**Performance Work Statement (PWS) Engineering Support**

**For Small Unmanned Aircraft Systems (SUAS)**

**Sample Task Order (TO): W911QY-19-R-SUAS-ENG**

**08 November 2019**

**Scope**

This PWS describes the full spectrum of Technical, Management, and Engineering support the Contractor will provide to support the Product Manager (PdM) Small Unmanned Aircraft Systems (SUAS) and its customers under this Task Order (TO).

## Objectives

The Small Unmanned Aircraft Systems (SUAS) Product Office (PdO)—a product office within Project Manager for Unmanned Aircraft Systems (PM UAS)—has a need for continued systems and sustainment engineering support to the SUAS requirements, operations, and capabilities. These system requirements will be defined and/or executed through the Short Range Reconnaissance (SRR) Air Vehicle (AV), the Medium Range Reconnaissance (MRR) AV, the Long Range Reconnaissance (LRR) AV, and the Handheld Ground Control System (H-GCS). The RQ-11B Raven and RQ-20A Puma AVs currently execute the respective MRR and LRR SUAS AV roles with an Original Equipment Manufacturer (OEM) Commercial Off-The-Shelf (COTS) H-GCS. Additionally, PdM SUAS will integrate modifications to the MRR Flight Control System (FCS), the H-GCS, and the Digital Data Link (DDL) radio to operate in a new frequency spectrum. Future SUAS LRR and SRR AVs will also require Tactical Open Government-owned Architecture (TOGA) H-GCS systems and sustainment engineering integration and requirements assessments during the handheld ground control prototype production phase to validate requirements, demonstrate interoperability, and long-term supportability.

The MRR FCS is a modification of the RQ-11B avionics suite and other RQ-11B components. The updated RQ-11B Raven system will be re-designated RQ-11C and will meet or exceed the performance of the currently fielded systems. The systems and sustainment engineering of the final FCS solution and integration may be required during this contract period and will comply with spectrum reallocation mandates.

Additionally, the current Ground Control Station (GCS), Hub, Hand Controller, and Reconnaissance, Surveillance, and Target Acquisition (RSTA) Laptop will be replaced with the TOGA H-GCS to allow the H-GCS to perform the following:

1. Connect by cable to a radio frequency head unit (i.e., ten-feet and 50-feet versions)
2. Connect to various external power sources
3. Connect to a Selective Availability Anti-Spoofing Module (SAASM) key-fill device
4. Connect via USB to an external disc drive
5. Connect H-GCS to H-GCS via master / slave cable
6. Be transported in a rugged carrying case
7. Be trained via Operator’s Manual
8. Be repaired via Repair Manuals

The aforementioned products are expected to be developed and integrated concurrently by the PdM. All system and sustainment engineering and related products are expected to be executed within this TO.

**General Information**

The Department of Defense (DoD) has developed a new cybersecurity standard and certification for DoD Contractors. It is named, “Cybersecurity Maturity Model Certification (CMMC)”. The intent of the CMMC is to improve cybersecurity deficiencies in the defense industrial base and secure the supply chain. The final standard for CMMC is expected by 2QFY20.

**Applicable Documents**

All top-level documents are listed in the Document Summary List (DSL) by number, title, and date. The document versions specified on the DSL take precedence over the generic references cited in this TO.

The following documents also apply to this TO:

* + - Capability Production Document for (U) Rucksack Portable Unmanned Aircraft System (RPUAS) Increment 2, Version 1.04, 23 November 2013
    - Shadow / Raven Unmanned Aerial System Validated On-Line Lifecycle Threat (VOLT) Report, Information Cut-off Date: 31 January 2019, Validation Memorandum: 18 March 2019 (Contractor required to access this S//NF document to assess “threat environment” and incorporate threat-related requirements into performance specifications)
    - System Specification Raven SUAV-0002, Revision B, 02 May 2016
    - SUAS Puma AE with Digital Data Link Operator’s Manual, 62869\_A, June 2011
    - Waveform Specification for SUAS Digital Data Link (DDL) Version 1.5,  
      24 February 2010
    - SUAS Specification Tree (see Figure 2-1)
    - TOGA H-GCS Level 3 Technical Data Package (TDP)
    - Draft TOGA H-GCS Subsystem Specifications for Hardware and Software,  
      30 October 2019
    - Family of Small Unmanned Aircraft Systems Security Classification Guide,  
      22 November 2017

