AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGES
U	1		3

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER *(If applicable)*
P00023	07/28/2022	H912699318A064001	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE	SCD
NAVSUP FLC Norfolk, Detachment Philadelphia 700 Robbins Avenue, Bldg. 2B Philadelphia, PA 19111-5083	N00189	DCMA HAMPTON 2128 Pershing Avenue Fort Eustis, VA 23604	S5111A	C

8. NAME AND ADDRESS OF CONTRACTOR *(Number, street, county, State and ZIP Code)*

MYMIC, LLC
1040 University Blvd, Suite 100
Portsmouth, Virginia 23703-2650

CODE 1TPC7 FACILITY CODE 005677419

(X) ☐ 9A. AMENDMENT OF SOLICITATION NUMBER

9B. DATED *(SEE ITEM 11)*

☒ 10A. MODIFICATION OF CONTRACT/ORDER NUMBER
N00178-14-D-7846/N0018919F3001

10B. DATED *(SEE ITEM 13)*
12/17/2018

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

SEE SECTION G

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	
☐	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☒	D. OTHER *(Specify type of modification and authority)* Pursuant to FAR 52.232-22, the purpose of this modification is to provide incremental funding.

E. IMPORTANT: Contractor ☒ is not ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (*Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

SEE PAGE 2

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
		Ivan Varela , Contracting Officer	
15B. CONTRACTOR/OFFEROR *(Signature of person authorized to sign)*	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA /s/Ivan Varela *(Signature of Contracting Officer)*	16C. DATE SIGNED 07/28/2022

Section C - Description/Specifications/Statement of Work

PERFORMANCE-BASEDWORKSTATEMENT(PBWS)

Directorate of Management

Information Technology and Knowledge Engineering Support (IT/KE) Task Order

1.0 INTRODUCTION.

The mission of Directorate of Management (DOM) is to serve the Chairman of the Joint Chiefs of Staff (CJCS), providing the best military advice. On behalf of the Director, the mission of the DOM is to lead, advocate, or enable the effective and efficient development of IT capabilities in support of the Joint Staff mission while complying with applicable federal laws and DoD Regulations.

2.0 BACKGROUND.

The DOM is responsible for providing assistance to the Chairman of the Joint Chiefs of Staff and Joint Staff through management, planning and direction of support activities including correspondence administration, budget and finance, action management and archiving, information technology, services, resources and all aspects of staff and information security.

3.0 OBJECTIVE & SCOPE.

The contractor shall provide non-personal services to support the DOM mission in three key functional areas: Knowledge Engineering, Information Technology Support, and Information Technology (IT) Project Management.

Knowledge Engineering (KE). The DOM provides technology synergy and requirements assistance to the Directorates, Senior Leadership, and the National Military Command Center via a team of embedded or centrally managed Knowledge Engineers. The team enables synergy by integrating requirements, initiatives, and developments to leverage JS knowledge and information to facilitate the JS decision-making process. The places of performance for the Knowledge Engineers will be NCR, HR, and Site R.

Information Technology Support (ITS). The Joint Staff has outsourced IT and network service to external organizations. The Information Technology Support team serves as the advocate to these external service providers for the Joint Staff users. The ITS team will actively

monitor trouble ticket queues and identify languishing tickets that need action on by the service providers. Additionally, the ITS team will connect and configure Joint Worldwide Intelligence Communications System (JWICS) end user devices such as thin clients, Top Secret Voice Over Internet phones, and printers. The places of performance for the Information Technology specialists will be NCR and HR.

Information Technology (IT) Project Management. The DOM/CRD provides IT project management assistance to the Directorates, Senior Leadership, and the National Military Command Center via a team of centrally managed Project Managers. The team will be TS/SCI eligible and complete projects execution using guidance from the Project Management Body of Knowledge (PMBOK), and by providing IT technical analysis and oversight to ensure successful delivery from external service providers. The places of performance and approximate workloads for the Project Managers will be NCR (70%), HR (25%), and Site R (5%).

-

4.0 APPLICABLE DOCUMENTS.

Each of the applicable documents contains information that is pertinent to KE, IT, IT PM, and eDTRM.

JSI 8000.01, Joint Staff Chief Information Officer

DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program

PMBOK® (current version), “Project Management Body of Knowledge”

CJCSI 5124.01, Charter of the Knowledge Management Cross-Functional Team (KMCFT)

CJCSI 5124.01, "Charter of the Knowledge Management Cross-Functional Team"

JSM 5762.01 Series, "Joint Staff Portal Governance"

JSI 5761.01 Series, "Joint Staff Content Management Policy"

DJSM 0610-06, "Enterprise Content Management Working Group (CMWG)

DJSM 0348-12, "Official Networks of Record - Joint Staff Information Networks"

DoD Instruction 8220.Ac "Knowledge Management (KM) For The DoD"

Committee on National Security Systems Instruction Number 4009, "National Information Assurance Glossary," April 6, 2015

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014 DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016

DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015

DoD Instruction 8110.01, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD," November 25, 2014

DoD Instruction 8320.02, "Sharing Data, Information, and Technology (IT) Services in the Department of Defense," August 5, 2013

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015

Federal Chief Information Office Council, "2012 Clinger-Cohen Core Competencies and Learning Objectives," December 2012

"Department of Defense Dictionary of Military and Associated Terms," current edition

Office of the Deputy Secretary of Defense, "Department of Defense Information Resources Management Strategic Plan," April 1, 2015

Office of Management and Budget, "The Common Approach to Federal Enterprise Architecture," version 2, May 2, 20122

Office of Personnel Management, "Data Standards for the Cybersecurity Category/Specialty Area," December 1, 2016

Office of the DoD Chief Information Officer, "Department of Defense (DoD) Chief Information Officer (CIO) Campaign Plan," November 19, 2012

Office of the DoD Chief Information Officer, "DoD Enterprise Service Management Framework," edition III, March 4, 2016

5.0 REQUIREMENTS.

The Contractor shall provide a broad spectrum of non-personal services support which enable the Joint Staff to successfully execute the DOM IT support services mission. These requirements include:

5.1 Contractors shall continually provide situational awareness to the Government through effective communication and a combination of the following 5.1 sub-tasks: The Program Manager overseeing these tasks will have a Masters of Science degree in a technical or management discipline from an accredited college or university with a minimum of seven (7) years of below task related experience to include a minimum of five (5) years managing complex projects involving large numbers of people in subordinate groups; OR a Bachelor's degree in a technical or management discipline from an accredited college or university with a minimum of fifteen (15) years of below task related experience managing progressively more complex systems / projects involving large numbers of people in subordinate groups.

