PERFORMANCE WORK STATEMENT

Utility Monitoring and Control Systems (UMCS) Sixth Generation (VI)

(Revision Date: 18 June 2026)

PART 1
GENERAL INFORMATION

1.1 Description of Services. The contractor shall provide all personnel, equipment tools, materials supervision, and other items and non-personal services necessary to provide the Procurement and Installation (P&I) of and/or the Maintenance and Service (M&S) of Facility Related Control Systems (FRCS) including but not limited to: Utility Monitoring and Control Systems (UMCS), Heating, Ventilation and Air Conditioning (HVAC) systems to include chiller/boiler systems installation and/or integration, Supervisory Control and Data Acquisition (SCADA) Systems, Fire Alarm Systems (FAS), life safety systems, other automated control systems including chemical / biological / radiological contaminant detection / filtration / response, utilities (electric/ gas/ water/ steam) metering, power/electrical distribution/power generation systems (include but not limited to photovoltaic, backup generator, microgrid, uninterruptible power supplies), other utility systems (central plant, water distribution, electrical distribution, sewer systems) and Electronic Security Systems (ESS), and security and/or force protection measures such as, but not limited to, barriers, fencing, gates, window treatments, hardening, and lighting.

1.2 Background. The U. S. Army Corps of Engineers Engineering & Support Center, Huntsville (CEHNC) maintains Centers of Expertise in UMCS and ESS. As Centers of Expertise, CEHNC provides direct support to Government agencies for the P&I and M&S of UMCS and related systems as described above.

1.3 Objectives. The Contractor shall provide technical support, procurement, installation, monitoring, and M&S for UMCS, ESS and related systems. These services include those actions required to preserve and maintain the systems in such a condition that they may be effectively used for their designated functional purpose.

1.4 Scope. This contract will require the Contractor to have the capability to respond to multiple requests simultaneously and to work at diverse locations. The Contractor shall provide all engineering and services necessary for the P&I of new and/or upgrades to Direct Digital Control (DDC) systems, existing HVAC systems, SCADA systems, or other automated control systems on Government facilities. This contract will require monitoring and control and M&S of control systems at Government facilities, municipalities and educational institutions to meet specific installation requirements. The Multiple Award Task Order Contract (MATOC) will predominantly be services contracts, but some task orders may have construction and supply elements. The task orders will include the necessary clauses, terms, conditions, instructions, and references for each of these work elements as applicable (services, construction, and supply).

1.4.1 These services also include Preventive Maintenance (PM), Corrective Maintenance (CM), repair/ replacement/modernization, equipment inventories, condition assessments, identification and/or validation of problems and deficiencies, preparation of work plans describing method of correction/repair, actual execution of work plan to repair failed or failing systems and associated equipment, facility management support, project management, central monitoring services, minor construction work within or exterior to a facility, development of PM plans, development of recommended spare parts lists, and other activities associated with operation, maintenance, and repair. Facility maintenance/repair/renovation shall conform to the requirements of the Unified Facilities Guide Specifications (UFGS) and Unified Facilities Criteria (UFC) as per the Performance Work Statement (PWS) issued with each Task Order (TO) award, and/or other applicable codes and standards.

1.4.2 Services will include, but are not limited to, developing of equipment installation engineering plans, providing hardware and software, providing system cybersecurity engineering and implementation, system testing and check-out, performing facility modification and minor construction required to support equipment installation, providing technical solutions that incorporate applicable force protection measures, interfacing with and installing new data transmission equipment, determining compatibility of new equipment with existing systems and integrating them, preparing system and component documentation, providing operation and maintenance manuals, providing training, warranting systems, maintaining and servicing systems, retro-commissioning systems, operating and monitoring

systems, preparing after action and other reports, providing as-built installation drawings, system evaluations, configuring/programming systems, system administration systems, provide inspections/functional tests/recommendations on control systems, and other technical and programmatic support services.

1.5 Ordering Period. This effort will be accomplished via individual TOs awarded under multiple Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts that have an ordering period of seven years (36 month base period and two, 24 months option periods). The Period of Performance (PoP) will be specified in each TO award.

1.6 Service Contract Labor Standards. TOs from this contract may be issued which are subject to Service Contract Labor Standards (see Revolutionary FAR Overhaul (RFO) 52.222-41). In the event that individual service task orders contain minor incidental work subject to the Construction Wage Rate Requirement (formerly known as the Davis-Bacon Act), Construction Wage Rate Requirements (RFO 52.222-6) will apply. The latest version of the wage determinations for the geographical areas in which the work is to be performed will be incorporated with the issuance of the TO solicitation. Wage determinations may also be found at www.wdol.gov. TOs with performance in foreign countries will not be subject to either Service Contract Labor Standards or Construction Wage Rate Requirements. For work overseas not subject to Service Contract Labor Standards and Construction Wage Rate Requirements, the contractor shall comply with local labor laws in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 252.222-7002, Compliance with Local Labor Laws (Overseas) (DEVIATION 2026-O0040). Additionally, Defense Base Act (DBA) insurance requirements will be included in TOs performed overseas, when required.

1.7 General Requirements

1.7.1 Quality Control Program (QCP). The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's QCP is how he assures himself that his work complies with the requirements of the contract. At a minimum, the contractor shall develop quality control procedures that address the areas identified in Appendix A, Performance Requirements Summary (PRS).

1.7.1.1 Corporate Quality Control and Surveillance Plan. Contractor shall develop, document, and implement an effective quality control and surveillance program for this contract and document in a plan. The QC Plan shall be submitted within 30 calendar days after MATOC award and shall include at a minimum the following documents: Corporate QC Manager appointment letter, QC organizational structure (organization chart), inspection procedures, recordkeeping procedures, report templates, and any other information as required to describe the QC program. At a minimum, the Contractor shall follow an inspection process (e.g. three phase inspection process (preparatory, initial, and follow-up) or other Government approved inspection methodology) and include sample forms to be filled out for each definable feature at the TO level. After acceptance of the QC Plan, the Contractor shall submit any proposed changes to the Government, tracked through CMP/Quality Control System (QCS) for approval by the UMCS Program Manager or COR on the MATOC.

1.7.1.2 Site Specific Quality Control Plan and Surveillance Plan. A task/site specific quality control plan shall be developed/adapted to the services specified in individual TOs and submitted as required per TO. The site-specific QC Plan shall include the following documents at a minimum: The QC Manager appointment letter (include duties and authorities at a minimum), summary of inspection procedures to be followed, sample inspection forms (preparatory, initial, follow-up) or other Government approved inspection methodology forms, and the list of definable features of work that the inspections will be based off. The Government shall be provided a minimum of 48-hour notification (based on workdays), unless otherwise specified at the TO level, of any inspection meetings. The Government is not required to be present but must be notified and given the opportunity to attend. It is the responsibility of the Contractor to maintain the inspection reports and to submit them to the Government via email within 5 days of completion. Additional details may be included at the TO level. After acceptance of the QC Plan, the Contractor shall submit any proposed changes to the Government, tracked through CMP/QCS for approval by the COR on the TO.

1.7.2 Quality Assurance (QA). The Government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP) and will include an evaluation of the Contractor's

performance. This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s). The Government may conduct QA inspections at any time on all phases and types of work performed. If any Government QA review identifies a process/work product failure or identifies noncompliance with safety practices, the Contractor will be issued a Corrective Action Request (CAR). Each CAR will be annotated as a critical nonconformance, major nonconformance, or minor nonconformance. Definitions and required contractor response times are:

* Critical Nonconformance: a nonconformance that is likely to result in hazardous or unsafe conditions for individuals using, maintaining, or depending upon the supplies or services, or is likely to prevent performance of a vital agency mission. Contractor is provided 24 hours (one business day) to provide written response to the CAR.

* Major Nonconformance: a nonconformance, other than critical, that is likely to result in failure of the supplies or services, or to materially reduce the usability of the supplies or services for their intended purpose. Contractor is provided 72 hours (three business days) to provide written response to the CAR.

* Minor Nonconformance: a nonconformance that is not likely to materially reduce the usability of the supplies or services for their intended purpose or is a departure from established standards having little bearing on the effective use or operation of the supplies or services. Contractor is provided up to 15 business days to provide written response to the CAR.

1.7.3 Government Remedies. The KO shall follow 52.246-4, “Inspection of Services-Fixed Price” for contractor’s failure to perform satisfactory services or failure to correct non-conforming services.

