

VENDOR:											
VENDOR POC:											
VENDOR POC EMAIL:											
VENDOR POC PHONE:											
Date of Report:											
CONTRACT #	DO #	TOTAL CUMULATIVE LIFE CYCLE AMOUNT EXCLUDING FEES	PERIOD OF PERFORMANCE	CUSTOMER DEPARTMENT (e.g., AF, Army, DLA, DOJ)	VENDOR INVOICE PERIOD	AMOUNT PAID VENDOR FOR INVOICE PERIOD (amount without DITCO Fee)	AMOUNT REMITTED TO DITCO THIS PERIOD (1% of Column G)	FINAL INVOICE yes or no	VENDOR EFT NUMBER	EFT DATE	TOTAL CHECK AMOUNT
FY22 Q1											
					Total FY22 Q1	\$0.00	\$ -				
FY22 Q2											
					Total FY22 Q2	\$ -	\$ -				
FY22 Q3											
					Total FY22 Q3	\$0.00	\$ -				
FY22 Q4											
					Total FY22 Q4	\$ -	\$ -				
					Total Contract to Date	\$ -	\$ -				

#	RFP Document	Section	Subsection	Page #	Impact	Question
Number of Comment	Select the appropriate RFP document from the drop down list	Indicate the document section name and/or number	Indicate the sub-section name and/or number	Indicate the page number of the referenced document	Select the appropriate impact category from the drop down list	Insert question (plus any necessary context) pertaining to the JWCC documentation or other

EXAMPLE

1	PWS	5	5.5.6.1	17	Significant	What is meant by... ?
----------	------------	----------	----------------	-----------	--------------------	------------------------------

Comment Resolution Matrix Instructions

JOINT WARFIGHTING CLOUD CAPABILITY Quality Assurance Surveillance Plan

Prepared By:

Defense Information Systems Agency
Hosting and Compute Center (HaCC)

November 14th, 2021 (Original Date of Release)

September 7, 2022 (A0009 Update)

Table of Contents

Overview	3
Description of Services	3
Roles and Responsibilities	4
Contract Quality Requirements	5
Government Surveillance	6
Non-Conforming Performance	7
Data Analysis	8
Acceptance of Services	9
Quality Assurance Surveillance File	9
Manpower Data Reporting	10
QASP Changes	10
Performance Surveillance Summary	10

1. Overview

1.1. **Purpose.** The purpose of this plan is to identify the methods and procedures the government will use to ensure it receives the services/products under this contract, including those measures and metrics identified in the Performance Work Statement (PWS).

1.2. **Intent.** The intent of this plan is to allow the Government to consistently and fairly monitor the Contractor's quality control practices applied to delivered outcomes. In the event there is a quality issue, this plan provides the basis to identify any weaknesses or deficiencies, and enables the Government to provide the Contractor with the necessary information required for corrective actions to be taken to improve quality, processes and procedures. The Contractor is responsible for developing an effective and efficient methodology to ensure they meet and/or exceed the required thresholds of service stipulated in this contract. The Government intends to perform surveillance on this contract in accordance with this Quality Assurance Surveillance Plan (QASP), but reserves the right to monitor the contract in any manner and at any time necessary to ensure that the provided services conform to contract requirements. The Government reserves the right to apply quality assurance at the subcontract level, and may perform quality assurance at the Contractor's, or subcontractors, place of business. Non-conforming services discovered with subcontractors will be identified to the prime Contractor for resolution.

1.3. **Authority.** Authority for issuance of this QASP is provided under Part 46 of the Federal Acquisition Regulation (FAR), Inspection of Services clauses, which provide for inspection, acceptance and documentation of the services called for in the contract or orders. This acceptance is to be executed by the Contracting Officer (CO) or a duly authorized representative.