5.1.1 Post Award Conference. The Contractor shall attend the Post-Award conference convened by the Government. This conference is the first opportunity for the Government and contractor to meet and review contract requirements, terms, and conditions. It also serves as an opportunity for Government and contractor to discuss and clarify roles and responsibilities.

5.1.2 Periodic Progress Meetings. The Contracting Officer's Representative (COR), Technical Assistant (TA), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the COR will apprise the Contractor of how the Government views the Contractor's performance. The Contractor will apprise the Government of services performed and any problems experienced in supporting contract requirements. The COR will provide guidance to the contractor on actions required to resolve issues regarding contract performance.

5.1.3 Contractor Quality Control Plan (QCP). The Contractor shall develop an effective quality control plan to ensure services are performed in accordance with this task order and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program (QCP) assures the work performed complies with the requirement of the contract. After acceptance of the quality control plan the Contractor will receive the contracting officer's acceptance in writing of any proposed change to the QC system.

5.1.4 Monthly Status Report. The contractor will provide the COR and TA with a task order Monthly Status Report (MSR), Contractors Progress, Status and Management Report (contractor format acceptable) [FJCNFN1] by email. The format for the MSR will be proposed by the Contractor and agreed to by the Government and subject to change if required by the Government. The MSR will include the following at a minimum:

- Contractor's name and address
- Contract TO number
- Date of report
- Period covered by report
- Man-hours expended during the reporting period, and cumulatively for the TO
- Cost incurred for the reporting period and cumulatively for the task
- Description of progress made during the period, including any problems encountered
- Recommendations, if any for solution beyond the scope for the task area
- Results obtained in resolving previously reported problem areas
- Trips and significant results
- Plans for activities during the following period, including any outages, software updates
- Projected travel requirements and costs
- Summary of actual and projected costs for labor hours and travel for the entire period of performance
- Projection ahead 6 calendar months of scheduled, required, and executed labor and travel for each event and exercise. Forecast quarterly the level of effort for assigned exercises by functional areas, events, and non-event areas
- Summarize labor hours and travel funds expenditures by resource band and, to include total billed hours burdened cost, and travel, planned activities, any key personnel changes, and any shortfalls, issues or problems
- Completion of "required or mandatory" government training
- Meetings with The Joint Staff's IT Service Provider (JSP)

5.1.6 Data Rights. The Government has unlimited data rights on all information developed or delivered under this TO.

5.1.7 Release of Information. Project related documentation developed in support of this task order is not publicly releasable and shall be marked with the appropriate distribution statement as directed by the Government. The Contractor shall not release any project related material without the written permission from the COR.

5.1.8 Identification of Contractor Employees. All Contractor personnel working in situations where their Contractor status is not obvious to other 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.

5.1.9 Non-Disclosure. In the course of performance pursuant to this contract, the contractor may have access to nonpublic information, including Planning, Programming, Budgeting and Execution (PPBE) information. The Contractor agrees that it will not use or disclose any such information unless authorized in writing by the COR. The Contractor further agrees that it will use its best efforts to ensure that its employees and others performing services under this contract will not use or disclose any such information unless authorized by the COR. To that end, Contractor agrees that each of its employees and others performing duties under this task order will sign a Certificate of Non-disclosure. The Contractor also agrees to maintain an updated list of Contractor employees with certificates of non-disclosure at all times during the execution of this task order.

5.1.10 Travel. The Government expects some travel requirements with this task order. The Government's estimate of travel for this task order is $7,000.00. Detailed travel projections can be found in section 11.0 of this PBWS.

5.2 Contractors shall provide **Knowledge Engineering** mission requirements support to the DD CIO/ITS through a combination of the following 5.2 sub-tasks. The tasks in Section 5.2 require 50% of the personnel to have a TS/SCI clearance and the remaining personnel to have a TS clearance. The lead KE is required to have a Microsoft Certified: Power Platform Solution Architect Associate certification. All other KEs should have experience utilizing these tools and applications as well. All Senior level KEs will have a Master of Science degree from an accredited college in Engineering or Computer Science with a minimum of five (5) years of below task related experience, or a Bachelor's degree from an accredited college in Engineering or Computer Science with a minimum of five (5) years of below task related experience. Junior level KEs will have a Bachelor's degree from an accredited college in Engineering or Computer Science with a minimum of two (2) years of below task related experience.

5.2.1 Joint Staff Information Environment Assessment – the contractor shall continually assess the Joint Staff Information Environment and recommend improvements using IT and collaborative tools to allow JS leaders to better leverage the JS knowledge and make timely, informed decisions (Rev 1 / Medium Priority)

5.2.1.1 Reserved

5.2.1.2 The contractor shall conduct technical analysis (independently and the direction of the government) to enable data driven decisions to identify options or to validate courses of action in development and execution of Enterprise level services. (Rev 1 / Medium Priority)

5.2.1.3 The contractor shall provide data supported recommendations on Directorate proposed IT requirements, to include utility, integration and supportability of applications within the Enterprise and the Joint Information Environment (JIE). (Rev 1 / Medium Priority)

5.2.2 Portal and Collaborative Tool Development and Support – Joint Staff's primary means of sharing information is through Sharepoint-based portals on NIPR and SIPR. The objective is to develop smart, consolidated, and aligned IT solutions across the Joint Staff and to provide problem resolution and mission-oriented customer technical interface.

5.2.2.1 The contractor shall develop SharePoint and Knowledge Management tools based in support of user requirements. (Rev 1 / High Priority)

5.2.2.2 Reserved

5.2.2.3 The contractor shall develop workflows to streamline Joint Staff business processes (Rev 1 / High Priority)

5.2.2.4 Reserved

5.2.2.5 The contractor shall create, maintain, archive and present metrics in support of Joint Staff Knowledge Management transformation and process improvement efforts (Rev 1 / Medium Priority)

5.2.2.6 The contractor shall provide support to transition to newer KM/collaborative tool platforms and, if required, support transition/moving data to Enterprise hosted sites. (Rev 1 / High Priority)

5.2.2.7 The contractor shall keep the customer abreast of status, resolve issues as needed and facilitate solutions using enterprise IT capabilities and ensure services are aligned with the JS enterprise architecture, interoperable

services and network centric enterprise services. (Rev 1 / High Priority)

5.2.2.8 The contractor shall provide recommendations and input in the development and/or update of Joint Staff Knowledge Management Directives (Rev 1 / Medium Priority)

5.2.3 User support

5.2.3.1 The contractor shall provide 24/7 support to the NMCC/NJOIC and Joint Staff Crisis Management Team for real world events as well as exercises. The contractor shall assist in standing up and tearing down the Crisis Management Team (CMT) collaborative tools in preparation for exercises and actual events with on-site (2) hour response during CMT activation/operations. (Rev 1 / High Priority)

