872 of Public Law 115-232, "National Defense Authorization Act for Fiscal Year 2019", August 13, 2018; Sections 841-843 of Public Law 113-291, "National Defense Authorization Act for Fiscal Year 2019", December 19, 2014; DoD DTM 18-003, "Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records", April 9, 2018; USCENTCOM EXORD on Designation of Vendor Vetting Responsibilities in the USCENTCOM Theater Area of Operation, November 3, 2017; USCENTCOM EXORD on Designation of Vendor Vetting Responsibilities in the USCENTCOM Theater Area of Operation, MOD 01, July 10, 2019.Sections 841 to 843 of Public Law 113-291, "National Defense Authorization Act for Fiscal Year 2015", December 19, 2014.

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 Collection OMB Control Number 0704-0589,
effective 1/28/2020, Expiration date 1/31/2023