1.7.4 Place of Performance. The Contractor is responsible for performing the services required under this contract at the location as specified in the individual TOs. These UMCS services are required to support Department of Defense (DoD) installations or other Government facilities throughout the Continental United States, Alaska, Hawaii, and Outlying areas, as well as outside the Contiguous United States to include: Bahrain, Belgium, Brazil, Costa Rica, Ecuador, Gabon, Germany, Georgia, Greece, Haiti, India, Indonesia, Italy, Iraq, Jamaica, Japan, Kazakhstan, Kuwait, Malaysia, Mali, Montenegro, Norway, Poland, Republic of Korea, Romania, Saudi Arabia, Serbia, Suriname, Tanzania, United Arab Emirates, and United Kingdom where controls systems are installed. Other foreign jurisdictions may be added to the geographic scope of the base MATOC contracts after preparing a Justification and Approval for an out-of-scope modification to add a country in accordance with RFO Part 6, Competition Requirements, for approval by the appropriate approving authority. This will include verification that all contractors within the MATOC award pool can comply with the applicable requirements for the country to be added.

Work performed by the Contractor may be subject to other requirements or restrictions such as those issued by a U.S. Department of Defense theater-level Unified Combatant Commander (COCOM), e.g., U.S. Central Command (CENTCOM) requirements, which are provided under this contract. .

Entry and exit requirements to countries within the CENTCOM AOR, including Iraq, are contained within DFARS 252.225-7995, Contractor Personnel Performing in the United States Central Command Area of Responsibility (DEVIATION 2017-O0004), available at https://www.acq.osd.mil/dpap/policy/policyvault/Class_Deviation_2017-O0004.pdf .

Predeployment training requirements for Contractor personnel deploying to Iraq (and other countries as applicable) will be specified at the task order level.

Access to bases and installations within Iraq (and other countries as applicable) will be subject to varying operational, security, and force protection conditions. The Contractor shall coordinate with the CENTCOM (or other COCOM as applicable) Liaison Officer (LNO) for the status of such conditions for the bases and installations of interest. Granting access to bases and installations within Iraq may take up to 30 calendar days following request or notification of intent to enter.

1.7.5 Type of Contract. TOs will be firm-fixed price.

1.7.6 Security Requirements. This contract may require the handling and generation of classified information. Security requirements appropriate for each TO will be delineated in the individual TOs. Some TOs issued may require a security level of SECRET and some may require a higher level than SECRET. The Contractor shall meet the Industrial Security requirements of the National Industrial Security Program Operating Manual (NISPOM) for Safeguarding Classified Information (DoD 5220.22-M), which is now Part 117 of Title 32, Code of Federal Regulations. The clearance level will be determined by the User Agency. A DD Form 254 (DD 254), Contract Security Classification Specification, shall be provided. No classified work is authorized without an approved DD 254 and the appropriate personnel and facility security clearance. Personnel security clearances will be obtained by the contractor in accordance with the NISPOM. Facility security clearances will be obtained by the User Agency Security Office.

1.7.6.1 Physical Security. Reserved

1.7.6.2 Information Security. The Contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information systems including all subcontractor information systems utilized on contract. Unclassified DoD information shall only be disseminated within the scope of assigned duties and with a clear expectation that confidentiality will be preserved. Examples of such information include the following: non-public information provided to the Contractor, information developed during the contract, and privileged contract information (for ex: program schedules, contract-related tracking). Below are safeguards the Contractor, and all subcontractors, shall abide by to protect Government information.

a) Do not process DoD information on public computers (e.g., those available for use by the public in kiosks or hotel business centers) or computers that do not have access control.
b) Protect information by at least one physical or electronic barrier (e.g., locked room, login and password) when not under direct individual control.
c) Sanitize media (e.g., overwrite) before external release or disposal.
d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.
e) Limit information transfer to subcontractors or teaming partners with a need to know and commitment to at least the same level of protection.
f) Transmit email and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment.
g) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction.
h) Provide protection against computer network intrusions and data exfiltration, minimally including the following: updated malware protection devices, prompt application of security-relevant software patches/service packs/hot fixes, and monitoring and control of inbound and outbound network traffic as appropriate.
i) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.
j) The Contractor shall not release any information to the public without prior approval by the CEHNC Office of Public Affairs (i.e. trade publications and marketing information).

1.7.6.3 Site Specific Security Requirements**.** When Contractor personnel are at any Government site, installation or facility, they shall follow all security procedures and processes of the installation as stated and directed by the Government personnel at the site. The Contractor's security requirements for work in foreign countries will be based on the requirements set by the combatant commander of the Area of Responsibility (AOR) in which the work will be performed. The items that will be covered on a TO basis will include but are not limited to transportation into and out of the operating area, required clothing and equipment, transportation security while moving in the operating area, specific employee training prior to entering the operating area, etc. All security requirements will be further detailed at the time of TO awards.

1.7.6.4 Information Technology Systems. For TOs requiring access to Government Information Technology (IT) Systems, but not to classified information, the following requirements apply:

1.7.6.4.1 All contractor employees who are U.S. citizens working under this contract who require access to IT systems (stand-alone computers, network computers/systems, e-mail, etc.) shall, at a minimum, be designated into an IT I, II or III position in accordance with Army Regulation (AR) 25-2, Army Cybersecurity. The investigative requirement for an IT I position is a favorable Single Scope Background Investigation (SSBI); IT II and IT III positions require a favorable National Agency Check and written Inquires (NACI).

1.7.6.4.2 A Common Access Card (CAC) is also required for access to Government IT systems. Proof of the appropriate investigative requirement/background check will be verified through the Joint Personnel Adjudication System (JPAS) by the CEHNC security personnel.

1.7.6.4.3 Non-U.S. Citizens. Foreign nationals who work on a Corps of Engineers' contract or TO in the United States shall be approved by the Headquarters U.S. Army Corps of Engineers (HQUSACE) Foreign Disclosure Officer before beginning work on the contract or TO. This approval requirement also includes subcontractor employees. The Contractor shall submit to the KO the names of all foreign nationals proposed for performance under this contract or individual TOs, along with documentation to verify that he or she is legally admitted into the United States and has authority to work. This information will be forwarded to the CEHNC Security Officer for approval.

1.7.7 Contractor Management Platform (CMP). The Contractor must be prepared to transition from the Resident Management System (RMS) to the new CMP at any time during the period of performance of this contract, once the USACE enterprise implements this change. The Government will use CMP for Windows to assist in its monitoring and administration of TOs. The Government will use the CMP to assist in its monitoring and administration of TOs. The Contractor uses the Contractor Mode of CMP, to record, maintain, and submit various information throughout the contract period. The Contractor mode user manuals, updates, and training information can be downloaded from the CMP web site. The joint Government-Contractor use of CMP facilitates electronic exchange of information and overall management of TOs. CMP provides the means for the Contractor to input, track, and electronically share information with the Government in the following areas: Administration, Finances, Quality Control, Submittal Monitoring, Scheduling, and Import/Export of Data.

1.7.8 Safety Requirements

1.7.8.1 Corporate Safety and Health Program. The Contractor is required by regulation to develop and maintain a written Corporate Safety and Health Program (SHP) in compliance with the requirements of the Occupational Safety and Health Administration (OSHA), EM 385-1-1, 29 CFR 1910, 29 CFR 1926, 29 CFR 1960, and RFO 52.236-13.

1.7.8.2. All Safety submittals must be input into Construction Management Platform (CMP) and email sent to, at a minimum, the HNC PM, HNC Engineer, and UMCS Safety inbox (CEHNC-UMCS-Safety@usace.army.mil).

1.7.8.3. Site Visit Abbreviated Accident Prevention Plan (SVAAPP). A SVAPP is required if an Accident Prevention Plan with a site/survey activity hazard analysis (AHA) has not been previously provided and accepted by the CEHNC KO/COR in coordination with (ICW) CEHNC Safety and Occupational Health Office (SOHO). The SVAPP is necessary for any site visit where physical work will not be occurring. It shall be for visual inspection/observation or office type work only. The SVAAPP shall be approved prior to the Contractor performing any surveys on-site. An example of an SVAAPP can be obtained by contacting the CEHNC Safety Office. SVAAPP's shall be submitted electronically to the CEHNC Safety Office and Project Manager (Adobe PDF format) and uploaded to CMP for acceptance. Submission or acceptance requirements may be updated at the TO level.

1.7.8.4. Accident Prevention Plan (APP). The Contractor shall submit a site-specific prior to any installation/maintenance activities beginning at the site. The APP shall follow the minimum requirements of the 2024 version of Engineering Manual (EM) 385-1-1, Safety and Health Requirements Manual, Chapters 2-7 and submitted on the mandatory ENG Form 6293 (Accident Prevention Plan Worksheet). The Contractor shall coordinate with the facility representatives or facility contractor, on first aid, emergency phone numbers & response plans, site evacuation plans, lock out tag out procedures, any permit required procedures, obtaining a list of previously identified confined spaces, evacuation drills, hazardous/toxic environments/agents etc. This information shall be included in the APP. The APP shall also include site specific AHAs for the project. The APP must be submitted and accepted by the CEHNC KO/COR ICW CEHNC SOHO prior to starting any service/construction

work at the site. It should be readily available to all tiers of contractors (and their employees) on the jobsite. Safety submittals shall be written ICW the subcontractor when applicable; however, the prime contractor must review, concur, and ensure submittals meet EM 385-1-1 requirements PRIOR to uploading into CMP. Safety resubmittals shall include the original comments with detailed responses and highlight all changes in the resubmission. The APP shall be approved prior to the Contractor mobilizing on-site to perform work. Submission or acceptance requirements may be updated at the TO level.