5.2.3.2 The contractor shall provide support to Site R as necessary on an as-needed basis (during exercises and other events). (Rev 1 / High Priority)

5.2.3.3 The contractor shall provide on-site 24 hour response time to the assignment of Directorate KE requirements once input into the established "KE task/project tracker". (Rev 1 / High Priority)

5.2.3.4 The contractor shall provide dedicated support to the Joint Staff Top 7 senior leaders and the National Military Command Center (NMCC) and the National Joint Operations and Intelligence Center (NJOIC). (Rev 1 / High Priority)

5.2.3.5 The contractor shall develop training resources to assist Joint Staff Users and Site Owners fully leverage the implementation of Knowledge Management tools. (Rev 1 / Medium Priority)

Rev 1 / – Priority Matrix –

Priority	Risk Tolerance
High	High risk, must do. Government will prioritize with contractor (when needed).
Medium	Willing to accept some risk with possible delays in timelines
Low	Willing to accept risk of delays in timelines or inability to support within requested timeline

5.3 The contractors shall provide **Information Technology Support** for DD CIO/ITS mission requirements through accomplishment of the following 5.3 sub-tasks. The tasks in Section 5.3 require a TS/SCI clearance and a DoDI 8570.01M (IAT Level II) certification. Additionally, all personnel supporting this task will have a Bachelor's degree from an accredited college or university in a curriculum or career field of study in Computer Science or Information Systems with a minimum of 3 years of below task related experience; OR an Associate's degree from an accredited college or university in a curriculum or career field of study in Computer Science or Information Systems with a minimum of 3 years of below task related experience.

5.3.1 IT Issue Resolution: The contractor shall monitor existing Joint Staff NIPR, SIPR, and JWICS ticket queues. The contractor shall

assess, track, monitor, and escalate trouble tickets for incidents and problem resolution and verify with the customer when the incident/problem has been resolved within the specified time frame.

5.3.1.1 The contractor shall be required to do both morning and afternoon IT wellness checks across the J-Directorates. The contractor shall identify IT issues and elevate the issues to the appropriate service provider.

5.3.1.2 The contractor shall assist in the development, testing and implementation of a business process for validating IT service request completion

5.3.1.3 Independently and at the direction of the Government , the contractor shall provide technical trend analysis from available data sources to identify performance metrics that will enhance operational performance.

5.3.1.4 The contractor shall monitor, assess, and track service provider’s authorized service interruptions (ASIs) and advise the government on user impact during the ASI.

5.3.1.5 The contractor shall providedaily, weekly, monthly updates to users with open tickets

5.3.2 IT Requirements Support: The contractor shall assist in the development and validation of IT requirements

5.3.2.1 The contractor shall aid the Joint Staff Directorate IT Validators (J-Dir Validators) in the creation, refinement, submission, and validation of user IT requirements

5.3.2.2 The contractor assist in bi-weekly reviews of open IT requirements

5.3.3 Strategic Communications: The contractor shall support the delivery of DD CIO/ITS strategic communications to the JS users.

5.3.3.1 The contractor shall conduct face-to-face communications with users during the wellness checks to reinforce DD CIO/ITS strategic communications

5.3.3.2 As directed by the government, the contractor shall assist the DD CIO/ITS collect required information from JS users in order to complete tasked requests for information.

5.3.4 JWICS Installation Support: The contractor shall support the installation of JWICS end user devices

5.3.4.1 The contractor shall install and configure JWICS end user devices to include workstations, Top Secret Voice Over Internet Phones, printers, and desktop video teleconferencing systems.

5.3.4.2 The contactor shall support office moves through the removal, transport, and reinstallation of JWICS end user devices

5.3.4.3 The contractor shall dispose of end-of-life JWICS end user devices in accordance with security regulations

5.4 The contractor shall provide **Information Technology (IT) Project Management Support** for DD CIO/ITS mission requirements through accomplishment of the following 5.4 sub-tasks. The tasks in Section 5.4 require a TS/SCI clearance, and the Lead Project Manager must have a Bachelor's degree from an accredited college in Project Management or a related field, be Project Management Professional (PMP) certified with experience as a team lead with a minimum of five (5) years of below task related experience. All other Project Managers will have a Bachelor's degree from an accredited college in Project Management or a related field, significant experience working on Project Management Teams, be familiar with the Project Management Body of Knowledge (PMBOK®), and have a minimum of two (2) years of below task related experience.

5.4.1 Project Management: The Contractor shall support and assist overall government management of IT projects and IT requirements analysis, including cost, schedule, and capabilities. The Lead Project manager must be Project Management Professional (PMP) certified, with experience as a team lead.

5.4.1.1 The Contractor shall be responsible for all aspects of project management per the PMBOK®.

5.4.1.2 The Contractor shall establish and implement project management best practices to ensure all projects have well-defined requirements and deliverables. The Contractor will establish an effective means of creating plans of actions and milestones include decision points for correction, go/no-go decisions and identify a means of tracking progress.

5.4.1.3 The Contractor shall possess a complete understanding and have extensive experience in IT Project Management. This in-depth knowledge shall support the JS with refining and improving the overall value of the project management program for the JS.

5.4.2 Project Coordination: The Contractor shall liase with Service Providers to ensure delivery of externally provided services. External Service Providers include US European Command, US Central Command, Defense Information Systems Agency (DISA), Joint Service Provider (JSP), Defense Intelligence Agency, 114th Signal Battalion, 844th Communications Squadron, et al.

5.4.2.1 The Contractor shall be responsible for Project After Action Reports to ensure any deviations from process are documented and other team members are apprised.

5.4.2.2 The Contractor shall proactively coordinate with Project Management Branch government leaders and personnel to assist with overall quality management, efficiency and effectiveness of DD CIO/ITS Project Management.

5.4.2.3 The Contractor shall support government development of JS IT PM policies as well as documentation of IT PM procedures. Lead efforts to develop PM Standard Operating Procedures (SOPs) for IT projects.

6.0 PRODUCT DELIVERY.

The contractor shall provide all PBWS deliverables identified in Table 1 and those required by the J6 MAC contract. Deliver all required products in an electronic format, unless otherwise directed. Deliverables and document drafts will be delivered to the COR, TA or designated government official for comments in a Government approved Contractor format. Deliverables are subject to Government review and, if warranted, may be returned to the Contractor for revision. The Government will have five (5) working days to provide comments. Upon receipt of comments, the Contractor will provide the final product five (5) working days after receipt. Status on all deliverables to include metric adherence is required for inclusion in the MSR.

6.1 All deliverables become the property of the United States Government. All product deliverables will be delivered electronically to the Technical Assistant (TA), COR or designated government official.