**Requirements**

This section covers requirements for the system as a whole; however, the following sub-sections will contain component specific and functionally specific variations on what is required for this task. All Contract Data Requirements List (CDRL) references are contained in contract W911QY-13-DXXXX. The Contractor shall manage all integrated solution specification requirements updates to the current RQ-11B Raven and the follow on RQ-11C Raven for operation in conjunction with the TOGA H-GCS. The Contractor shall also provide the supporting test plans and reports for the updated system and develop / track an Integrated Master Schedule (IMS) of the Spectrum Reallocation events defined throughout this PWS. The Contractor shall support developmental and operational testing and support Government environmental lab testing to demonstrate that the proposed solutions meet the full functionality and reliability required In Accordance With (IAW) the SUAS specification documents.

**Project Management**

The Contractor shall conduct a kickoff meeting approximately two weeks after TO award. At the kickoff meeting, the Contractor shall provide an IMS that outlines this TO IAW CDRL A033. The IMS shall include, if required, the Government’s delivery of multiple Software (SW) and Hardware (HW) releases to the Contractor (i.e., data to be delivered as Government-Furnished Property (GFP)), validation phases for each SW and HW release, CDRL completion, additional FCS integration efforts, and other items deemed as necessary milestones based on GFP related to the FCS/DDL and TOGA H-GCS contracts. The IMS shall include planned updates to the RPUAS Family of Systems (FoS) specification documents, and estimated durations required to: evaluate Sprint SW releases, conduct HW tests for major HW revision releases, develop test procedures required and conduct flight testing of the MRR and LRR with TOGA H-GCS.

The Contractor shall develop and present a Systems Requirements Review (SRR) at the kickoff meeting a system review of the program to demonstrate an understanding of the contracted TO. In addition, the Contractor shall implement biweekly Integrated Product Team (IPT) meetings to cover completed, current, and future tasks as well as schedule / cost data associated with this PWS. The Contractor shall prepare and host an Interim Program Review (IPR). The IPR shall, as a minimum, consist of a review of the IMS, funding expenditure (i.e., both executed and planned), Problem Change Reports (PCRs), specifications completion report, test results, and planned activities for the remainder of the contract. Provide slides IAW CDRL A009.

The Contractor shall as required participate in IPTs with the FCS and TOGA H-GCS development vendors to support on-going development of RPUAS FoS specifications, Hardware-In-the-Loop (HWIL), test results, Interface Control Document (ICD) descriptions, and other items necessary to finalize the RPUAS FoS requirements for the FCS and TOGA H-GCS solutions.

**Systems and Sustainment Engineering and Requirements Analysis and Management**

The Contractor shall maintain the RPUAS FoS requirements to include Government-provided requirements in a commercially available requirements management tool. The Contractor shall allocate requirements from the released set of RPUAS specifications and Government-Furnished Information (GFI), including FCS Delivery Order requirements, into appropriate documents as defined by the SUAS Specification Tree (Version 1.0). The Contractor shall deliver up to 16 draft specifications and up to three released specifications. The Contractor shall deliver draft specifications No Later Than (NLT) 30 days prior to end of this TO Period of Performance (PoP). The Contractor shall deliver specifications for release to the Configuration Control Board (CCB) for approval NLT 30 days prior to end of this TO PoP. The requirements specification delivery shall include the document form for publication as well as the requirements database export (e.g., Comma-Separated Values (CSVs) or other compatible format) of the delivered specifications, per MIL-STD-961.

The Contractor shall purchase any SW licenses IAW CDRL A087 to support engineering and development activities defined in this PWS (e.g., Cradle requirements database, DOORS®, MATLAB®, etc.).

Systems Engineering and Requirements Management

The Contractor shall manage Engineering Review Boards (ERBs).

* + Schedule ERBs, Generate Minutes, and Close-Out Actions

The Contractor shall develop and deliver to the Government an Engineering Change Request (ECR) process.

The Contractor shall:

* + Manage ECRs through complete lifecycle and update Requirements Documents as necessary
  + Manage PCR Database (e.g., JIRA)
    - Define Plan to review and Close existing PCRs
    - Execute Plan to review and Close existing PCRs
    - Manage new PCRs
    - Manage SW Repository (e.g., Bitbucket)
    - Define Plan to Manage SW Repository
  + Maintain Requirements in Commercial Management Tool  
    (e.g., Cradle, DOORS®, etc.)
  + Manage Sub-System Specification Requirements
  + Create, modify, or review H-GCS, Radio, Antenna, and Control Segment Specifications based on Government direction
  + Manage the Defense Intelligence Information Enterprise (DI2E) Account including the User Accounts
  + Provide reports IAW CDRLs A004, A009, and A021.

