SUPPORTING STATEMENT – PART A

Joint Contingency and Expeditionary Services (JCXS) —2015-32809

A. Justification

1. Need for the Information Collection

As per RS HQ Vendor Vetting FRAGO 215-2015 Vendor Vetting Process and USFOR-A FRAGO 14-165 (MOD 2) Directs Sub Units to Adhere to Vendor Vetting Process, all companies/vendors operating within CENTCOM are to be registered in the Joint Contingency Contracting System (JCCS).

Para 3 (2) (a) of RS HQ Vendor Vetting FRAGO 215-2015 Vendor Vetting Process states "registering in JCCS means the vendor/contractor and all sub-contractors have created a profile in JCCS, provided all required information and submitted all required documents. Contracting Officers must ensure all vendors have a sufficient JCCS registration prior to submitting a vetting request"

In accordance with DoD instruction “RS HQ Vendor Vetting FRAGO 215-2015 Vendor Vetting Process and USFOR-A FRAGO 14-165 (MOD 2)” and other appropriate policy and regulations, the information collection requirement is necessary to evaluate vendors for possible approval and acceptance to conduct business, access to U.S military installations, and adherence to US regulatory mandates. The Joint Contingency and Expeditionary Services (JCXS) family of systems is the DoD’s agile, responsive, and global provider of Joint expeditionary acquisition business solutions that fulfill mission-critical requirements while supporting interagency collaboration – to include, but not limited to, contracting, exception to policy arming of contractors, financial support, spending analysis, contract close-outs, staffing, strategic sourcing, and reporting.

The Joint Contingency Contracting System (JCCS) is a web-based service that sits on the JCXS platform, designed to, and currently used to register foreign vendors for Installation Access Eligibility. These vendors must provide company and banking information as well as appropriate identification documents in order to have the opportunity to conduct such business. If the vendor does not provide the requested information, then proper verification of credentials and a security review cannot be completed properly. It is of national security interest for the US to maintain force protection for our US forces and coalition partners. Vendor evaluation is paramount to achieving this objective.

In accordance with DoD instruction “USFOR-A FRAGO 16-143 MOD 1 Arming Procedures for DoD Contractors” the Armed Contractor Oversight Directorate (ACOD) will “coordinate with

DRAFT

contracting agencies, vendors, and their representatives to facilitate the arming authorization process via the web-based Civilian Arming Authorization Management System (CAAMS)". Per the instruction, a Synchronized Pre-Deployment and Operational Tracker (SPOT) employment Letter of Authorization (LOA), DD Form 2760, Law of Armed Conflict/Rules for the Use of Force Training Certification, Acknowledgement of Training, Weapons Qualifications, and a Background Investigation, must accompany all exception to policy (ETP) contractor requests.

The Civilian Arming Authorization Management System (CAAMS) provides a standardized and automated process for the submission, review, approval, and compliance management of the contractor arming process. Moreover, the application provides both visibility and audibility to capture and report current and potential Contractors' arming information, location, and arming compliance. Most importantly, U.S. Forces and coalition partners, civilians, and contractors could potentially face force protection risks posed by nefarious actors; hence CAAMS is an integral part of the National Defense Security operation.

Both web applications are part of the Joint Contingency and Expeditionary Services (JCXS) Portfolio.

DRAFT

Table 1: Collection Authorities

Attachment	Document	Authority	Issuing Authority	Description
1	DTM	Executive	US Government	Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records
2	NDAA, Sec. 841	Legislative	US Government	Prohibition on Providing Funds to the Enemy
NA	FRAGO T-CFLCC 100550Z	DoD	CENTCOM	Classified; Supports Vendor Vetting
NA	JCXS ATO#	J61	US Government	Sensitive; Authorization for JCXS to Operate
3	FRAGO 16-143 MOD-1	DoD	CENTCOM	Arming ETP Contractors

2. Use of the Information

In accordance with appropriate acquisition policy and regulations, any contractor that wants to conduct business with or on U.S Government/Military installations must be registered

through JCXS. Contractors/vendors, the respondents, shall input all company, personal, and employee data into the respective JCXS website (JCCS and/or CAAMS) to enable the U.S Government to ensure the safety of U.S. personnel in theater, and ensure the U.S. Government is not contracting with any enemy entities or potential threats. Prime contractors and their subcontractors are responsible for ensuring the database contains up-to-date, real-time information regarding their identity, employment, finances, affiliations, and other associated documentation.