1.7.8.5. Addendums to the APP - The Contractor is responsible to verify that any Proposals, Service Orders, Change Orders, and Contract Modifications are covered under the current accepted APP. If the pending work effort is NOT covered under the initial task order APP, the contractor shall submit, for Government review and acceptance, an addendum to the APP.

1.7.8.6. Activity Hazard Analysis (AHA) - Before beginning each activity, task or Definable Feature of Work (DFOW) involving a type of work presenting hazards not experienced in previous project operations, or where a new work crew or subcontractor is to perform the work, the Contractor(s) performing that work activity must prepare an AHA. AHAs shall be provided to the Prime Contractor for review and approval before submitting into CMP for review and acceptance by USACE. The Prime Contractor shall review the accepted AHAs periodically (at least annually in conjunction with an APP review) and update as necessary when procedures, scheduling, or hazards change.

1.7.9. Safety Officials

1.7.9.1. Prime Contractor Corporate Safety Official. This contract requires a minimum of one Corporate Safety Official to manage and oversee the implementation of the Prime Contractor's Safety Program. The Corporate Safety Official shall follow the roles and responsibilities listed in EM 385-1-1 (2024) Chapter 2-4.f. This individual is not required to physically be on the project site.

1.7.9.2. Site and Safety Health Officer (SSHO). No work shall be conducted onsite unless a SSHO is present as described and EM 385-1-1 (2024) Chapter 2-8.b. SSHOs shall be designated on the required ENG Form 6282 found in Chapter 2 of EM 385-1-1. High risk activities require a L1 SSHO. L1/L2 SSHOs are allowed to dual hat with a competent person other than the project manager/onsite manager. He/She cannot manage non-safety individuals on the jobsite. Triple hatting is not allowed. L3s can be a subcontractor dual-hat employee if it is explained in the APP how the prime contractor will exhibit stringent direction and control over the L3's and overall jobsite safety.

1.7.9.3. SSHO Coverage on projects is determined by the type of work that is occurring. Please refer to the SSHO Chart in the task order level PWS for the minimum acceptable SSHO coverage for UMCS work. If an activity is not listed, it is the prime contractor's responsibility to ensure that SSHO coverage is adequate for the activities occurring onsite. During high-risk activities, the functions and roles of the L1SSHO shall be a singular, full-time responsibility (no other collateral duties). Such activities include, but are not limited to: crane operations, excavations greater than 5-feet, permit required confined space entry, asbestos/lead abatement, and any other high hazard activity listed in the PWS for each task order. The Contractor must demonstrate that the L1SSHOs non-safety duties are transferred to another employee when full-time SSHO responsibilities are warranted per the risk activities. The SSHO must be at the location of the high hazard activities while they are being conducted.

1.7.10. Exposure Hour and Mishap Reporting

1.7.10.1. Exposure Hour Reporting (Monthly Man-hour reporting) - In accordance with EM 385-1-1, the Contractor shall complete a monthly summary report of accident experience, exposure, Restricted Duty (RD) and Lost Workdays (LWD) prior to the 10th of the following month. Exposure data consists of man-hours (prime and subcontractors) expended in direct performance of the work performed on the jobsite. Hours associated with administrative activities such as payroll, human resource, service order managers, etc., are not counted. The information cut-off date will be the last day of each month. If no hours are worked on the project/task, a report showing zero (0) is required.

1.7.10.2. Mishap Reporting – Mishaps shall be reported in accordance with the EM 385-1, 2-8(d) and Table 2-1. The Huntsville Center Contracting Officer, Project Manager and Safety Office shall be notified as soon as practical, but no more than twenty-four hours, after any mishaps, including recordable accidents, incidents, and near misses. All mishap notifications will be submitted in accordance with the task order.

1.7.10.3. Post Award Conference/Periodic Progress Meetings. The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office. The KO, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the Government will apprise the Contractor of how the Government views the contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

1.7.10.4. Program Manager. The Contractor shall provide a program manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the KO. The program manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract.

1.7.10.5. Identification of Contractor Employees. All contract personnel attending meetings and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

1.7.11 Travel

1.7.11.1 Locations: In support of various tasks and specified on TOs, the Contractor shall be required to travel to DoD facilities located worldwide. Travel shall be performed in accordance with RFO 31.205-46.

1.7.11.2 Travel Outside the Continental United States Immunization Requirements: As specified in each TO, the Contractor shall be required to travel to locations both shore and afloat. Contractor employees who deploy to locations that require immunizations shall do so in accordance with DoD Foreign Clearance Guide or other agreements that the United States may have with the country.

1.7.11.3 Letter of Authorization. Some travel shall require a Letter of Authorization (LOA). As noted in DFARS 225.771-3(e), a LOA is necessary to enable a contractor employee to process through a deployment processing center; to travel to, from, and within a theater of operations; and to identify any additional authorizations and privileges. As required by TO, the Contractor shall initiate a LOA for each prospective traveler. If required at the TO level, the Contractor shall use the Synchronized Pre-deployment & Operational Tracker (SPOT) web-based system to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs.

If it is in the Government's interest, the Contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs shall be signed/approved by the Contracting Officer for the TO who is registered in the SPOT system.

1.7.12. Base Contract Submittals. The Contractor shall submit the following documents (following format in the table below), tracked through CMP/QCS within thirty (30) days of base contract award to the UMCS Program Manager. The documents shall be submitted under TO #0001, minimum obligation. After approval, all proposed changes by the Contractor shall be submitted under TO #0001

Submittals	Tracked in CMP/QCS	Form 4025 Required	CD/DVD	E-mail	
				PgM	Safety Office
Corporate Safety and Health Program	Yes	Yes	√	√	√
Corporate Quality Control and Surveillance Plan	Yes	Yes	√		
Corporate Management Plan	Yes	Yes	√		
Unless otherwise specified, all report formats shall be Microsoft Office (Word and Excel) and /or Adobe PDF					

