DEPARTMENT OF THE AIR FORCE
UNITED STATES AIR FORCES CENTRAL COMMAND (AFCENT)
AL UDEID AIR BASE, QATAR

MEMORANDUM FOR USAFCENT/DAA

FROM: USAFCENT/A6OI

SUBJ: Approval to Operate for Joint Contingency Contracting System 3.7.x (JCCS) on the USAFCENT NIPRNet Enterprise

1. In accordance with CCR 25-206, Network Operations, I recommend the USAFCENT DAA approve the connection and operation of JCCS 3.7.x on USAFCENT Enterprise NIPRNet and issue an AtO with an ATD of 14 May 2012. This AtO shall be granted for purpose of system development and installation onto the USAFCENT NIPRNet Enterprise.

2. Overview: JCCS allows contracting officers and enterprise management leaders a complete look at the contracting process from receipt of a purchase request to the final contract payment and close out actions. These system capabilities dramatically reduce required contract planning times, allowing for a level of customer support in a contingency contracting environment. The contracting system stores information about all registered and approved host nation vendors.

3. The USAFCENT NOSC Information Assurance section reviewed available documentation and verified that sufficient system security countermeasures have been implemented and an acceptable level of protection exists. See attachment 1.

4. A signed copy of this AtO shall be posted on the USAFCENT Commander's Dashboard on SIPRNet to inform the Network Control Centers JCCS is authorized as specified above.

5. The assigned Information Assurance Officer at each USAFCENT site is required to follow DAA and NOSC provided guidance throughout the life cycle of the system. Changes to the current configuration of JCCS may nullify this approval.

6. The DAA POC is the USAFCENT NOSC, DSN 965-1488.

MICHAEL J. HARTZELL, YD-02, SPAWAR
USAFCENT Information Assurance Manager

Attachment:
Review and Risk Summary Checklist

1st Ind, USAFCENT/DAA

MEMORANDUM FOR USAFCENT/A6OI

Approve/Disapprove the use of Joint Contingency Contracting System (JCCS) 3.7.x on the USAFCENT NIPRNet with an ATD of 14 May 2012.

HARRY H. BLANKE III, Colonel, USAF
Designated Approving Authority

Review and Risk Summary for: Joint Contingency Contracting System 3.7.x (JCCS)

PMO Information	
Mitigating Factors:	

Review Checklist:

1. Desktop Review	**Yes**	**No**	**N/A**	**Comments**
1.1 Will the requested application be deployed on a non-STIG compliant server environment?		N		**If yes, explain the architecture the product will be used on and reason for deviation**
1.2 Does the application process, produce, or store sensitive data (e.g. Classified, Privacy Act, HIPAA…)?		Y		**Data is protected via inherited encryption and layered defense**
1.3 Is the application developed/controlled by a foreign country?		N		
1.4 Is the application vendor listed under the "Excluded Parties List"?		N		**http://www.epls.gov**
1.5 Are there any minimum hardware/software requirements for the application (e.g., OS version, RAM, storage space, etc.)?			?	**If yes, list SW/HWrequirements. (on file at NOSC IA P&R)**
1.6 Does it require a network connection to operate (e. g., auto-updates, help files, interface with other systems)?		N		**If yes, identify ports** (Not required, but may be used online)
1.7 Are administrator rights required to install application?	Y			
1.8 Are there any known vulnerabilities for the application (NVD and Security Focus check)?		N		**http://cve.mitre.org/cve/index.html**
1.9 Does application employ use of mobile code technology?	Y			**Use of mobile code must comply with the requirements of DoDI 8552.01. (on file at NOSC IA)**
1.13 System will receive security patches via AFCENT approved method?	Y			
1.14 System will receive virus signature updates via AFCENT approved method?	Y			
1.15 Is the system compatible with the current SDC?	Y			**https://afeemo.gunter.af.mil/ApplicationCompatibility/default.aspx**