2. Description of Services

2.1. **Scope of Work.** The U.S. Department of Defense (DoD) seeks to establish enterprise-class cloud computing through the Joint Warfighting Cloud Capability (JWCC). JWCC is a multi-vendor, enterprise-wide solution that will provide globally available commercial cloud services, across all security domains, classification, and impact levels (ILs), from the strategic level to the tactical edge (TE), including Disconnected, Disrupted, Intermittent, or Limited (DDIL) environments, at scale. JWCC will lay the foundation for DoD to fully leverage "X as a Service" (XaaS) cloud capabilities and service offerings to enable current and future Department initiatives.

2.2. **Contract.** The JWCC Indefinite-Delivery, Indefinite-Quantity (IDIQ) acquisition environment consisting of multiple IDIQ contracts that allows for Firm-Fixed-Price (FFP), Time and Materials (T&M), and hybrid (a mix of FFP and T&M) TOs; travel will only be on a T&M basis. The period of performance is inclusive of a three-year base period and two one-year option periods, with a shared ceiling maximum value of \$9 billion, and with decentralized ordering across the DoD Enterprise. The JWCC IDIQ acquisition environment has specific FAR clauses cited for quality control, as well as a contractor-delivered Quality Control Plan (QCP) (CDRL A010), and additional quality measures and metrics identified in the final awarded submission. This plan will specifically identify the minimum quality control measures to be evaluated by the government. However, as "cloud" evolves as a technology, additional measures and associated

metrics may be added as necessary and appropriate to ensure both the Government and Contractor are satisfied with both performance and quality of delivered capabilities.

3. Roles and Responsibilities

3.1. To fully understand the roles and the responsibilities of the parties (Government and Contractor), it is important to first define the distinction in terminology between the Contractor's QCP and the Government's QASP. In accordance with (IAW) FAR Part 52.246-1 -- Contractor Inspection Requirements, the Contractor, and not the Government, is responsible for management and quality control actions necessary to meet the quality standards set forth by the contract and its task orders (TO). The Contractor develops and submits a QCP (CDRL A008) for Government approval in compliance with contract requirements. Once accepted, the Contractor then uses the QCP to guide the complete documentation of the processes and implementation methods and approaches required to manage the quality control actions to achieve the specified outcomes.

3.2. The QASP is created by the Government and put in place to guide the surveillance and oversight of the Contractor's quality control efforts to assure that they are delivering timely and effectively those results specified in the contract or TO. The QASP is not a part of the Contract nor is it intended to duplicate the Contractor's QCP.

3.3. Upon approval of a Contractor's QCP, the Contracting Officer's Representative (COR) makes any necessary revisions to the QASP based on the Contractor's QCP. The COR shall not revise the QASP in a way that alters Performance Objectives, Standards, and Acceptable Quality Levels (AQL) from either the contract or the approved QCP. This plan shall provide the COR with a basis of evaluation to identify deficient performance or quality of delivery, and provide verifiable input for the required performance report via the Contractor Performance Assessment Reporting System (CPARS).

3.4. The QASP is a tool for the Government and remains a living document throughout the life of the contract and/or task order performance period. The CO may direct unilateral changes to the QASP as needed. At the discretion of the government, the Contractor will be advised of any QASP modification. The QASP, while not an element of the contract, will include the performance criteria summary of the contract, and use these contract elements as the basis for evaluation and assessment of Quality and Performance during contract execution. The method of surveillance, surveillance calendar, schedule, and frequency of surveillance are not elements of the PWS.

3.5. The role of the Government is to monitor the effectiveness of the Contractor's quality control activities and to ensure contract quality standards are achieved. (ref. FAR Part 46 – Government Contract Quality Assurance)

Government Personnel:

Contracting Officer (KO) - A person duly appointed with the authority to enter into, administer and terminate contracts on behalf of the Government. The named KO is the only authority who can legally commit the Government and, as the Government's agent, is the only

person that is authorized to modify the contract. The JWCC Contract allows for decentralized ordering, and as such, each TO KO is the authority for their TOs, while the JWCC contract KO is the single authority with regard to the IDIQ contract. The KO is the final authority for determining the adequacy of the contractor's performance, per IDIQ or TOs as appropriate. KO decisions for the JWCC IDIQ contract or TOs, as appropriate, are final.