PART 2
DEFINITIONS & ACRONYMS

A&A – Assess and Authorize

AAPP – Abbreviated Accident Prevention Plan

ACA – Agent for the Certification Authority

ACE-IT – Army Corps of Engineers Information Technology

AHA – Activity Hazard Analysis

AO – Authorizing Official

AODR – Authorizing Official Designated Representative

AOR – Area of Responsibility

APMS – Army Portfolio Management System

APP – Accident Prevention Plan

AR – Army Regulation

ATC – Authority to Connect

ATO – Authority to Operate

C&A – Certification and Accreditation

CAC – Common Access Card

CAL – Category Assurance List

CAR – Corrective Action Request

CAT - Category

CBT – Computer Based Training

CDRL – Contract Data Requirements List

CIA – Confidentiality, Integrity and Availability

CIO – Chief Information Officer

CM – Corrective Maintenance

CMP – Construction Management Platform

CND – Computer Network Defense

COB – Close of Business

COR – Contracting Officer Representative

CPAR – Contractor Performance Assessment Reporting System

CR – Cost Reimbursement

CS – Control Systems

CUI – Controlled Unclassified Information

CEHNC – U.S. Army Corps of Engineers, Engineering and Support Center, Huntsville

DA – Department of the Army

DBA – Defense Base Act

DFARS – Defense Federal Acquisition Regulation Supplement

DHS – Department of Homeland Security

DID – Data Item Description

DISA – Defense Information Systems Assurance

DoD – Department of Defense

DoDD – Department of Defense Directives

DoDI – Department of Defense Instructions

DDC – Direct Digital Controls

EM – Engineering Manual

eMASS – Enterprise Mission Assurance Support Service

ER – Engineering Regulation

ESS - Electronic Security System

FAS - Fire Alarm System

FRCS- Facility Related Control Systems

FSC –Federal Service Code

GDA – Government Designated Authority

HVAC – Heating, Ventilation, and Air Conditioning

HQUSACE – Headquarters, U.S. Army Corps of Engineers

IA – Information Assurance

IAM – Information Assurance Manager

IASAE – Information Assurance System Architect and Engineer

IAT – Information Assurance Technical

IAVA – Information Assurance Vulnerability Alerts

IAVM - Information Assurance Vulnerability Management

IAW – In Accordance With

ID/IQ – Indefinite Delivery / Indefinite Quantity

IO – Information Owner

ISO – Information System Owner

ISSM – Information System Security Manager

ISSO – Information System Security Officer

IT – Information Technology

JPAS – Joint Personnel Adjudication System

JTR – Joint Travel Regulations

KO – Contracting Officer

LHE – Load Handling Equipment

LOA – Letter of Authorization

LWD – Lost Workday

M&S – Maintenance and Service

MATOC – Multiple Award Task Order Contract

NACLC – National Agency Check with Law and Credit

NEC – Network Enterprise Center

NISPOM – National Industrial Security Program Operating Manual

NIST – National Institute of Standards and Technology

O&A – Over and Above

O&M – Operation and Maintenance

OEM – Original Equipment Manufacturer

OND – Operational Need Date

OO – Ordering Officer

OSHA - Occupational Safety and Health Administration

P&I – Procurement and Installation

PAC – Package Approval Chain

PIT – Platform IT

PGI – Procedures, Guidance and Information

PgM – Program Manager

POA&M – Plan of Actions and Milestones

PM – Preventive Maintenance

PoP – Period of Performance

PPS – Ports, Protocols, and Services

PRS – Performance Requirement Summary

PVT – Performance Verification Test

PWS – Performance Work Statement
QA - Quality Assurance

QASP – Quality Assurance Surveillance Plan

QC - Quality Control

QCP – Quality Control Program

QCS – Quality Control System

RD - Restricted Duty

RFO – Revolutionary FAR Overhaul

RFP – Request for Proposal

RMF – Risk Management Framework

RMS – Resident Management System

SAP – Security Authorization Package

SCA – Security Control Assessor

SCA-R – Security Control Assessor Representative

SCADA - Supervisory Control and Data Acquisition Systems

SHP – Safety Health Program

SISO – Senior Information Security Officer

SO – Service Order

SSBI – Single Scope Background Investigation

SPOT – Synchronized Pre-Deployment & Operational Tracker

SSHO – Site Safety Health Officer

STIG – Security Technical Implementation Guides

TO – Task Order

UC APL – Unified Capabilities Approved Products List

UFC – Unified Facilities Criteria

UFGS – Unified Facilities Guide Specification

UIC – Unit Identification Code

UMCS - Utility Monitoring and Control System

UR – User Representative

USACE – United States Army Corps of Engineers

PART 3
GOVERNMENT PROPERTY AND SERVICES

RESERVED

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4.1 General: The Contractor shall furnish all labor, supervision, travel, equipment and materials as required to perform the work under the individual TO PWS.

4.2 Reserve.

4.3 Security Clearances: Security requirements appropriate for each TO will be delineated in the individual TOs. The Contractor shall have or be capable of obtaining a facility clearance through SECRET. All key personnel designated shall have or be able to obtain a security clearance of SECRET. The Contractor shall comply with the security requirements of the Department of Defense Contract Security Classification Specification, DD Form 254.

PART 5
SPECIFIC TASKS

5.1 Basic Services. The following requirements and deliverables will be required under the base contract and shall therefore be applied to subsequent TOs. Additional requirements described in each TO, once awarded, may complement, emphasize, or add to any requirements or processes mentioned in this paragraph. The Government

reserves the right to expand the requirements of any TO so long as the requirement does not force the Contractor to perform outside the scope of what would be considered reasonably within the bounds of this contract. Each TO will identify the nature and scope of the work required.

5.1.1 Contractor shall participate in a post-award orientation conference at the site prior to installation work. The work will be associated with P&I of and/or the M&S of FRCS including but not limited to: UMCS, HVAC systems installation and/or integration, SCADA systems, FAS, life safety systems, other automated control systems including chemical / biological / radiological contaminant detection / filtration / response, utilities (electric/ gas/ water/ steam) metering, ESS, and security and/or force protection measures such as, but not limited to, barriers, fencing, gates, window treatments, hardening, and lighting. HVAC systems may include central plant equipment and systems (e.g., chillers, boilers, cooling towers), distribution systems (e.g., duct work, chilled water piping, hot water piping, drain piping), and unitary heating and cooling equipment (e.g., unitary heat pumps, unitary air conditioners). The work may include design of systems (such as defined above) and will be further clarified in each TO.

5.2 Specific task areas or functions to be performed at the TO level are listed below. All tasks are to be performed in accordance with criteria, specifications, drawings, original manufacturer's published procedures (if applicable), and Contract Data Requirements List (CDRL), Form DD 1423 (See Section J, Exhibits C, D, E, & F). As applicable to specific tasks, the Contractor shall:

5.2.1 Participate in a post-award orientation meeting at the site prior to commencing work. Provide a QCP, a Project Schedule and an APP.

5.2.2 Perform an existing site conditions survey to validate the quantities of system equipment and verify existing site conditions. Provide a written report noting all identified discrepancies.

5.2.3 Perform engineering surveys or assessments to develop or verify design drawings and equipment lists. Provide a report identifying equipment incompatibility concerns between the existing and new systems.

5.2.4 Prepare and provide mechanical equipment installation engineering plans.

5.2.5 Prepare and provide electronic equipment installation engineering drawings to include drawings related to installation and assembly of the computers, field equipment panels, data transmission equipment, interfaces, instrumentation and all other equipment.

5.2.6 Prepare and provide system installation engineering drawings, instrumentation installation drawings, wiring diagrams, procedures for field installation of all equipment, and system testing procedures, as defined in UFC 3-470-01 and UFC 3-410-02, or latest Corps of Engineers technical guidance.

5.2.7 Provide Mechanical Equipment. Install equipment IAW original manufacturer's published procedures and documentation and as required by the specifications.

5.2.8 Provide Hardware and Software. Install hardware and software IAW original software developer's published procedures and documentation and as required by the specifications. Resolve compatibility issues and establish an interface between existing and new systems. All software and software updates shall be approved by the Government prior to installation. Provide graphics for the system IAW criteria and specifications using data from drawings, engineering surveys and manufacturer's data.

5.2.9 Perform factory testing, Performance Verification Testing (PVT), endurance testing, and commissioning IAW the applicable and referenced sections of criteria and specifications in this TO. For PVT and at his/her sole discretion, the KO may require consideration from the contractor equivalent to reimbursing the cost of the Project Engineer and/or other Government PVT witness (including, but not limited to the labor and travel of personnel conducting the subsequent PVT reassessment) in the form of a credit to the contract price if the contractor does not pass the initial PVT attempt.

5.2.10 Perform minor ancillary work required to support equipment installation.

5.2.11 Provide all data transmission equipment IAW specifications, drawings and manufacturer's published documentation. Install in compliance with Network Enterprise Center (NEC) or its equivalent authority, Department of Defense (DOD) and Component Specific applicable certification and accreditation requirements, policies and procedures.

5.2.12 Interface to all existing data transmission equipment IAW specifications, drawings and manufacturer's published documentation. Comply with all requirements of the DOD, Component, NEC, or its equivalent authority related to interfacing with the existing communication system. Provide technical data, equipment and software in compliance with Cybersecurity policy and requirements.

5.2.13 Provide all required Operation and Maintenance (O&M) Manuals.

5.2.14 Provide training as required by the applicable sections of the specifications listed in Section H, Exhibit F.

5.2.15 Provide a System Warranty. Provide an unconditional (excluding acts of God and negligence of Government personnel), one-year parts and labor warranty from time of Government acceptance (i.e. successful PVT) for the new components of the entire system: mechanical equipment, ancillary components, subsystems, data transmission system, and all Contractor furnished software.

5.2.16 Provide after-action reports, accident reports, minutes of each meeting, confirmation notices of communications, field inspection reports, calibration reports, and installation progress reports. Copies shall be furnished to the Government within 5 working days or sooner, if required, after each specific action.

5.2.17 Provide final As-Built Drawings. All drawings shall be generated in electronic media compatible with the latest version of Microstation, AutoCAD, or as defined in individual TOs. Drawings shall be delivered within 30 calendar days after the written acceptance of the system by the Government.

5.2.18 Provide software licensing and configuration tools related to UMCS, ESS, SCADA, other control and monitoring systems and HVAC systems as further clarified by individual TO.

5.2.19 Perform special engineering services and studies related to UMCS, ESS, SCADA, other control and monitoring systems and HVAC systems as further clarified by individual TO.

5.2.20 Provide all M&S and/or operation of systems as specified.

5.2.21 Comply with Cybersecurity Requirements. Prepare and provide system cybersecurity design deliverables, specifications, and construction submittals/technical artifacts as defined in UFC 4-010-06, UFGS 25-05-11, and / or latest Corps of Engineers, DoD, and / or Federal agency technical guidance. Provide system, security, and network engineering services, RMF (Risk Management Framework) process services, project specifications, and deliverables to support system owner required cybersecurity activities to obtain operational, accreditation, and / or connection approvals. Provide cybersecurity maintenance services, vulnerability identification and mitigation, and continuous monitoring services required to maintain secure baselines and accreditations. Cybersecurity requirements will be further clarified by individual Task Order level Performance Work Statements.