6.1.1:

Contracting Officer's Representative (COR):

Mr. William T. Staggs, (703) 697-9115, william.t.staggs2.civ@mail.mil

6.1.2: Technical Assistant (TAs):

Lt Col Darris L. Johnson, USAF, JS DOM SJS CRD, Pentagon, Washington DC;

darris.l.johnson4.mil@mail.mil

Table1. Deliverables

#	Deliverable	Description	Due Date	POC
D001	Quality Control Plan-	Procedures to identify, prevent, and ensure non-recurrence of defective services	Within 15 calendar days at the beginning of the PoP.	TA and COR

	Ref 5.1.3			
D002	Monthly Status Report.	Progress, status, and management report addressing specific accomplishments, man-hour and funds product deliverables, expenditures by function (to include total billed hours burdened cost, and travel), planned activities, any key personnel changes, and any issues and problems requiring the COR's or the Government's attention.	Within 15 calendar days of each month	TA and COR

	Ref. 5.1.4			
D003	Analysis Reports, Information Papers, Information and Decision Briefs. Ref 5.2	Presentation of analysis and assessment work suitable for briefing leadership.	Within 15 days of the analysis, or request of	TA

	– 5.4		the Government	
D004	Meeting Minutes, Discussion Notes, and Project Summaries. Ref 5.2 – 5.4	Accurate capture of meetings, projects and decision discussions	5 days of meeting	TA

7.0 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

In accordance with Federal Acquisition Regulation (FAR) Part 46 of the Federal Acquisition Regulation, Inspection of Services clauses, the purpose of the QASP is to ensure that the Contractor meets the performance standards contained in this task order. This QASP is a living document. Flexibility in the QASP is required to allow for an increase or decrease in the level of surveillance necessary based on Contractor performance. Periodically, the TA and/or COR may provide a copy of the QASP to the Contractor to facilitate open communication. Table 2 is an example of the metrics that will be used to measure satisfactory performance in meeting TO objectives and requirements:

Table2. Quality Assurance Surveillance Plan (QASP)

Performance Rating Element	Performance Objective	Performance Standard	Surveillance Method	Incentive/Disincentive for Meeting or Not Meeting the Acceptable Quality Level
Quality of Product or Service	Submit quality deliverables and products: Slides, Reports, Analysis Reports, Papers, CMD Status Reports.	Deliverables shall be accurate, complete, and in the correct format per direction of government and within samples provided.	COR/TA monitoring and review of products / service.	Acceptable performance of task requires the contractor to meet at a minimum 90% accuracy and completeness with correction to 100% upon identification of deficiencies, executed within COR/TA specified timelines. Ratings input in CPARS for retrieval by

Performance Rating Element	Performance Objective	Performance Standard	Surveillance Method	Incentive/Disincentive for Meeting or Not Meeting the Acceptable Quality Level
				government agencies.
Task Order Deliverables	Meet performance deadlines as defined in Plan of Action and Milestones (POAM). Submit quality deliverables and products: Slides, Analysis Reports, Papers, CMD Status Reports.	Deliverables shall be accurate, timely, complete, and in the correct format per direction of government and within samples provided.	COR/TA monitoring of deliverables and POAM.	Acceptable performance of task requires the contractor to meet at a minimum 90% accuracy and completeness with correction to 100% upon identification of deficiencies, executed within COR/TA specified timelines. Ratings input in CPARS for retrieval by government agencies.
Management and Contract Performance	Coordinate activities to execute the task order.	Professionalinteraction between contractor and gov't officials 90% of time; with reasonable and cooperative behavior in problem identification and corrective actions.	COR/TA monitoring.	Ratings input in CPARS for retrieval by government agencies.
Regulatory Compliance	Obtain/maintain personnel security clearance levels and Joint Staff directed training referenced in PBWS.	100% personnel security levels reported to the COR upon task order award and as required.	COR/TA monitoring.	100% personnel security levels and training requirements maintained throughout the task order period. Ratings input in CPARS for retrieval by government agencies.
Cost Control / Invoicing	Properly manage not-to-exceed labor and other direct costs, and accurate invoicing. All travel pre-approved by COR/TA. All overtime, if authorized, pre-approved.	Labor costs do not exceed normal billable hours per month; and all invoices are 100% correct and submitted on time.	COR/TA monitoring of monthly status reports and invoice. Travel pre-approval. Overtime pre-approved.	Estimates for labor and travel are within acceptable rates as government travelers. No cost overruns; and, any invoice discrepancies are corrected within COR/TA specified timelines. Ratings input in CPARS for retrieval by government agencies.

8.1 Minimum Security Clearance. A Top Secret (TS) minimum security clearance level is required as contractors may require access to Unclassified, Secret, and TS. Minimum TS (interim final) clearance is necessary for all requirements in this task order due to Joint Staff Pentagon office access constraints. Approximately 10 percent will require access to TS/SCI, ACCM, or NC2 data which will require a TS clearance based on an SSBI completed within the last five (5) years with SCI eligibility. Knowledge Engineers supporting specialized information categories in support of the Directorates or NMCC shall possess the appropriate level of clearance and access(s) (i.e. SCI Compartments, COSMIC Top Secret, ACC, etc.) to support the assigned tasks.

8.2 Safeguarding Government Property. The Contractor will be responsible for safeguarding all Government equipment, information and property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials will be properly secured.

8.3 Controlled Unclassified Controls. The Contractor will mark, safeguard, manage, and protect all controlled unclassified and personally identifiable information as required by regulation.

8.4 Classified Material Controls. The Contractor shall mark, safeguard, manage and protect all classified information in accordance with guidance provided in the DD Form 254 (Contract Security Classification Specification)

8.5 Classified Marking Guidance. The Contractor shall comply with the guidance published on the Controlled Access Program Coordination Office (CAPCO) Question and Answer Register.

9.0 EQUIPMENT(GFE)AND MATERIAL:

9.1 Government will furnish the contractors designated to be in the JS spaces with workspace and equipment to accomplish the tasks in this work statement. Apportionment and location of spaces and type of LAN accounts will be provided by the Government. The Government will provide utilities, heating and air-conditioning, and telephone service. Additionally, the Government will provide routine office equipment and a work station and access to suitable networks required to accomplish the task order requirements during the period of this task order. The Government will approve adjustments in the number of workstations as contractor personnel numbers change. Contractor shall comply with JS property management/inventory policies for all Government provided equipment. The Government will provide all supplies and other materials required at the Government site to accomplish the task order requirements.

9.2 In addition to DOM access, contractor will be provided, as required; access to the Joint Staff, other selected combatant commands, Services, and supporting activities.