JCCS is one of the proven acquisition solutions that supports the Procure-to-Pay lifecycle for vendors involved in contingency and expeditionary operations. Through many contracting office correspondences via email, social media, DoD or Federal websites, or by word of mouth by repeat customers, the JCCS solution is known as an integral part of the U.S. contract award process. Hence, the JCCS collection process is entrenched in the battle rhythm as a trusted repository for vendors. Moreover, the capability was designed to give vendors the option to view the website in their native language via Google Translate. This feature supports the various registration requirements and facilitates an awareness of usage in the vendor community. In the event that a vendor has questions, concerns, and/or issues due to language barriers, the application promptly displays a help desk icon on each webpage for users to access real time support or a written response from the respective site administrators.

The JCXS PMO also has customer support staff that operates during their given time zones and has an onsite resource embedded in various contracting offices to provide immediate assistance. By leveraging the commonly-used internet access process, the user inputs the URL to the secure hosted, 508 compliant JCXS website (https:www.jccs.gov). The vendor is automatically prompted to agree to DOD IA policies and procedures as well as the present and future privacy disclosures.

By navigating through a user-friendly graphical user interface (GUI), the users are prompted to input information thru various formats of drop down lists, radio buttons, pick-lists etc. The users receive visual notification via red asterisks *-if information is missing or not formatted correctly, as well as on screen notifications during the various process stages of approval. Both JCCS and CAAMS have email notifications for various communications. Please see screenshots that details the complete end to end collection experience.

The information collected is required to maintain the safety of contractors and U.S. armed forces while ensuring the U.S. Government is not doing business with entities at odds with U.S. interests.

3. Use of Information Technology

DRAFT

The use of information technology has been considered appropriate for the purposes of this collection. The Vendors have the ability to input the required information into JCCS and CAAMS, which are secured, web-based systems that the contractors can easily access with the correct right to use. The percentage of annual respondents that complete and submit the collection electronically is 100%. This is due to the data completion in a web based-HTML format.

4. Non-duplication

As part of the JCXS platform, JCCS collects information from foreign vendors looking to do business with the U.S. Government OCONUS. The data from SAM (System for Award Management) can be used to pull company information also required by JCCS. What differentiates JCCS from SAM is that SAM can be used to pull U.S. company information while JCCS is able to distinguish foreign vendors from U.S. vendors. Additional data required for contingency operations including financial information (shareholder information), company ownership information, contracts held with the U.S. Government, subcontractor information, and employee information are not collected by SAM. JCCS is used to collect this data set.

There are no known systems used to process ETP contractors' arming requests.

5. Burden on Small Business

The information collection associated with small businesses is the minimum consistent with applicable laws, Executive orders, regulations, and other prudent business practices.

6. Less Frequent Collection

Information is necessary to be collected annually based on license expirations and other base access requirements

Information is necessary to be collected on occasion due to any base access requirement records that may have changed for the company since the original/annual collection.

Information is necessary to be collected on occasion due to any new contractor request to carry arms.

7. Paperwork Reduction Act Guidelines

There are no special circumstances that require the collection to be conducted in a manner inconsistent with the guidelines in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

DRAFT

Part A: PUBLIC NOTICE

The 60-Day Notice for this proposed information collection was published in the Federal Register on Wednesday, December 30, 2015. The 60-Day Notice can be found at 80 FR 81531.The JCXS PMO received One (1) comment by phone asking for clarification of how the data would be collected. The response provided is that data will be collected by web-based form. No comments were received via the Federal Register website.