5.3 TO Requirements

5.3.1 The Contractor shall perform the work under individual TOs. Each TO will identify the specific work to be performed. Individual TOs may add additional technical requirements as necessary to define the work, including Specifications, Technical Manuals, Engineer Instructions, and EMs. The performance period will be negotiated and determined for each individual TO. Contractor shall prepare and submit a detailed project schedule in Primavera (unless otherwise specified at the TO level) that shows an appropriate breakout of activities and includes any key milestones that may be stated in individual TOs. Contractor shall submit a technical solution meeting all the requirements in the PWS, including sufficient detail for the Government to evaluate the Contractor's technical solution versus the requirements in Adobe PDF format. The Contractor shall submit cost and pricing data associated

with the technical solution, to include labor rates, markups, material costs, and detailed subcontractor pricing in an unlocked MS Excel format (cost narratives may be submitted in Adobe PDF format). Cost and pricing data details shall be in enough detail to substantiate any proposed costs, and so that the Government can determine whether the pricing proposed is fair and reasonable.

5.3.2 Awards will be determined based on best value to the Government unless stated otherwise in the Request for Proposal (RFP).

5.4 Information Support and Documentation.

5.4.1 All required technical information, and data shall be delivered in accordance with the requirements, quantities, and schedules set forth in Section J, Exhibit C, CDRL DD Form 1423, Data Item Description (DID) DD Form 1664, or as otherwise specified or required. The requirements for contents and detail of operation and maintenance manuals, testing documentation (including level and detail) shall be as described in applicable UFGS and shall be further clarified in the individual TO PWS.

5.4.2 Contractor shall be responsible for preparing after-action and other reports to include progress reports, minutes of all meetings, confirmation notice for telephone calls, field inspection reports, calibration reports and installation reports. Copies of all such documents shall be furnished, within five working days, to the points of contact identified in the TO after each specific action. Project status shall be formally reported monthly.

5.5 Continuation and Completion of Work.

5.5.1 The Contractor shall conduct all work under the direction of a COR appointed by the KO. This representative shall be responsible for the coordination of all work under each individual TO. The Contractor's company officer or representative designated as Program Manager shall be responsible for the complete coordination of all work under this contract. All work shall be accomplished in accordance with the contractor's approved QC Plan. The Government may elect to provide third party technical inspection.

5.5.2 Warranty: The systems, all its components, subsystems, data transmission system, and all Contractor-furnished software shall be covered by warranty. The Contractor shall warrant all products and services provided under each TO (material and labor) for a period of one year from the date of Government acceptance (i.e. successful PVT), or the offeror's standard commercial warranty period, whichever is greater. The Contractor shall provide the necessary support required to maintain the warranty. Upon any product/service failure during the warranty period, Contractor's response time to restore system service shall be within the timeframes indicated herein. "Mission Critical Outages" will require a maximum of 4-hour response time during normal working hours and maximum of 16-hour response time for after hours (defined as outside "normal" 0700-1600 working hours) and one (1) day to restore system operation. All other outages will require a maximum of three (3) working days response time and seven (7) working days to restore system operation. System outages assessed as "Mission Critical" will be at the discretion of the KO or COR.

5.5.3 Contractor's warranty letter shall be submitted after successful completion of PVT. Warranty letter shall indicate at a minimum: standard project warranty dates and points of contact, equipment warranties and points of contact, list of equipment (make/model/serial number of equipment) with Original Equipment Manufacturer (OEM) warranties that extend beyond the project warranty period, and OEM warranty documentation.

5.7 Performance Measures.

5.7.1 Performance Measures for each TO will be agreed upon before award depending on the nature of services and/or work required. The Government will monitor contractor performance under this contract using the method of surveillance specified in the QASP (See Appendix A) and PRS.

5.7.2 Performance measures will be determined on a TO by TO basis. Examples of specific performance measures include quality of product or service, schedule, cost control, customer satisfaction, safety, performance (including the number of CARs), complexity of work, and management of key personnel.

5.8 System Security Engineering Maintenance and Support. The Contractor shall adhere to cybersecurity regulations and directives and provide system security engineering. Contractor shall design, develop, and integrate cybersecurity into each system (to include all hardware, software and / or equipment) IAW the DoD, Department of the Army (DA), any other applicable Government Agency standards or regulations.

5.9 Key Personnel. The Contractor shall notify the Government of any key personnel changes. The Contractor shall not substitute any employee for an employee specifically named in its proposal without the prior written consent of the KO. The Government reserves the right to disapprove any changes that are not in the best interest of the Government. Required Key Personnel are identified below and shall, at a minimum, meet the requirements listed for each discipline.

Program Manager: The Program Manager (PgM) shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. Typical seven to ten (7 - 10) years relevant experience in the UMCS/ESS/FAS/SCADA technology field, including five (5) years of experience in a management or supervisory capacity and five (5) years in the functional area of the program to be managed. PgM proposed shall have a Bachelor's degree in engineering or business from an accredited university or college, or a related field, or in the project's functional area.

Project Manager: Responsible for planning and executing major portions of the project. Prepares and maintains the project scope, schedule, and budget. Primary point of contact for the customer on assigned tasks. Oversees all work and takes corrective action as necessary to ensure success of assigned tasks. Manages staffing, budget, prioritization, and other personnel matters. May serve as technical lead for assigned tasks. Experience with Government or industry processes, procedures, standards, methodologies, or tools as relative to the assignment. Typical five (5) years experience in the project management field plus demonstrated experience in the project's functional area. Bachelor's degree from an accredited university or college. PMP certification preferred.

Contracts Manager: Shall have the full authority as a Company representative in all matters relating to contracts to include but not limited to: contracts negotiations, modifications, and proposal submittals. The person proposed shall have ten (10) years experience in the contracting field, including five (5) years of experience in a management level capacity. The person proposed shall have a Bachelor's degree in business from an accredited university or college, or a related field, or in the project's functional area.

Quality Control Manager: Typical seven to ten (7 - 10) years relevant experience in the quality control field, including five (5) years experience as a Quality Control Manager. The person proposed shall have a Bachelor's degree from an accredited university or college, in a related field, or in the project's functional area.

Fire Protection Engineer: Will represent the company with fire alarm system engineering products and solutions and the adherence to applicable codes. Provides Professional Engineering Stamp for fire alarm systems. The person proposed shall have ten (10) years experience in the Fire Protection engineering field, including five (5) years in the functional area of the project to be managed. Must have a U.S. Professional Engineers certification. The person proposed shall have a Bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area.

Site Superintendent: Provides site wide management of personnel for routine activities according to established procedures or instructions. Complies with the standards and organizational requirements relative to specific assignments. Five (5) years of experience related to specific heating ventilation and air conditioning experience with associated controls. Experience with Government or industry processes, procedures, standards, methodologies, or tools as relative to the assignment. High School diploma, plus technical training in field related to task assignment.

HVAC Technician: Provides support for HVAC/Controls activities according to established procedures or instructions. Works independently to assist with technical support for elements such as: complex processes, structural elements, electric/electrical/electronic components, equipment, applications, systems, software, networks, satellites, telecommunications, facilities, or machinery. Complies with the standards and organizational requirements relative to specific assignments. Five (5) years of experience related to specific heating ventilation and air conditioning experience with associated controls. Experience with Government or industry processes,

procedures, standards, methodologies, or tools as relative to the assignment. High School diploma, plus technical training in field related to task assignment.

Senior Security System Engineer (SSE): The Senior SSE is responsible for the design, development, implementation, and/or integration of a DOD IA architecture, system, or system component for use within CE (computing environment), NE (network environment), and/or enclave environments. Must meet the Department of Defense Directive (DoDD) 8570.01 "Information Assurance Training, Certification, and Workforce Management" and DoD 8570-M "Information Assurance Workforce Improvement Program" requirements for IAM (Information Assurance Manager) Level 3 and IAT (Information Assurance Technical) Level 3, or IASAE (Information Assurance System Architect and Engineer) Level 3.

Security System Engineer (SSE): The SSE is responsible for the design, development, implementation, and/or integration of a DOD IA architecture, system, or system component for use within CE (computing environment), NE (network environment), and/or enclave environments in support of higher ranking IA professionals. Must meet the Department of Defense Directive (DoDD) 8570.01 "Information Assurance Training, Certification, and Workforce Management" and DoD 8570-M "Information Assurance Workforce Improvement Program" requirements for IAM (Information Assurance Manager) Level 1 or 2, and IAT (Information Assurance Technical) Level 1 or 2, OR IASAE (Information Assurance System Architect and Engineer) Level 1 or 2.

Senior Electrical/Mechanical Engineer: Will represent the company with engineering products and solutions. The person proposed shall have ten (10) years experience in the Electrical/Mechanical engineering field, including five (5) years in the functional area of the project to be managed. The person proposed shall have a Bachelor's degree in engineering from an accredited university or college. Must have a Professional Engineers certification.

Electrical/Mechanical Engineer: Will provide mechanical/electrical engineering products and solutions. Five (5) years experience in the Electrical/Mechanical engineering field, including three (3) years demonstrated experience in the functional area. Bachelor's degree in engineering from an accredited university or college.

Senior Electronic Security Engineer: Will represent the company with electronic security system engineering products and solutions. The person proposed shall have ten (10) years experience in the electronic systems/information technology field and demonstrated experience in the project's functional area. The person proposed shall have a Bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area. Must have a Professional Engineers certification.