10.0 PLACE OF PERFORMANCE.

10.1 The work required under this PBWS will primarily be accomplished at the designated Joint Staff facilities in the Pentagon and Hampton Roads. The Contractor may also be required to work at other Government or Contractor sites within the National Capital Region (NCR), Norfolk or Suffolk, VA. Access to the Government's facilities will be coordinated with the Contracting Officer's Representative (COR). The Contractor will travel as required with prior approval of the TA or COR.

11.0 TRAVEL.

11.1 Contractor Travel will be in accordance with the applicable requirements of this PBWS.

11.2 The Government's requirement for Contractor personnel to travel will be within the NCR, Norfolk, VA, Suffolk, VA, and to Site-R. For travel outside of the NCR the Contractor shall coordinate all task order related travel with the COR and provide travel information for compliance with travel policies and requirements. These trips are expected to be of short duration and funded by the Government through the Task Order. Contractor travel is subject to approval of the TA or COR prior to executing any portion of the travel requirement, such as ticket purchases, rental vehicles, and schedules.

11.3 Travel Coordination. The Contractor is responsible for all Contractor travel arrangements associated with this TO. The Contractor will not make arrangements or take any actions on behalf of government personnel, such as room reservations or setting aside blocks of rooms, which may have the appearance of a contractor obligating Government funds.

11.4 KE Travel (Section 5.2 requirements):

Purpose	Location	Duration	Freq	# People
Site R Support	Site R	1 week	As needed	2

11.5 ITS Travel (Section 5.3 requirements):

Purpose	Location	Duration	Freq	# People
User Support	Norfolk/Suffolk	2 days	Monthly	1

11.6 IT PM Travel (Section 5.4 requirements)

Purpose	Location	Duration	Freq	# People
Project Oversight	Site R	1 day	Monthly	1
Project Oversight (Pending Distribution)	Norfolk/Suffolk	1 day	Monthly	1

11.5eDTRM Travel (Section 5.5 requirements):

Purpose	Location	Duration	Freq	# People

11.7 Travel Regulations. The contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitations of funds specified in this task order.

12.0 GOVERNMENTTASKORDERMANAGEMENT

12.1 Contractor Officer's Representative (COR): William T. Staggs, william.t.staggs2.civ@mail.mil

12.2 Technical Assistant (TA):

12.2.1 Lt Col Darris L. Johnson, USAF, JS DOM CRD, Pentagon, Washington DC; darris.l.johnson4.mil@mail.mil

13.0 PERIOD OF PERFORMANCE

13.1 Period of Performance.

Base: 17 December 2018 through 16 December 2019

Option I: 17 December 2019 through 16 December 2020

Option II: 17 December 2020 through 16 December 2021

Option III: 17 December 2021 through 16 December 2022

INVOICE CERTIFICATION – WAWF

See DFARS 252.232-7006 in Section G.

1. The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program.The Contractors supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DOD 8570.01-M, and joint staff regulation, must be completed upon contract award. The Contractor shall meet the applicable information assurance certification requirements, including:

1. DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

1. Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

1. The Contractor will provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

1. Contractor personnel who do not have proper and current certifications will be denied access to DoD information systems for the purpose of performing information assurance functions.

1. GENERAL CONTRACTOR INFORMATION

1. Release of Information.Project-related documentation developed in support of this TO is not publically releasable and marked with the appropriate distribution statement as directed by the Government.

1. Information Assurance Contractor Training and Certification

1. Negligent Discharge of Classified Information (NDCI). When information is placed on or processed on an information system with insufficient security controls to appropriately protect it (e.g., classified data on an unclassified system) there is a potential for an unauthorized disclosure. Such actions will be classified as a security violation, specifically a negligent discharge of classified information or NDCI. Contractors that cause NDCIs during the course of the contract shall be held financially liable for all actual accumulated restoration costs incurred, as described below, but not less than $2,500 per incident.Such costs will be deducted from the contract price, and are not reimbursable.

15.3.1 Restoration costs above $2,500 will be itemized. DISA has developed Classified Message Incident procedures that will be followed in the event of an NDCI by the Contractor. Personally Identifiable Information (PII) incidents fall under this category. This is not an exclusive remedy (e.g., in the case of PII spillage, identity theft or other insurance may be needed to protect the individuals). NDCI Cleanup actions may include server destruction, hard drive wipe and destruction or containment actions.

1. Contractor Situational Awareness.All assigned Contractors are required to review Joint Staff NIPR/SIPR homepage daily for situational awareness of DoD and JS activities.

1. General Contractor Training.All assigned Contractors will complete mandatory JS training as required by the Government.

1. List of acronyms within the TO requirements and deliverables:

Table 3. Acronyms

CFE	Contract Furnished Equipment
CFM	Contract Furnished Material

CIO	Chief Information Officer

CJCS	Chairman of the Joint Chiefs of Staff
COR	Contracting Officer’s Representative

CPARS	Contractor Performance Assessment Reporting System

DISA	Defense Information Systems Administration
DoD	Department of Defense

DoDD	DOD Directive

DoDI	DOD Instruction
eDTRM	eDocument, Task and Records Management

ERM	Electronic Records Management

GFE	Government Furnished Equipment
GFM	Government Furnished Material

IT	Information Technology

JS	Joint Staff
JSAP	Joint Staff Action Package

JSI	Joint Staff Instruction

JSM	Joint Staff Manual
JSP	Joint Service Provider

JTR	Joint Travel Regulation

KE	Knowledge Engineering
LAN	Local Area Network

MSR	Monthly Status Report

NCR	National Capital Region
NDCI	Negligent Discharge of Classified Information

NMCS	National Military Command System

NIPR/NIPRNET	Non-classified Internet Protocol Router Network
PII	Personally Identifiable Information

PMBOK®	Project Management Body of Knowledge

POP	Period of Performance
PMP	Project Management Professional

QASP	Quality Assurance Surveillance Plan

QC	Quality Control
QCP	Quality Control Plan

SCI	Sensitive Compartmented Information

SIPR/SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure

TA	Technical Assistant

TO	Task Order
TS	Top Secret

WAWF	Wide Area Workflow

Personnel Qualifications (Minimum)

(a) Personnel assigned to or utilized by the Contractor in the performance of this contract shall, as a minimum, meet the experience, educational, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional timely manner.

(b) The Government may review the resumes of Contractor personnel proposed to be assigned at any time to determine whether the contractor has sufficient experience to perform the services of this task order.

(c) If the Ordering Officer questions the qualifications or competence of any person performing under the contract, the burden of proof to sustain that the person is qualified as prescribed herein shall be upon the Contractor.