Part B: CONSULTATION

The JCXS system is DIACAP certified having been subjected to and passed thorough security testing and evaluation by independent parties. Consultation takes place through a documented governance process with key stakeholders where the collection is reviewed as required. The information being requested is ordered from an outside sponsoring agency that regulates what information is collected and how frequently it is collected. JCXS does not consult with respondents regarding information posted via the website but rather directs them to the sponsoring agency. Respondents have full access to the JCXS Helpdesk via JCXS webpage for assistance and clarity of the website.

9. Gifts or Payment

There is not any payments or gift provided to respondents, other than remuneration of contractors under their contracts

10. Confidentiality

To meet safeguards specified by the Privacy Act of 1974, JCXS displays a consent message upon accessing the portal (Appendix A) and a Privacy Statement on the Vendor log-in page (Appendix B).

Our need for a PAS, PIA, and SORN is due to Force Protection; A vetting cell uses the sensitive information (bank information) collected on vendors in JCCS to investigate whether or not the USG will allow these companies to do business with the U.S. Government OCONUS. The Armed Contractor Oversight Directorate (ACOD) uses the sensitive information collected on contractors in CAAMS to verify the identity and necessity of the request to provide a recommendation to bear arms. Without this information, investigations would not be as thorough and in turn, would put our forces at more risk.

JCXS follows the guidelines for storing, maintaining, and disseminating collected data presented in the DLA Records Schedule-8500 Information Security (Appendix C).

See attached for a draft copy of the JCXS SORN.

DRAFT

11. Sensitive Questions

Sensitive information collected by JCXS applications include Individual Names, Family information, Company Name and Address, Employee Information (Name, Parents, Phone Number, e-mail address), Company Financial Information, data from/images of Documentation (Passport/Identification Document, Industry Licenses), and Tribe Information.

Vetting cells use the financial information from JCCS collectively to follow money trails of the vendors and ensure funds are not being used to fund terrorist activities. The exact reasons and specific uses or vetting procedures of the collected information are classified and unknown to the system administrators. ACOD collects the information to verify identification, completion of training, and arming request justification.

12. Respondent Burden, and its Labor Costs

Estimation of Respondent Burden Hours					
	Number of Respondents	Number of Responses per Respondent	Number of Total Annual Responses	Response Time (Amount of time needed to complete the collection instrument)	Respondent Burden Hours (Total Annual Responses multiplied by Response Time) Please compute these into hours)
JCCS	4000	1	4000	0.5 hours, (30 minutes)	2000 hours
CAAMS	1500	1	1500	.5 hours (30 minutes)	750 hours
Total	5500	2	4000	1 hour (60 minutes)	2750 hours

13. Respondent Costs Other Than Burden Hour Costs

14. Cost to the Federal Government

	Joint Contingency Contracting System (JCCS)	Civilian Arming Authorization Management System (CAAMS)	Total
Number of Responses	4000	1500	5500

DRAFT

Processing Time Per Response (in hours)	.25	.25	.5
Hourly Wage of Worker(s) Processing Responses	21*	21*	$42
Cost to Process Each Response (Processing Time Per Response multiplied by Hourly Wage of Worker(s) Processing Responses)	5.25	5.25	$10.50
Total Cost to Process Responses (Cost to Process Each Response multiplied by Number of Responses	21,000	7,875	$28,875

*GS-7 pay grade used for Hourly Wage from OPM 2016 Pay & Leave schedule

Operational and Maintenance Costs						
Equipment	Printing	Postage	Software Purchases	Licensing Costs	Other	Total
0	0	0	0	0	0	0

Total Cost to the Federal Government		
Operational and Maintenance Costs	Labor Cost to the Federal Government	Total Cost (O&M Costs + Labor Cost)
0	$25,000	$25,000

DRAFT

15. Reasons for Change in Burden
    The burden listed above includes the burden of respondents and responses from all of the JCXS applications.