Electronic Security Engineer: Will represent the company with electronic security system engineering products and solutions. The person proposed shall have five (5) years experience in the electronic systems/information technology field and demonstrated experience in the project's functional area. The person proposed shall have a Bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area.

Network Specialist: Responsible for the design, implementation, and defense of the network. Must meet the Department of Defense Directive (DoDD) 8140 "Information Assurance Training, Certification, and Workforce Management" and DoD 8140 "Information Assurance Workforce Improvement Program" requirements for IAT (Information Assurance Technical) Level 1 or 2, OR IASAE (Information Assurance System Architect and Engineer) Level 1 or 2 OR meet the requirements for any type of Computer Network Defense (CND) professional (CND-A, CND-IS, CND-IR, CND-AU) mentioned in the aforementioned regulations.

5.10 Service Contract Reporting. The Government operates and maintains a secure data collection site where the Contractor will report on ALL services required for performance of this contract. The Contractor is required to completely fill in all the information in the format using the following web address https://www.sam.gov (see SAM User Guide). See RFO 52.204-14, Service Contract Reporting Requirements, for reporting requirements.

5.11 MAINTENANCE AND SERVICE:

5.12 Preventive Maintenance (PM): Contractor shall perform all PM activities consistent with the operational requirements to ensure continuous operation and reliability of each system.

5.13 Corrective Maintenance (CM): The Contractor shall replace, or repair failed, damaged, or defective hardware, software, instrumentation, and controls on the equipment specified in the PWS. Repair may be overhaul, reprocessing, or replacement of nonfunctional parts or materials that have failed or deteriorated by action of the elements or usage and have not been corrected through maintenance, or it is the replacement of the entire unit or system if beyond economical repair. Repair work may also include inspection testing, cleaning lubrication, adjustment, calibration and part or component replacement and programming as required completing the service call repair.

5.14 Service Orders: Service Orders (SO) will be used for CM services not covered in the PM portion of the contract as indicated in the TO PWS. Ordering Officers (OO) may be appointed by the KO at the TO level and are authorized to approve SOs at or below their designated threshold. Contractors will be provided a copy of the OO appointment letter as applicable. The Contractor must ensure that they do not accept work above the OO's authority. All other SOs require approval by the KO. The Contractor will normally prepare and submit a SO to the designated Government representative for routing and/or approval. The SO will describe the work to be performed, associated cost, and all required backup documentation. Upon approval, the contractor shall perform the work described on the SO.

5.15 Record Keeping: The Contractor shall keep records/logs/checklists of all PM inspections that are performed that track the following at a minimum: date and time of inspection, asset name, asset tag information, locations, work performed, any parts replaced, and if there are any corrective issues required from the inspection. The log shall be maintained for all required system devices, equipment, sub-systems, and components. Complete logs shall be kept and be available for inspection on site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the equipment itemized in the TO.

5.16 Specific task areas or functions that may be performed are listed below. All tasks are to be performed IAW the requirements of the specifications, drawings, original manufacturer's published procedures (if applicable), and CDRLs.

5.16.1 Perform site surveys, develop technical recommendations including assessment of existing equipment, identification and validation of problems and deficiencies, and provide repair/replacement/modernization recommendations.

5.16.2 The contractor must have sufficient spare parts or access to spare parts to meet TO delivery requirements.

5.16.3 Maintain, and update as necessary, accurate as-built drawings of the system.

5.16.4 Repair, maintain, and update systems, including associated data transmissions systems. Contractor shall comply with all requirements of the NEC, or its equivalent authority related to installation of new data transmission equipment and systems.

5.16.5 Provide, populate and maintain computerized maintenance management software system, including the generation of work tickets for maintenance activities.

5.16.6 Provide central monitoring services, including associated facilities, equipment, appurtenances and trained monitoring personnel for the service of remotely monitoring alarm systems and taking actions as appropriate. This service may require a facility that is always staffed and in operation.

PART 6
APPLICABLE PUBLICATIONS

6.1 All technical and programmatic work performed under this contract and its TOs shall comply with the applicable criteria issued by DoD, Department of the Army, and other Government Agencies within and outside DoD. The criteria documents issued by the Corps of Engineers shall be used as the primary criteria unless alternate, additional or supplementary criteria is stated in the individual TO. Applicable regulations issued by the Department of the

Army with associated DoD issued policy and Department of Defense Instructions (DoDI), and/or Department of Defense Directives (DoDD) shall be followed. Where these regulations, policy and criteria are applicable to UMCS, ESS or related installation, testing, operation, management, etc., those requirements shall be incorporated. A list of applicable criteria is provided in Section J, Exhibit D.

6.2 Individual TOs will include a list of regulations and criteria documents applicable for survey, analysis, design, and cost estimate preparation.

PART 7
SPECIAL REQUIREMENTS

7.1 In addition to complying with the requirements outlined in RFO Part 22.13, RFO Clause 52.222-35, RFO Clause 52.222-37, DFARS 222.13 and Department of Labor regulations, USACE contractors and subcontractors at all tiers are encouraged to promote the training and employment of U.S. veterans while performing under the resultant contract. USACE contractors are encouraged to seek out highly qualified veterans to perform services under this contract. The following resources are available to assist USACE contractors in their outreach efforts:

Federal Veteran employment information at https://www.opm.gov/fedshirevets/
Department of Labor Veterans Employment Assistance https://www.dol.gov/agencies/vets
Department of Veterans Affairs- VOW to Hire Heroes Act https://www.benefits.va.gov/vow/
Army Wounded Warrior Program- https://www.army.mil/article/4245/army_wounded_warrior_program_aw2
U.S. Chamber of Commerce Foundation-Hiring Our Heroes
https://www.uschamberfoundation.org/solutions/workforce-development-and-training/hiring-our-heroes

PART 8
ANTITERRORISM (AT) REQUIREMENTS

8.1. General security requirements and guidance: The security requirements described below apply to all contract personnel (including employees of the prime Contractor ("Contractor") and all subcontractor employees) supporting the performance requirements of this contract. The Contractor is responsible for compliance with these security requirements. Questions regarding security matters shall be addressed to the designated Government representative (e.g., Contracting Officer Representative (COR), Requiring Activity (RA) representative, or Contracting Officer (if a COR or other RA representative is not appointed)). Contract personnel are critical to the overall security and safety of US Army Corps of Engineers (USACE) installations, facilities and activities, and security awareness training contributes to those efforts. The Department of Defense (DoD) and Army security training requirements specified below, if applicable, are performance requirements; all applicable contract personnel shall complete initial training within 30 days of contract award or the date new contract personnel begin performance on the contract. Within five business days from the completion of training, the Contractor shall provide written documentation (e.g., email or memorandum) to the Government representative. The documentation shall include the names of contract personnel trained and which training they completed; the Contractor shall maintain training records as part of their contract files and be prepared to provide copies of training certificates to the Government representative. Contractor personnel and vehicles are subject to search when entering federal installations. Additionally, all contract personnel shall comply with Force Protection Condition (FPCON) measures, Random Antiterrorism Measures (commonly referred to as "RAMs"), and Health Protection Condition (HPCON) measures. The Contractor is responsible for meeting performance requirements during elevated FPCON and/or HPCON levels in accordance with applicable RA plans and procedures—this includes identifying mission essential and non-mission essential personnel. In addition to the changes otherwise authorized by the changes clause of this contract, should the FPCON or HPCON levels at any individual facility or installation change, the Government may implement security changes that affect contract personnel. The Contractor shall ensure all contract personnel are aware of their security responsibilities, including any site-specific requirements identified in local policies or procedures.

8.2. Antiterrorism (AT) Level I training: All contract personnel requiring routine access to Army installations, facilities, and controlled access areas, or requiring network access shall complete initial and annual refresher AT

Level I awareness training. Online AT Level I awareness training is available at https://jko.jten.mil/ (website subject to change).

8.3. Physical security and access control requirements: All contract personnel requiring physical access to a federal installation or facility shall comply with the access control procedures of that location. Contract personnel requiring unescorted access to meet contract performance requirements on a DoD installation in the US shall be vetted by the installation/facility Provost Marshal/Directorate of Emergency Services/Security Office using the National Crime Information Center-Interstate Identification Index (commonly referred to as "NCIC-III") and Terrorist Screening Database (commonly referred to as "TSDB"). Contract personnel shall comply with all personal identity verification requirements specified in installation/facility policies and procedures. Contract personnel who do not meet requirements for unescorted access to USACE facilities shall coordinate escorted access with the Government representative, as needed. Contract personnel who receive keys, access cards, or lock combinations that provide access to government-owned property shall comply with key and lock control procedures of the RA.