(d) The Contractor must have the personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in delivery orders. The work history of each Contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Ordering Officer reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

1. Program Manager

The Program Manager overseeing these tasks will have a Masters of Science degree in a technical or management discipline from an accredited college or university with a minimum of seven (7) years of below task related experience to include a minimum of five (5) years managing complex projects involving large numbers of people in subordinate groups; OR a Bachelor's degree in a technical or management discipline from an accredited college or university with a minimum of fifteen (15) years of below task related experience managing progressively more complex systems / projects involving large numbers of people in subordinate groups.

2. Project Manager

The contractor shall provide **Information Technology (IT) Project Management Support** for DD CIO/ITS mission requirements through accomplishment of the following 5.4 sub-tasks. The tasks in Section 5.4 require a TS/SCI clearance, and the Lead Project Manager must have a Bachelor's degree from an accredited college in Project Management or a related field, be Project Management Professional (PMP) certified with experience as a team lead with a minimum of five (5) years of below task related experience. All other Project Managers will have a Bachelor's degree from an accredited college in Project Management or a related field, significant experience working on Project Management Teams, be familiar with the Project Management Body of Knowledge (PMBOK®), and have a minimum of two (2) years of below task related experience.

3. **Knowledge Engineer (Senior) and 4. Knowledge Engineer**

The tasks in Section 5.2 require 50% of the personnel to have a TS/SCI clearance and the remaining personnel to have a TS clearance. The lead KE is required to have a Microsoft Certified: Power Platform Solution Architect Associate certification. All other KEs should have experience utilizing these tools and applications as well. All Senior level KEs will have a Master of Science degree from an accredited college in Engineering or Computer Science with a minimum of five (5) years of below task related experience, or a Bachelor's degree from an accredited college in Engineering or Computer Science with a minimum of five (5) years of below task related experience. Junior level KEs will have a Bachelor's degree from an accredited college in Engineering or Computer Science with a minimum of two (2) years of below task related experience.

4. **Help Desk Specialist (Senior)**

The contractors shall provide Help Desk Specialist (Senior) **Information Technology Support** for DD CIO/ITS mission requirements through accomplishment of the following 5.3 sub-tasks. The tasks in Section 5.3 require a TS/SCI clearance and a DoDI 8570.01M (IAT Level II) certification. Additionally, all personnel supporting this task will have a Bachelor's degree from an accredited college or university in a curriculum or career field of study in Computer Science or Information Systems with a minimum of 3 years of below task related experience; OR an Associate's degree from an accredited college or university in a curriculum or career field of study in Computer Science or Information Systems with a minimum of 3 years of below task related experience.

Section D - Packaging and Marking

All deliverables shall be packaged and marked IAW Best Commercial Practice.

Section E - Inspection and Acceptance

CLAUSES INCORPORATED BY REFERENCE
52.246-5 Inspection of Services—CostReimbursement
APR 1984

Section F - Deliveries or Performance

CLIN - DELIVERIES OR PERFORMANCE

The Period of Performance of the following Firm line Items are as follows:

1000	12/17/2018 - 12/16/2019
1001	12/17/2019 - 12/16/2020
1002	12/17/2020 - 12/16/2021
1003	12/17/2021 - 12/16/2022
3000	12/17/2018 - 12/16/2019
3001	12/17/2019 - 12/16/2020
3002	12/17/2020 - 12/16/2021
3003	12/17/2021 - 12/16/2022

The Period of Performance of the following Option line Items are as follows:
No option line items.
The Period of Performance of the following Award Term line Items are as follows:
No award term line items.

The Period of Performance of the following Firm items are as follows:

1000	12/17/2018 - 12/16/2019
1001	12/17/2019 - 12/16/2020
1002	12/17/2020 - 12/16/2021
1003	12/17/2021 - 12/16/2022
3000	12/17/2018 - 12/16/2019
3001	12/17/2019 - 12/16/2020
3002	12/17/2020 - 12/16/2021
3003	12/17/2021 - 12/16/2022

Section H - Special Contract Requirements

LIABILITY INSURANCE (COST TYPE CONTRACTS)

The following types of insurance are required in accordance with the clause entitled “INSURANCE-LIABILITY TO THIRD PERSONS” (FAR 52.228-7) and shall be maintained in the minimum amounts shown:

(1) Comprehensive General Liability: $200,000 per person and $500,000 per accident for bodily injury. No property damage general liability insurance is required. (2) Automobile Insurance: $200,000 per person and $500,000 per accident for bodily injury and $20,000 per accident for property damage. Comprehensive form of policy is required. (3) Standard Workmen’s Compensation and Employer’s Liability Insurance (or, where maritime employment is involved, Longshoremen’s and Harbor Worker's Compensation Insurance) in the minimum amount of $100,000.

COST LIMITATION CEILINGS ON INDIRECT RATES

If an offeror proposes cost limitation ceilings on indirect rates, the offeror is advised that the Government may evaluate the offeror’s cost proposal accordingly. The decision to propose cost limitation ceilings is the offeror’s decision. In the event the offeror proposes indirect rate limitations, these same ceiling rate limitations may be incorporated into any resultant contract without discussion. Under any cost reimbursement contract, the indirect rates billed shall be limited to the ceiling rate(s) identified in the contract. Any costs incurred above ceiling rates are not allowable.

APPOINTMENT OF CONTRACTING OFFICER'S REPRESENTATIVE

(a) The Contracting Officer hereby designates the following individual as Contracting Officer’s Representative(s) (COR) for this contract:

Mr. William T. Staggs; (703) 697-9115, william.t.staggs2.civ@mail.mil

(b) In the absence of the COR named above, all responsibilities and functions assigned to the COR shall be the responsibility of the alternate COR acting on behalf of the COR. The Contracting Officer hereby appoints the following individual as the alternate COR:

Not applicable

SUP 5252.203-9401 NOTIFICATION OF USE OF FORMER/RETIRED MILITARY AND/OR SENIOR EXECUTIVE SERVICE PERSONNEL (Dec 2009)
If the contractor intends to use the services of a former or retired Flag or General Officer, or former or retired member of the Senior Executive Service in the performance of this contract and/or any task order issued under this contract, the contractor shall notify the contracting officer of the name of such individual including a description of the services such individual will be performing, the military branch from which individual retired or separated, and their rank or SES position at time of separation. Such notification shall be provided in writing prior to performance

of services under the contract and/or task order by such individual.

SUP 5252.203-9402 USE OF INFORMATION/TECHNICAL DATA (DEC 2009)

In the performance of this contract, the Contactor will be required to utilize and/or have access to significant amounts of information related to military and homeland security operations and programs. Any information obtained by the Contractor or personnel working for the Contractor from any DoD/Government/private source in the performance of this contract shall be used only for the purposes of the performance of this contract. The Contractor and personnel working for the Contractor shall not use, release, sell, or reveal any information obtained in the performance of this contract to any person or entity not authorized herein. The Contractor shall ensure that its personnel comply with these requirements.