# HWIL Testing

The Contractor shall as required conduct HWIL testing of the Government-furnished solution for the RQ-11C MRR and LRR systems IAW CDRL A064. The Contractor shall review the Government-furnished list of radio requirements and develop a test schedule along with test procedure(s) and perform verification and validation of the Government-furnished software with the TOGA H-GCS IAW CDRL A074.

The Contractor shall utilize the TOGA H-GCS, MRR, and LRR to perform tests and collect data required to support the Airworthiness Release (AWR) process. The Contractor shall document all failures as PCRs and deliver the test procedure(s) and accompanying data IAW CDRLs A008, A009, and A039 within 20 business days. The report shall provide information regarding the issue and its severity and shall provide a reference to generated PCRs.

## Configuration Management (CM) Plan (HW/SW CM Processes and CM Plan)

The Contractor shall update, maintain, and deliver CM processes and tools for SUAS HW and SW configuration items IAW CDRL A085.

The CM processes shall include instructions for PdM SUAS-approved entities with proper credentials to access stored source code, PCRs, and technical data. The CM processes shall include instructions for PdM SUAS-approved entities to create bootable images that can be released via DoD-approved media. The CM processes shall be documented in a SW configuration item management plan IAW CDRLs A066 and A085.

Verification of approved CM processes shall be delivered ten working days prior to the IPR IAW CDRL A009.

Tools in support of configuration management of SW configuration items are defined as any code, macros, or other enabling media required to execute CM processes within the DI2E framework. The DI2E framework includes the GFP tools provided to manage information placed on the DI2E server. All code, macros, or other enabling media shall be provided to the Government in whole with Government Purpose Rights.

## Document Review

The Contractor shall review the following GFP documents as necessary for accuracy and completeness. The GFP will be provided as necessary 15 working days prior to review. The Contractor shall submit recommended document changes as PCRs, enter them in the ERB process, and deliver a findings report along with the redlined document IAW CDRL A009. The report(s) shall consist of identification of the issue, its severity, and a proposed solution for correcting the issue.

* + - Interface Control Document for the TOGA H-GCS and FCS solution
    - Computer SW Product Document
    - Quality Program Plan
    - SW Resources Data Reporting Document
    - CM Plan
    - Specification Requirements Verification Matrix
    - System / Subsystem Specification documents
    - SW Test Plan
    - SW Test Report
    - SW Test Description document
    - System/SW Joint Systems Integration Laboratory (JSIL) Development and Management Plan
    - SW Development Plan
    - SW Version Description
    - SW Design Description
    - TOGA H-GCS Test Procedures, Reports, and Acceptance Test Plan
    - TOGA H-GCS Level 3 TDP Portions as Required

## Logistics and Training

The Contractor shall support this effort with shipping, receiving, inventorying, and warehousing the HW and SW associated with this program.

## Deliverables

The Contractor shall provide the following IAW their proposed schedules, as negotiated and approved during contract award (NOTE: Certain deliverables may be dependent on GFP delivery to the Contractor and contract award with the FCS solution vendor. The Contractor shall utilize the DI2E server to support SW requirements document maintenance and SW code):

The Contractor shall also provide the CDRLs listed below to the recipient(s) listed on the CDRL and submit them electronically via the PM UAS TopVue system:

1. CDRL A009 – A technical report provides fully documented results of studies or analysis performed including briefing slides.
2. CDRL A011 – Technical Reports. This provides formatting guidelines for documenting reports and requirements.
3. CDRL A016 – Revisions to Existing Government Documents. Ten working days prior to the IPR, the Contractor shall identify shortcomings with the delivered Government documents for which review and comments have been solicited and deliver comments to the Government as needed.
4. CDRL A033 – Integrated Master Schedule (IMS). Ten working days after contract award, the Contractor shall detail three levels of relevant effort within the IMS.
5. CDRL A044 – Supplier’s Configuration Management Plan to define a SW configuration item management plan.
6. CDRL A055 – Data Accession List (DAL). Ten working days prior to the IPR and 30 days prior to the end of this TO PoP, the Contractor shall provide a data accession list calling out all documentation recorded and kept in association with the product(s) being provided. The purpose is to allow the Government the opportunity to request otherwise not-provided substantiation records and design documentation necessary for the life cycle support of the product(s) being provided.
7. CDRL A058 – Specification Requirements Verification Matrix (SRVM). Ten working days prior to the IPR, the Contractor shall develop and deliver an SRVM to define how the Government identified and baselined elements of the system / sub-system specification document are to be verified, validated, and or tested.
8. CDRL A087 – SW License Requirements List.
9. CDRL A095 – Inspection and Test Procedure.