8.4. Contract personnel requiring a common access card (CAC): Contract personnel will be issued a common access card (CAC) only if duties involve one of the following: (1) both physical access to a DoD facility and access to DoD information systems or networks; (2) remote access to a DoD information system or 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 6 months or more. Before CAC issuance, contract personnel must have, at a minimum, a favorably adjudicated Tier 1 investigation or an equivalent or higher investigation in accordance with applicable Army regulations and Homeland Security Presidential Directive-12 (HSPD-12). At the discretion of the RA, an initial CAC may be issued based on a favorable review of a fingerprint check and a successfully scheduled Tier 1 investigation with the National Background Investigations Bureau. The RA provides contract personnel with additional information and forms to initiate the CAC issuance process, and/or to initiate background investigations, when required. Contract personnel shall complete these processes within established timelines to avoid delays.

8.5. Security requirements for contract performance outside the US: For contract performance requirements that involve services or delivery in a foreign country, the Contractor shall comply with the requirements of DFARS clause 252.225-7963, as applicable. For performance requirements that involve contract personnel accompanying or supporting US Armed Forces deployed outside the US, the Contractor shall comply with the requirements of DFARS clause 252.225-7040, as applicable. Contract personnel accessing DoD or other federal facilities outside the US shall comply with applicable Status of Forces Agreements and Geographic Combatant Command requirements. Prior to contract personnel traveling outside the US, the Contractor shall provide documentation of AT, OPSEC, and other required training to the COR, or other RA representatives. Additionally, contract personnel shall comply with travel requirements specified in the DoD Foreign Clearance Guide, including country and theater clearance processes.

8.6. Suspicious Activity Reporting training (e.g. iWATCH, CorpsWatch, or See Something, Say Something): All contract personnel shall receive initial and annual refresher training from the RA representative on the local suspicious activity reporting program. This locally developed training provides contract personnel with general information on suspicious behavior, and guidance on reporting suspicious activity to the project manager, security representative or law enforcement entity.

8.7. Contract personnel requiring access to Government information systems: All contract personnel with access to a government information system (including USACE business systems and CAC-enabled websites) shall comply with applicable DoD and Army regulations and shall use the organization's UserID-Password Administration and Security System (U-PASS) at commencement of services to request network user accounts. Contract personnel shall complete DoD Information Assurance Awareness training prior to accessing information systems, and annually thereafter.

8.8. Contracts requiring a formal OPSEC program: The Contractor shall develop an OPSEC SOP/Plan within 90 days of contract award. The OPSEC SOP/Plan shall be reviewed and accepted by the RA OPSEC Officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it,

and why it needs to be protected. In accordance with Army and DoD regulations, the contractor shall have a certified Level II OPSEC coordinator, who shall ensure OPSEC compliance during contract performance.

8.9. Training requirements for the protection of sensitive information: All contract personnel with access to critical information (as identified in the RA's OPSEC Program) shall complete initial and annual refresher OPSEC Level I Awareness training, which is available at the following websites: https://www.iad.gov/ioss/, or http://www.cdse.edu/catalog/operations-security.html (websites subject to change). All contract personnel with access to Controlled Unclassified Information (CUI) shall complete initial and annual refresher CUI training in accordance with applicable Army policy.

8.9.1. Cybersecurity Maturity Model Certification (CMMC) and CUI-FCI Compliance.

All contract personnel must comply with CMMC requirements, as detailed in the Defense Federal Acquisition Regulations Supplement (DFARS). To enhance the security of information and reduce risk of cyber-attacks the Department of War (DOW) established the CMMC Program, which requires pre-award assessment of information and covered contractor systems against established cybersecurity standards for safeguarding FCI and CUI.

Controlled Unclassified Information (CUI) or Federal Contact Information (FCI) will apply if the contract is available for public release. CUI or FCI will also apply if the contractor is required to have CUI residing in or transitioning through their information system at any time.

Cybersecurity Maturity Model Certification **(**CMMC).

CMMC is not required if CUI and FCI does not apply to this contract, only CMMC Level 1 applies.

CMMC Level 3 (self-certification + C3PAO + DIBCAC) applies if there **is** a Reasonable expectation that the release of the CUI would place National Security or Critical Systems (ex. Nuclear, cyber, missile defense)

CMMC Level 2 (self-certification) applies if there **is not** a Reasonable expectation that the release of the CUI would place National Security or Critical Systems (ex. Nuclear, cyber, missile defense)

CMMC Level 2 (self-certification + C3PAO) applies if any portion of the CUI anticipated in the contract and listed in the "Defense" Category

CMMC Level 2 (self-certification only) applies if no portion of the CUI anticipated in the contract and listed in the "Defense" Category

8.10. Information Assurance (IA)/Information Technology (IT) requirements: All contract personnel performing IA/IT services must comply with DoD training and certification requirements specified in DoD 8140, Information Assurance Workforce Improvement Program. Contract personnel shall provide the Government representative with documentation of requisite certification(s) prior to performing on the contract. In accordance with applicable DoD, Army, and USACE regulations, the Contractor shall ensure that all information systems (IS) and platform information technology (PIT) systems developed and/or supported under this contract comply with cybersecurity and architectural requirements, including, but not limited to: security technical implementation guides (STIG)(e.g., the current version of the Application Security and Development STIG, and the internet access point (IAP) demilitarized zone (DMZ) STIG), and the use of security controls developed under the risk management framework documentation for the system or platform. The Contractor shall address questions regarding these provisions to the Government representative, who will coordinate between the Contractor and the USACE Chief Information Officer (CIO).

8.11. Contracts requiring handling or access to classified information: The prime Contractor shall have a Facility Clearance (FCL) at the appropriate level prior to performance on the contract; the RA will sponsor the prime contract company in obtaining the FCL. All cleared contract personnel shall comply with the FCL requirements, as well as applicable laws and regulations regarding contractor access to national security information. For classified contracts, the RA will generate the DD Form 254, which will be attached to the contract.

8.12. Threat Awareness Reporting Program: All contract personnel who maintain an active security clearance shall receive initial and annual refresher training on the Threat Awareness and Reporting Program (commonly referred to as “TARP”), provided by a Counterintelligence Agent. As determined by the servicing Counterintelligence Agent for the RA, contract personnel may complete web-based TARP training.

8.13. Escorting in classified and/or sensitive areas: In accordance with applicable regulations, all contract personnel who do not possess the appropriate security clearance or access privileges will be escorted in areas where they may be exposed to classified information or operations, sensitive information or activities, or restricted areas.

8.14. Pre-screen candidates using E-Verify Program: Contractors shall comply with the requirements set forth in RFO clause 52.222-54 Employment Eligibility Verification and RFO Subpart 22.18 in using the E-Verify Program at (https://www.e-verify.gov/) (website subject to change) to meet the contract employment eligibility requirements. Contractors are encouraged to cooperate with Federal and State agencies responsible for enforcing labor requirements to include eligibility for employment under United States immigration laws in accordance with RFO 22.1802-1. An initial list of verified/eligible candidates shall be provided to the COR no later than three business days after the initial contract award. When contracts are with individuals, the individuals will be required to complete a Form I-9, Employment Eligibility Verification, and submit it to the Contracting Officer to become part of the official contract file.

8.15. Contracts requiring armed security guards: All contract personnel performing contract security guard duties shall comply with the Individual Reliability Program in accordance with AR 190-56 (The Army Civilian Police and Security Guard Program), as well as applicable installation, facility and area commander installation/facility policies and procedures regarding storing weapons and ammunition in accordance with AR 190-11 (Physical Security of Arms Ammunition, and Explosives).

8.16. Contracts requiring delivery of food and water: The supplies delivered under this contract shall be transported in delivery conveyances maintained to prevent tampering with and/or adulteration or contamination of the supplies, and if applicable, equipped to maintain a prescribed temperature. All delivery vehicles and storage locations are subject to inspection at any time by the COR, Post Veterinarian, law enforcement officers, or other RA representatives authorized to conduct such inspections. When the sanitary conditions of the delivery conveyance have led, or may lead to product contamination, adulteration, constitute a health hazard, the delivery conveyance is not equipped to maintain prescribed temperatures, or the transport results in product “unfit for intended purpose,” supplies tendered for acceptance may be rejected without further inspection. As the holder of a contract with the DoD, the Contractor shall ensure that all products and/or packaging have not been tampered with or contaminated. The Contractor shall ensure all delivery conveyances are always locked or sealed, except when actively loading or unloading. Unsecured vehicles shall not be left unattended. All incoming truck drivers shall provide adequate identification upon request. In the event of an identified threat to a delivery location, or a heightened force protection/Homeland Security threat level, the Contractor may be required to adjust delivery routes to minimize vulnerability risks and enable direct delivery to DoD facilities.

The Requiring Activities (RA) ATO must complete the AT/OPSEC coversheet to ensure the security language is suitable for the supporting organization and location. Additional security requirements may be delineated in individual task orders. Other security practitioners may develop additional security-related language to be included in the requirements document based on the current security posture or threat environment.

APPENDIX A

1.0 Performance Requirements Summary (PRS): Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. All performance objectives listed in the table may not apply to the specific project being performed. A project specific PRS will be included in the PWS at the TO level.