5252.204-9400 Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information (July 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – "DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)" dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY

This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES

Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

ACCESS TO DOD IT SYSTEMS

In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System

or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS

The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE

The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product) the individual’s start date. Failure to provide the required documentation at least 30 days prior to the individual’s start date may result in delaying the individual’s start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor’s Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product) To be considered for a favorable trustworthiness determination, the Contractor’s Security Representative must submit for all employees each of the following:

SF-85 Questionnaire for Non-Sensitive Positions Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission) Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

52.219-6 Notice of Total Small Business Set-Aside.

As prescribed in 19.508(c), insert the following clause:

Notice of Total Small Business Set-Aside (Nov 2011)

(a) *Definition*. "Small business concern," as used in this clause, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

(b) *Applicability*. This clause applies only to—

(1) Contracts that have been totally set aside or reserved for small business concerns; and

(2) Orders set aside for small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) General.

(1) Offers are solicited only from small business concerns. Offers received from concerns that are not small business concerns shall be considered nonresponsive and will be rejected.

(2) Any award resulting from this solicitation will be made to a small business concern.

(d) *Agreement*. A small business concern submitting an offer in its own name shall furnish, in performing the contract, only end items manufactured or produced by small business concerns in the United States or its outlying areas. If this procurement is processed under simplified acquisition procedures and the total amount of this contract does not exceed $25,000, a small business concern may furnish the product of any domestic firm. This paragraph does not apply to construction or service contracts.

(End of clause)

Section I - Contract Clauses

09RA 52.217-9 -- OPTION TO EXTEND THE TERM OF THE CONTRACT. (MAR 2008)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days prior to completion of the base period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed four years.

252.209-7998 REPRESENTATION REGARDING CONVICTION OF A FELONY CRIMINAL VIOLATION UNDER ANY FEDERAL OR STATE LAW (DEVIATION 2012-O0007) (MAR 2012)

(a) In accordance with section 514 of Division H of the Consolidated Appropriations Act, 2012, none of the funds made available by that Act may be used to enter into a contract with any corporation that was convicted of a felony criminal violation under any Federal or State law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.
(b) The Offeror represents that it is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal or State law within the preceding 24 months.

(End of provision)

252.209-7999 Representation by corporations regarding an unpaid delinquent tax liability or a felony conviction under any Federal law (Deviation 2012-O0004) (JAN 2012)

(a) In accordance with sections 8124 and 8125 of Division A of the Consolidated Appropriations Act, 2012, (Pub. L. 112-74) none of the funds made available by that Act may be used to enter into a contract with any corporation that –

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that –

(1) It is ( ) is not ( ) a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability,

(2) It is ( ) is not ( ) a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.
(End of provision)

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request,

the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

FAR Clauses: http://acquisition.gov/far/ DFARS Clauses: http://www.acq.osd.mil/dpap/dars/dfarspgi/current/

(End of clause)

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (OCT 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services--Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Items. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) Definitions. As used in this provision-

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to--

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to--

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(d) Representations. The Offeror represents that--

(1) It [] will, [] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information

required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that--

It [] does, [] does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures.

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment--

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services--

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment--

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services--

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2020)

(a) Definitions. As used in this clause--

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical

infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system,

or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number,

manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available

information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications

equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.204-26 Covered Telecommunications Equipment or Services--Representation (OCT

2020)

(a) Definitions. As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) Representations.

(1) The Offeror represents that it [ ] does, [ ] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it [ ] does, [ ] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

252.204-7016 Covered Defense Telecommunications Equipment or Services --

Representation (Dec 2019)

(a) Definitions. As used in this provision, covered defense telecommunications equipment or services has the meaning provided in the clause 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered defense telecommunications equipment or services".

(c) Representation. The Offeror represents that it [ ] does, [ ] does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

252.204-7017 Prohibition on the Acquisiton of Covered Defense Telecommunications

Equipment or Services--Representation (Dec 2019)

The Offeror is not required to complete the representation in this provision if the Offeror has represented in the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services--Representation, that it "does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument."

(a) Definitions. Covered defense telecommunications equipment or services, covered mission, critical technology, and substantial or essential component, as used in this provision, have the meanings given in the 252.204-7018 clause, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, of this

solicitation.

(b) Prohibition. Section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits agencies from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part

of any system.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.govfor entities that are excluded when providing any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology

as part of any system, unless a waiver is granted.

(d) Representation. If in its annual representations and certifications in SAM the Offeror has represented in paragraph (c) of the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services--Representation, that it "does" provide covered defense telecommunications equipment or services as a part

of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument, then the Offeror shall complete the following additional representation:

The Offeror represents that it [ ] will [ ] will not provide covered defense telecommunications equipment or services as a part of its offered products or services to DoD in the performance of any award resulting from this solicitation.

(e) Disclosures. If the Offeror has represented in paragraph (d) of this provision that it "will provide covered defense telecommunications equipment or services," the Offeror shall provide the following information as part of the offer:

(1) A description of all covered defense telecommunications equipment and services offered (include brand or manufacturer; product, such as model number, original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable).

(2) An explanation of the proposed use of covered defense telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition referenced in paragraph (b) of this provision.

(3) For services, the entity providing the covered defense telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known).

(4) For equipment, the entity that produced or provided the covered defense telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications

Equipment or Services (Dec 2019)

(a) Definitions. As used in this clause--

Covered defense telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities;

(2) Telecommunications services provided by such entities or using such equipment; or

(3) Telecommunications equipment or services produced or provided by an entity that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Covered foreign country means--

(1) The People's Republic of China; or

(2) The Russian Federation.

Covered missions means--

(1) The nuclear deterrence mission of DoD, including with respect to nuclear command, control, and communications, integrated tactical warning and attack assessment, and continuity of Government; or

(2) The homeland defense mission of DoD, including with respect to ballistic missile defense.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. In accordance with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91), the contractor shall not provide to the Government any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless the covered defense telecommunication equipment or services are covered by a waiver described in Defense Federal Acquisition Regulation Supplement 204.2104.

(c) Procedures. The Contractor shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.govfor entities that are excluded when providing any equipment, system, or service, to carry out covered missions, that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver is granted.

(d) Reporting.