16. Publication of Results
    The information collected shall not be tabulated or published.

17. Non-Display of OMB Expiration Date

    The JCXS submission is not requesting an approval for avoiding display of the expiration date for OMB approval of the information collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

There are no exceptions to the certification accompanying this Paperwork Reduction Act submission.

DRAFT

APPENDIX

Appendix A: Consent to Monitor

You are accessing a US 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 purposed 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 measure (e.g., authentication and access controls) to protect USG interest—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.

Appendix B: Privacy Statement

Authority: T-CFLCC 100550Z, USARCENTCFLCC 240400Z, AFRICOM OPORD 16-001 , ACI 4800.07

Principal Purpose(s): The investigate vendors for installation access eligibility. Records may be used as a management tool for statistical analysis, tracking, reporting, and evaluating program effectiveness and conducting research. However, if you indicate you may represent a threat to self or others, you will be reported to the appropriate authorities in accordance with DoD/military branch of service and component regulations and established protocols.

Routine Use(s): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records may be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To authorized DoD military occupational specialty contractors for the purpose of responding to service member or family member need. To contractors and grantees for the purpose of supporting research studies concerned with the effectiveness of non-medical counseling interventions. To local law enforcement entities for the purpose of intervention to prevent harm to the individual (self) in accordance with DoD/military branch of service and component regulations and established protocols. Any release of information contained in this system of records outside the DoD under a routine use will be compatible with the purpose(s) for which the information is collected and maintained. The DoD

DRAFT

Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense compilation of systems or records notices may apply to this system.

Disclosure: Voluntary; however, failure to provide this information will result in an inability to access US Government Installations to perform contract work.

Appendix C: DLA Records Schedule

DLA RECORDS SCHEDULE – 8500
INFORMATION SECURITY

This Schedule relates to implementation of DoD, Federal Government, and NIST issuances in ADP security, communications network security, and emanations security. Includes records relating to the administration and implementation of ADP and Communications Security policies, plans, programs, procedures and systems, ADP security risk management, accreditation, certification, and security programs.

SCHEDULE: 8500
INFORMATION SECURITY

	A		B	C
Rule	**Record Series Title and Description**		**Disposition Instruction (Include Cutoff Instructions)**	**Disposition Authority**
1	**ADP Security Arrangements**. Documents relating to arrangements to provide DLA activities with ADP security facilities and countermeasures. Supersedes DLA record series: 151.05		**Temporary.** *Destroy when superseded, obsolete or no longer needed for reference*	N1-361-91-7
2	**System Access Records.** These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: • User profiles • Log-in files • Password files • Audit trail files and extracts • System usage files • Cost-back files used to assess charges for system use • System Authorization Access Requests (SAARS/DD 2875 Forms) • Appointment/Termination Files (DD Form 577) Exclusion 1. Excludes records relating to electronic signatures Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement Supersedes DLA record series: 110.75, 151.07, 151.09, 151.09A and 151.09B (GRS 24, Item 6a, N1-361-96-1, GRS 20, Item 1c)	**Systems requiring special accountability for access.** These are user identification records associated with systems which are highly sensitive and potentially vulnerable (i.e., systems containing information that may be needed for audit or investigative purposes, and those that contain classified records) (i.e., DD Form 577)	**Temporary. Cutoff at end of Event.** *Destroy 6 years after password is altered or user account is terminated.*	GRS 3.2, Item 031 (DAA-GRS-2013-0006-0004)
2.01		**Systems not requiring special accountability for access.** (i.e., DD Form 2875)	**Temporary. Cutoff at end of Event.** *Destroy 1 year after user's account is terminated from the system or when no longer needed for administrative, legal, audit or other operational purpose, whichever is later.*	GRS 3.2, Item 030, (DAA-GRS-2013-0006-0003)