Procurement and Installation Performance Requirements Summary			
Performance Objective	PWS Ref Level (plus all other applicable areas)	Acceptable Performance Level (Standard)	Performance Threshold
1. Zero reportable safety incidents	Specified at TO level	In accordance with EM 385-1-1 and all applicable OSHA regulations	Zero reportable incidents
2. Complete Performance Verification Test (PVT)	Specified at TO level	In accordance with PWS requirements and applicable UFGS	First-time pass without significant punch-list items
3. Preparation and submittal of all applicable technical deliverables	Specified at TO level	In accordance with applicable UFGS, UFCs, and PWS requirements	On time delivery within Project Schedule and "A" or "B" grade in CMP
4. Submittal of security engineering and cybersecurity documentation	Specified at TO level	Meets requirements established in PWS	Minimal defects
5. Adherence to accepted project schedule	Specified at TO level	Within established contract period of performance	No more than 2 percent variance from critical path
6. Preparation and submittal of all non-technical deliverables to include contract compliance documentation	Specified at TO level	In accordance with contract deliverable table in PWS	Meet all contract reporting requirements

Maintenance and Service Performance Requirements Summary			
Performance Objective	PWS Ref Level (plus all other applicable areas)	Acceptable Performance Level (Standard)	Performance Threshold
1. Zero reportable safety incidents	Specified at TO level	In accordance with EM 385-1-1 and all applicable OSHA regulations	Zero reportable incidents
2. Quality and Timeliness of Deliverables	Specified at TO level	As outlined in the PWS.	90% compliance, Zero Deviation
3. Project Schedule	Specified at TO level	Within established period of performance	No more than 2 percent variance from critical path

4. Perform Preventive Maintenance	Specified at TO level	System is maintained IAW the PM schedule, and such that the systems are continuous and reliable.	95% Compliance
5. Perform Corrective Maintenance	Specified at TO level	System is repaired IAW PWS response times and procedures such that the systems are continuous and reliable.	95% Compliance

1.1 Types of Surveillance to select from:

1.1.1 Random Sampling: Appropriate for frequently recurring tasks. Evaluate randomly selected samples of the lot to determine the acceptability of the entire lot.

1.1.2 100 Percent Inspection: Appropriate for tasks that occur infrequently. Inspect and evaluate performance each time task is performed

1.1.3 Periodic Surveillance: Evaluation of samples selected on other than 100% or statistically random basis (52.246-4), i.e. monthly, quarterly, semi-annually etc.

1.1.4 Customer Feedback: A method carried out by soliciting customer/end user satisfaction of technical services performed by the Contractor.

1.2 Incentives: If contractor performance meets or exceeds contractual requirements.

1.2.1 Positive Past Performance evaluation rating within the Contractor Performance Assessment Reporting System (CPARS).

1.2.2 Favorable consideration for continued service through contract option exercise (if applicable).

1.3 Consequences: Potential Government remedies for not meeting performance thresholds on a firm fixed price TO:

1.3.1 Government increasing the surveillance method that is stated in the QASP.

1.3.2 Possible Termination for Default.

1.3.3 Negative Past Performance evaluation rating within the Contractor Performance Assessment Reporting System (CPARS).

1.3.4 Unfavorable consideration for continued service through not exercising the next contract option(s) (if applicable).

1.3.5 Government remedies identified in the services and/or construction clauses identified in the contract.

APPENDIX B
QUALIFICATION OF CONTRACTOR PERSONNEL

Program Manager
The Program Manager (PgM) shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. Typical seven to ten (7 - 10) years relevant experience in the UMCS/ESS/FAS/SCADA technology field, including five (5) years of experience in a management or supervisory capacity and five (5) years in the functional area of the program to be managed. PgM proposed shall have a bachelor's degree in engineering or business from an accredited university or college, or a related field, or in the project's functional area.

Project Manager
Responsible for planning and executing major portions of the project. Prepares and maintains the project scope, schedule, and budget. Primary point of contact for the customer on assigned tasks. Oversees all work and takes corrective action as necessary to ensure success of assigned tasks. Manages staffing, budget, prioritization, and other personnel matters. May serve as technical lead for assigned tasks. Experience with Government or industry processes, procedures, standards, methodologies, or tools as relative to the assignment. Five (5) years' experience in the project management field plus demonstrated experience in the project's functional area. Bachelor's degree from an accredited university or college. PMP certification preferred.

Contracts Manager
Shall have the full authority as a Company representative in all matters relating to contracts to include but not limited to contracts negotiations, modifications, and proposal submittals. The person proposed shall have ten (10) years' experience in the contracting field, including five (5) years of experience in a management level capacity. The person proposed shall have a bachelor's degree in business from an accredited university or college, or a related field, or in the project's functional area.

Quality Control Manager
Typical seven to ten (7 - 10) years' relevant experience in the quality control field, including five (5) years' experience as a Quality Control Manager. The person proposed shall have a bachelor's degree from an accredited university or college, in a related field, or in the project's functional area.

Fire Protection Engineer
Will represent the company with fire alarm system engineering products and solutions and the adherence to applicable codes. Provides Professional Engineering Stamp for fire alarm systems. The person proposed shall have ten (10) years' experience in the Fire Protection engineering field, including five (5) years in the functional area of the project to be managed. Must have a U.S. Professional Engineers certification. The person proposed shall have a bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area.

Site Superintendent
Provides site wide management of personnel for routine activities according to established procedures or instructions. Complies with the standards and organizational requirements relative to specific assignments. Five (5) years of experience related to specific heating ventilation and air conditioning experience with associated controls. Experience with Government or industry processes, procedures, standards, methodologies, or tools as relative to the assignment. High School diploma, plus technical training in field related to task assignment.

HVAC Technician
Provides support for HVAC/Controls activities according to established procedures or instructions. Works independently to assist with technical support for elements such as: complex processes, structural elements, electric/electrical/electronic components, equipment, applications, systems, software, networks, satellites, telecommunications, facilities, or machinery. Complies with the standards and organizational requirements relative to specific assignments. Five (5) years of experience related to specific heating ventilation and air conditioning experience with associated controls. Experience with Government or industry processes, procedures, standards,

methodologies, or tools as relative to the assignment. High School diploma, plus technical training in field related to task assignment.

Senior Security System Engineer (SSSE)
The Senior SSE is responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within CE (computing environment), NE (network environment), and/or enclave environments. Must meet the DoDD 8140 "Information Assurance Training, Certification, and Workforce Management" and DoD 8140 "Information Assurance Workforce Improvement Program" requirements for Information Assurance Manager (IAM) Level 3 and Information Assurance Technical (IAT) (Information Assurance Technical) Level 3, or Information Assurance System Architect and Engineer (IASAE) Level 3.

Security System Engineer (SSE)
The SSE is responsible for the design, development, implementation, and/or integration of a DOD IA architecture, system, or system component for use within CE (computing environment), NE (network environment), and/or enclave environments in support of higher-ranking IA professionals. Must meet the DoDD 8140 "Information Assurance Training, Certification, and Workforce Management" and DoDD 8140 "Information Assurance Workforce Improvement Program" requirements for IAM Level 1 or 2, and IAT Level 1 or 2, OR IASAE Level 1 or 2.

Senior Electrical/Mechanical Engineer
Will represent the company with engineering products and solutions. The person proposed shall have ten (10) years' experience in the Electrical/Mechanical engineering field, including five (5) years in the functional area of the project to be managed. The person proposed shall have a bachelor's degree in engineering from an accredited university or college. Must have a Professional Engineers certification.

Electrical/Mechanical Engineer
Will provide mechanical/electrical engineering products and solutions. Five (5) years' experience in the Electrical/Mechanical engineering field, including three (3) years demonstrated experience in the functional area. Bachelor's degree in engineering from an accredited university or college.

Senior Electronic Security Engineer
Will represent the company with electronic security system engineering products and solutions. The person proposed shall have ten (10) years' experience in the electronic systems/information technology field and demonstrated experience in the project's functional area. The person proposed shall have a bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area. Must have a Professional Engineers certification.

Electronic Security Engineer
Will represent the company with electronic security system engineering products and solutions. The person proposed shall have five (5) years' experience in the electronic systems/information technology field and demonstrated experience in the project's functional area. The person proposed shall have a bachelor's degree in engineering from an accredited university or college, or a related field, or in the project's functional area.

Network Specialist
Responsible for the design, implementation, and defense of the network. Must meet the Department of Defense Directive (DoDD) 8140 "Information Assurance Training, Certification, and Workforce Management" and DoD 8140 "Information Assurance Workforce Improvement Program" requirements for IAT (Information Assurance Technical) Level 1 or 2, OR IASAE (Information Assurance System Architect and Engineer) Level 1 or 2 OR meet the requirements for any type of Computer Network Defense (CND) professional (CND-A, CND-IS, CND-IR, CND-AU) mentioned in the aforementioned regulations.