(1) In the event the Contractor identifies covered defense telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, the Contractor shall report at https://dibnet.dod.milthe information in paragraph (d)(2) of this clause.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information

about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available

information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered defense telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

CLAUSES INCORPORATED BY REFERENCE
52.202-1 Definitions NOV 2013 52.203-3 Gratuities APR 1984

52.203-5 Covenant Against Contingent Fees MAY 2014

52.203-6 Restrictions on Subcontractor Sales to the Government SEP 2006

52.203-7 Anti-Kickback Procedures MAY 2014

52.203-8 Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity MAY 2014

52.203-10 Price or Fee Adjustment for Illegal or Improper Activity MAY 2014

52.203-12 Limitation on Payments to Influence Certain Federal Transactions OCT 2010

52.203-13 Contractor Code of Business Ethics and Conduct OCT 2015
52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights
APR 2014
52.204-2 Security Requirements AUG 1996

52.204-4 Printed or Copied Double-Sided on Postconsumer Fiber Content Paper MAY 2011

52.204-9 Personal Identity Verification of Contractor Personnel JAN 2011

52.204-10 Reporting Executive Compensation and First-Tier Subcontract Awards OCT 2016

52.204-13 System for Award Management Maintenance OCT 2016

52.204-18 Commercial and Government Entity Code Maintenance JUL 2016

52.204-19 Incorporation by Reference of Representations and Certifications DEC 2014

52.204-21 Basic Safeguarding of Covered Contractor Information Systems JUN 2016

52.209-6 Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment
OCT 2015

52.209-9 Updates of Publicly Available Information Regarding Responsibility Matters
JUL 2013
52.209-10 Prohibition on Contracting with Inverted Domestic Corporations
NOV 2015
52.210-1 Market Research APR 2011 52.215-2 Audit and Records—Negotiation OCT 2010

52.215-8 Order of Precedence—Uniform Contract Format OCT 1997
52.215-17 Waiver of Facilities Capital Cost of Money OCT 1997

52.215-21 Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data—Modifications--Alternate III OCT 1997

52.215-23 Limitations on Pass-Through Charges--Alternate I OCT 2009

52.216-7 Allowable Cost and Payment JUN 2013 52.216-8 Fixed Fee JUN 2011

52.217-8 Option to Extend Services NOV 1999

52.219-6 Notice of Total Small Business Set-Aside NOV 2011

52.219-14 Limitations on Subcontracting JAN 2017

52.219-28 Post-Award Small Business Program Rerepresentation JUL 2013

52.222-2 Payment for Overtime Premiums JULY 1990 52.222-3 Convict Labor JUNE 2003

52.222-21 Prohibition of Segregated Facilities APR 2015 52.222-26 Equal Opportunity SEP 2016

52.222-35 Equal Opportunity for Veterans OCT 2015

52.222-36 Equal Opportunity for Workers with Disabilities JUL 2014

52.222-37 Employment Reports on Veterans FEB 2016

52.222-40 Notification of Employee Rights Under the National Labor Relations Act DEC 2010 5

2.222-50 Combating Trafficking in Persons MAR 2015

52.223-5 Pollution Prevention & Right-To-Know Information MAY 2011

52.223-6 Drug-Free Workplace MAY 2001 52.223-10 Waste Reduction Program MAY 2011

52.223-17 Affirmative Procurement of EPA-Designated Items in Service and Construction Contracts. MAY 2008 52.223-18 Encouraging Contractor Policies to Ban Text Messaging While Driving AUG 2011

52.223-19 Compliance with Environmental Management Systems MAY 2011

52.224-3 Privacy Training JAN 2017 52.228-7 Insurance—Liability to Third Persons MAR 1996

52.232-17 Interest MAY 2014

52.232-18 Availability of Funds APR 1984

52.232-23 Assignment of Claims MAY 2014

52.232-25 Prompt Payment--Alternate I FEB 2002

52.232-22 Limitation of Funds APR 1984

52.232-33 Payment by Electronic Funds Transfer—System for Award Management JUL 2013
52.232-39 Unenforceability of Unauthorized Obligations JUN 2013

52.233-1 Disputes MAY 2014 52.233-3 Protest after Award--Alternate I JUN 1985

52.233-4 Applicable Law for Breach of Contract Claim OCT 2004

52.237-2 Protection of Government Buildings, Equipment, and Vegetation APR 1984

52.242-1 Notice of Intent to Disallow Costs APR 1984

52.242-3 Penalties for Unallowable Costs MAY 2014

52.242-4 Certification of Final Indirect Costs JAN 1997 52.242-13 Bankruptcy JUL 1995

52.243-2 Changes—Cost Reimbursement--Alternate I APR 1984 52.244-2 Subcontracts OCT 2010

52.244-5 Competition in Subcontracting DEC 1996

52.244-6 Subcontracts for Commercial Items NOV 2017

52.245-1 Government Property JAN 2017

52.245-9 Use and Charges APR 2012 52.246-25 Limitation of Liability—Services FEB 1997

52.247-67 Submission of Transportation Documents for Audit FEB 2006

52.249-6 Termination (Cost-Reimbursement) MAY 2004

52.249-14 Excusable Delays APR 1984

52.253-1 Computer Generated Forms JAN 1991

252.201-7000 Contracting Officer's Representative DEC 1991

252.203-7000 Requirements Relating to Compensation of Former DoD Officials SEP 2011

252.203-7001 Prohibition on Persons Convicted of Fraud or Other Defense-Contract-Related Felonies DEC 2008 252.203-7002 Requirement to Inform Employees of Whistleblower Rights SEP 2013

252.203-7004 Display of Hotline Posters OCT 2016

252.204-7003 Control of Government Personnel Work Product APR 1992
252.204-7005 Oral Attestation of Security Responsibilities NOV 2001

252.204-7015 Notice of Authorized Disclosure of Information for Litigation Support MAY 2016

252.205-7000 Provision of Information to Cooperative Agreement Holders DEC 1991

252.209-7004 Subcontracting with Firms that are Owned or Controlled by the Government of a Country that is a State Sponsor of Terrorism OCT 2015

252.211-7007 Reporting of Government-Furnished Property AUG 2012

252.216-7009 Allowability of Legal Costs Incurred in Connection With a Whistleblower Proceeding SEP 2013 252.223-7004 Drug-Free Work Force SEP 1988

252.225-7048 Export-Controlled Items JUNE 2013

252.226-7001 Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns SEP 2004

252.227-7013 Rights in Technical Data--Noncommercial Items FEB 2014

252.227-7015 Technical Data--Commercial Items FEB 2014

252.227-7027 Deferred Ordering of Technical Data or Computer Software APR 1988
252.232-7010 Levies on Contract Payments DEC 2006

252.242-7006 Accounting System Administration FEB 2012

252.243-7002 Requests for Equitable Adjustment DEC 2012

252.245-7001 Tagging, Labeling, and Marking of GovernmentFurnished Property APR 2012

252.245-7002 Reporting Loss of Government Property DEC 2017

252.245-7003 Contractor Property Management System Administration APR 2012

252.245-7004 Reporting, Reutilization, and Disposal DEC 2017