Contracting Officer's Representative (COR) – An individual designated in writing by the KO to perform specific technical and administrative functions within the scope and limitations of their written appointment (e.g., surveillance of contractor's performance, accept services). The COR is not empowered to make any contractual commitments, authorize any changes to a TO or the JWCC IDIQ contract or in any way obligate additional funds by the Government; this authority rests solely with the KO.

Contract Administrator – The official Government representative with delegated authority by the KO and is appointed to administer a contract. This individual is normally a member of the appropriate Contracting/Procurement career field and advises on all technical contractual matters.

Property Administrator – An authorized representative of the KO, appointed in accordance with agency procedures. This individual is responsible for administering the contract requirements and obligations relating to government property in possession of a contractor.

Contractor Personnel:

Program Manager- Responsible for running complex programs and projects. Supervises the project team and manages conflicts within different departments. Plans and sets project goals and milestones and develops risk management strategies. Defines resources and schedules for the implementation of the program. Clearly defines requirements and sets targets accordingly. Recognizes areas for internal improvement and develops plans for implementing the improvements.

Quality Manager- Responsible for quality achievement and performance improvement throughout the organization. Develops, implements, communicates, and maintains a quality plan to bring the Company's Quality Systems and Policies into compliance with quality system requirements. Direct the activities of quality personnel to measure key quality characteristics of processes from inception to completion. Establishes the standards of service for customers or clients.

4. Contract Quality Requirements

4.1. **Quality Control Program.** The contractor's Quality Control Program requirements are identified in multiple delivered contractual documents including the Contractor's Quality Control Plan (QCP, CDRL A008), and quality control items identified throughout the J-1 PWS, including a specific performance metrics section (Part 7.1). The Contractor shall maintain and enforce, as specified in the QCP, and quality control items specified in the PWS, which comply with the requirements of this contract. This establishes the minimum acceptable quality level for acceptance of delivery of outcomes and services to the Government

4.2. **Government Quality Assurance.** The Government will perform Quality Assurance surveillance of the Contractor and the performance outcomes as specified in the Contractor's

QCP (CDRL A008) and PWS in accordance with this QASP to ensure acceptable levels of contract performance are achieved and that the Contractor is maintaining acceptable levels of Quality Control to ensure fully acceptable services are provided.

5. Government Surveillance

5.1. Methods of Surveillance include but are not limited to:

- A. **100% Inspection** - This is an inspection method whereby all outputs are monitored. This method provides the best indication of contractor performance and the most documented basis for determining contract payment actions. However, it requires extensive COR resources, and therefore, is not practical for most service requirements. 100 % inspection is preferred when the PWS requirement is so critical that non-performance would pose a direct risk to the safety of personnel or property, or when the work occurs infrequently and the output population is small.
- B. **Procedural Inspection** - This is an inspection method whereby a process or configuration is assessed for compliance with a requirement or specification. This method provides the best indication of contractor performance on creation of processes or procedures for the documented basis for determining contract payment actions. However, it requires extensive COR resources, and therefore, is not practical for most continuous operational service requirements. This type of inspection is preferred when the PWS requirement stipulates a process, configuration or other repeatable behavior mechanisms is necessary for overall performance.
- C. **Random Sampling** - When a service is performed relatively frequently and a statistically valid sample can be selected for audit. This is the most appropriate method for frequently recurring tasks. Random Sampling is a means of evaluation by observing or inspecting some part (a sample), but not all, of a population or lot of the contract requirements to assist the Government with determining whether standards set forth in the contract have been met. This tool is not the KO's only option nor is the tool usage mandatory. When performing random sampling, an updated version of Military Standard 105E Tables/ANSI/ASQC Z1.4 (a web based tool is located at: <https://www.sqconline.com/military-standard-105e-tables-sampling-attributes>) may be used to determine the sample size and the acceptance and rejection numbers. KO alternatively approved random sampling approaches may also be used for this process.
- D. **Periodic Sampling** - This method, sometimes called "planned inspection," consists of the evaluation of tasks selected on other than a 100% or random basis. It may be appropriate for tasks that occur infrequently, and where 100% inspection is neither required nor practical. A predetermined plan for inspecting part of the work is established using subjective judgment and analysis of agency resources to decide what work to inspect and how frequently to inspect it.
- E. **Customer Feedback** – This is not necessarily a valid method of surveillance, but a good indicator for areas where surveillance should be conducted or intensified. The COR may design a customer survey questionnaire to be used as an essential part of a well-publicized customer complaint program. In times of resource constraints, the use of customer surveys