**Period of Performance (PoP)** **–** 28 June 2020 through 27 June 2021 (NOTE: This is for the Base Contract ONLY. There will be four, one-year follow-on Options available for award. If all Options were awarded / exercised, this would project the PoP End Date to 27 June 2025 for a total of five years).

## Contract Line Item Numbers (CLINs)

## CLIN 0001 – ENGINEERING SERVICES. The Contractor shall provide all labor and materials (except GFP) required to perform all aspects of engineering services detailed in Section 3 of this PWS for the following systems: RQ-11B, RQ-11C, RQ-20A, TOGA H-GCS, and other systems as they become available. Specific requirements will be negotiated on individual TOs. This CLIN will be Firm Fixed Price (FFP). FOB: Destination.

## CLIN 0002 – TECHNICAL MANAGEMENT. The Contractor shall perform all aspects of Technical Management support at CONUS and OCONUS sites as required in support of SUAS and its customers—including Program Management and Administrative support—and deliver data items IAW the PWS and all applicable contract provisions. This CLIN will be FFP. FOB: Destination.

## CLIN 0003 – TECHNICAL DATA. The Contractor shall deliver all CDRLs to the Government IAW the CDRL Instructions and PWS. This CLIN will be FFP. FOB: Destination.

**CLIN 0004 – TRAVEL COST FOR ABOVE (IF APPLICABLE).** TO BE REIMBURSED AT ACTUAL COST WITH GENERAL AND ADMINISTRATIVE (G&A) ONLY IAW Section C of W911QY-13-D-0097 PWS and all applicable contract provisions. FOB: Destination.

## CLIN 0005 – CONTRACTOR MANPOWER REPORTING. The Contractor shall provide annual or end of PoP report IAW Contract Instructions and PWS. Report will account for all Contractor manpower (including Subcontractor manpower). This CLIN will be FFP. FOB: Destination.

**CLIN 0006 – OTHER DIRECT COSTS (ODCs) FOR ABOVE.** TO BE REIMBURSED AT ACTUAL COST WITH G&A ONLY IAW Section C of W911QY-13-D-0097 PWS and all applicable contract provisions. The ODCs are requirements outside of those based on the pre-negotiated fully burdened, fixed price labor rates, material, etc. Includes, but not limited to, Defense Base Act (DBA), Hazardous Pay, and Danger Pay. FOB: Destination.

## CLIN 0007 – VALUE ENGINEERING CHANGE PROPOSALS. The Contractor is encouraged to develop, prepare, and submit Value Engineering Change Proposals (VECPs) voluntarily. The Contractor shall earn a 50% share in any net acquisition savings realized from accepted VECPs IAW FAR 52.248. This CLIN will be FFP. FOB: Destination.

## CLIN 0008 – SHIPPING COST FOR ABOVE (IF APPLICABLE). TO BE REIMBURSED AT ACTUAL COST WITH G&A ONLY. Shipping costs cover costs incurred moving SUAS parts and systems inventory. FOB: Destination.

**Security**

The Contractor shall comply with the requirements of this contract’s DoD Contract Security Classification Specification (DD Form 254) and shall utilize the most current Army Family of Small Unmanned Aircraft Systems Security Classification Guide (SCG) for classification guidance. The SCG will be provided to the Facility Security Officer (FSO) after contract award. The Contractor shall maintain a facility clearances at the SECRET level for performance of duties under this contract. Significant upgrades and materiel procurement related to facility clearance shall be assessed and agreed upon jointly by the Contractor and the Government. The Contractor shall maintain a sufficient number of employees with a Personnel Security Clearance at the SECRET level to perform classified tasks during the performance of this contract. The Contractor is authorized to receive, generate, store and process classified information and HW up to and including the SECRET level, at the Contractor facility.

In order to accomplish the tasks required under this PWS, the Contractor shall maintain a valid U.S. COMSEC account throughout the PoP of this contract. The performance of this contract shall require access, generation, receipt, storage, and processing of Communication Security (COMSEC), Controlled Cryptographic Items (CCI) information, tactical ground control and airborne encryption equipment. Access to COMSEC/CCI information and equipment requires a final U.S. Government security clearance at the appropriate level. The Contractor(s) shall have access to COMSEC/CCI equipment, tactical ground control and airborne encryption equipment in support of the Small UAS (SUAS) products necessary for secure communications. All COMSEC/CCI equipment shall be controlled and chain of custody maintained through a Standard Form 153. The Contractor(s) shall be responsible for the protection of COMSEC equipment from the time of receipt of the equipment until transferred via the completion of an SF-153, inventory, confirmation of end item (COMSEC) and serial numbers on the SF-153 with signatures. GCA approval is required prior to authorizing a COMSEC account to a Subcontractor (NISPOM Chapter 9, Section 4, Paragraph 9-407).

The Contractor shall require access to threat related data in the performance of this contract, which will require access to Non-Sensitive Compartmented Information.

The Contractor shall require access to information marked For Official Use Only Controlled Unclassified Information (CUI).

IAW AR 381-12, Threat Awareness and Reporting Program (TARP), Contractor employees shall report threat-related incidents, behavioral indicators, and other matters of Counter Intelligence (CI) interest specified in AR 381-12, Chapter 3, to the Facility Security Officer (FSO), the nearest military CI office, the Federal Bureau of Investigation, or the Defense Security Service. Contractor employees working as an integral part of an Army organization shall complete annual Threat Awareness training in conjunction with Army personnel.

The Contractor’s FSO shall ensure that all applicable AR 381-12 requirements are implemented for personnel who work at Contractor facilities.

The performance of this contract shall require access, receipt, and storage of classified information, and equipment, and integration with classified HW at the SECRET level at Contractor facilities.

Classified information is, and remains for the duration of the classification, the property of the U.S. Government, regardless of proprietary claims. The Contractor shall provide adequate storage at their facility for classified material up to and including SECRET. The Contractor shall comply with FAR 52.204-2, Security Requirements, which requires Contractors to comply with the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5200.22-M (NISPOM), and any revisions notice to DoD 5220.22-M, notice of which has been furnished to the Contractor. Contractors processing Government information on Contractor IT systems shall adhere to Chapter 8, NISPOM at Contractor facilities.

There is no required OPSEC deliverable associated with this contract. However, the Contractor shall adhere to all OPSEC requirements outlined in the Program Executive Office, Aviation (PEO AVN) Policy Memorandum 18-04, Operational Security (OPSEC) Plan dated 15 May 2018, National Security Decision Directive (NSDD) No. 298, “National Operations Security Program”, dated January 22, 1988, DoD Directive 5205.02F, “DoD Operations Security (OPSEC) Program”, dated 20 June 2012, DoD Manual 5205.02-M, “DoD Operations Security (OPSEC) Program Manual”, dated 03 November 2008 and Army Regulation 530-1, “Operations Security”, dated 26 September 2014. PEO AVN Policy Memorandum 18-04, OPSEC Plan, will be provided under separate cover to the FSO.

The Contractor shall be authorized to use the Defense Courier Service for keyed COMSEC equipment only. Contractor Courier account will be established and maintained IAW Defense Courier Operation (DoDI 5200.33).

All requests for public release of information, articles, videos, etc., shall be submitted to the Strategic Communications Specialist, Program Executive Office (PEO) Aviation, (SFAE-AV-O), Building 5681, Wood Road, Redstone Arsenal, AL 35898. No request shall be sent or handed directly to UAS PO personnel. The submissions shall include a letter of transmittal certifying review by the FSO that the material has been reviewed and contains no classified information. The letter of transmittal shall include the contract number.  
A minimum of 15 working days is required to process and review the request.

Information or material will not be released until approval is granted.

The Contractor is NOT authorized to release any information, record, or data obtained to any one not associated with this contract without written consent of the Contracting Officer.

Additionally, for release of U.S. Government information to non-U.S. citizens and/or foreign nationals or foreign representatives the Contractor shall obtain an export license. The PEO Aviation Foreign Disclosure Officer will review all data prior to actual release.

Contractor shall submit Visit Requests via Defense Manpower Data Center Defense Security Service - Joint Personnel Adjudication System (JPAS). The UAS JPAS SMO is W0H9AA4RB. All Visit Requests shall include the Technical POC and Technical POC telephone number. Visit Requests shall not exceed a one year period or beyond the end of the contract if less than one year.

Contractors requiring access to Government IT Systems on Government installations shall adhere to the requirement of AR 25-2, Information Technology (IT) Rapid Action Revision (RAR) issue date 23 March 2009.

Contractor personnel shall utilize their company e-mail for transmitting official U.S. Government business. Official U.S. Government business shall not be transmitted via personal, private, and commercial e-mail accounts (e.g., YAHOO, Hotmail, Gmail, Juno, AOL, etc.).

Foreign Subcontractors are restricted from access to protected subsystems or functional military exercises.

Contractor personnel are not authorized to take pictures with any form of camera inside Government facilities or on military installations without prior coordination and approval of the Public Affairs office.

The UAS PO holds final determination on the approval for CACs. Consideration for a CAC will be addressed on a case-by-case basis. CACs will be considered for Contractor employees that are deploying, that work full time on a military installation, and for Contractor employees that require frequent access to multiple DoD installations in support of this contract. Justification, to include list of multiple DoD facilities, must be included with each request for a CAC. CAC shall not be left unattended in computer. CACs are the property of the U.S. Government and shall be given to the Contractor Facility Security Officer (FSO) upon termination of employment with the company, expiration of the CAC, replacement of a CAC, or upon contract completion. The FSO shall return the CAC to the UAS PO Government Contracting Officer Representative (COR) or the UAS PO Security Manager. The loss of a CAC shall be reported, on the first business day following the discovery of the lost CAC, to your chain of command, FSO, UAS PO COR, UAS PO Security Office (256-313-5330/256-313-2678) and to the issuing agency. Visit the Real time Automated Personnel Identification System (RAPIDS) site at: <https://www.dmdc.osd.mil/rsl/appj/site?execution=e2s1> for local sites. Unauthorized possession of a CAC can be prosecuted criminally under Section 701, Title 18, United States Code. FAR 52.204-9 - Personal Identity Verification of Contractor Personnel (January 2011) applies to this contract.

Photocopying of U.S. Government Identification (CAC) is a violation of Title 18, U.S. Code Part I, Chapter 33, Section 701 and punishable by both fine and imprisonment. Although the asking for Military/Government identification is totally permissible by commercial establishments, there is a prohibition on duplication of Government identification. A state driver license or other form of photo identification should be provided to be photocopied if an establishment insists on a photocopy of the traveler’s identification. Contractor shall ensure all employees are aware of this law.

Antiterrorism Instructions

The Contractor shall comply with the following Antiterrorism instructions/provisions below.

AT Level I training. This standard language is for Contractor employees with an area of performance within an Army controlled installation, facility or area. All Contractor employees, to include Subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The Contractor shall submit certificates of completion for each affected Contractor employee and Subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 15 calendar days after completion of training by all employees and Subcontractor personnel. AT level I awareness training is available at the following website: <http://jko.jten.mil>.

Access and general protection/security policy and procedures. This standard language is for Contractor employees with an area of performance within Army controlled installation, facility, or area. Contractor and all associated sub-Contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DoD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

For Contractors requiring Common Access Card (CAC). Before CAC issuance, the Contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation IAW Army Directive 2014-05. The Contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

For Contractors that do not require CAC, but require access to a DoD facility or installation. Contractor and all associated sub-Contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by Government representative), or, at OCONUS locations, IAW status of forces agreements and other theater regulations.

iWATCH Training. This standard language is for Contractor employees with an area of performance within an Army controlled installation, facility or area. The Contractor and all associated Subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 15 calendar days after contract award.

Army Training Certification Tracking System (ATCTS) registration for Contractor employees who require access to Government information systems. All Contractor employees with access to a Government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DoD Information Assurance Awareness prior to access to the IS and then annually.

For contracts that require OPSEC Training. Per AR 530-1 Operations Security, the Contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

For Information Assurance (IA)/Information Technology (IT) training. All Contractor employees and associated sub-Contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter.

For IA/IT certification. Per DoD 8570.01, DoD 8570.01-M, DFARS 252.239.7001 and AR 25-2, the Contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. All Contractor employees working IA/IT functions must comply with the baseline certification as stipulated in above references upon contract award.

For contracts that require handling or access to classified information. The Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified “Confidential,” “Secret,” or “Top Secret” and requires Contractors to comply with—(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DoD 5220.22-M, notice of which has been furnished to the Contractor.