provides an effective and efficient means of monitoring Contractor performance. Customer surveys should only supplement other surveillance efforts and be analyzed by surveillance personnel trained in validating customer complaints. Customers should be made aware of minimal Contractor performance requirements to be sure that customer responses to surveys are valid indicators of actual Contractor performance. The COR must investigate each customer complaint and validate the accuracy before any action will be taken.

5.2. **Surveillance Schedule.** The COR will develop a schedule of surveillance activities based on the Performance Standards as outlined in the Performance Requirements Summary, section 13, as well as any other critical contractual requirements determined to be higher risk requiring oversight. The surveillance timeline outlined in the schedule will be as detailed and in-depth as necessary to provide the Government with the objective quality evidence required to support acceptance of the services provided by the Contractor. The schedule will provide planned periodic surveillance during all required hours of the Contractor's operation. The schedule is considered "Controlled Unclassified Information" and is not releasable to anyone other than authorized Government personnel.

The schedule will identify the artifact, method of surveillance, the frequency of inspection, place of inspection (in remarks if non-electronic), and activity to be monitored (dates and times can be altered without a formal change to the schedule as long as all inspections are performed). Any modification to the schedule will be completed no later than seven calendar days prior to the beginning of the period it covers and a copy forwarded to the KO for information, review, and concurrence. An initial Surveillance will be conducted every 30 days. The COR will use the Procurement Integrated Enterprise Environment (PIEE)/Surveillance and Performance Monitoring (SPM) module while monitoring the contract.

5.3. **Inspection instructions/checklists.** The COR will develop inspection instructions/checklists for all planned inspections which may require special instructions on how to perform the inspection, what observations should be made, and specific details of what to look for to identify acceptable performance. The COR will use PIEE/SPM for the surveillance checklist.

5.4. **Documentation of Inspections.** All inspections/quality assessments will be documented and include, as a minimum, record, date, who performed the inspection, what was inspected, what standard of measure was used, and the assessment result. Successful or exceptional performance will be documented as well as deficiencies in Contractor performance. Documentation will be maintained for future reference, audit, proof of inspection, and past performance documentation.

6. Non-Conforming Performance

6.1. **COR Notification.** The COR will notify the Contractor, in writing, each time a non-conformant quality event has been observed and recorded and ask the Contractor to correct the problem or re-accomplish the service. The COR will record the contract requirement, the specific deficiency to the requirement, the date and time it was discovered, and have the Contractor formally acknowledge each deficiency in writing. The Contractor will be given a timeline, after notification and acknowledgement, to correct the deficiency IAW requirements of the contract. Deficiencies that cannot be corrected within the identified timeline will be reported to the KO.

6.2. **Customer Feedback.** Customer feedback can be in any format (verbal or written), but no matter the format, the COR will maintain a record of the positive or negative feedback.

- A. If immediate response to a complaint is required, the COR will provide the response to the requester as soon as practical.
- B. The COR will conduct an investigation to determine the validity of any negative comments received.
- C. If the negative comment is determined not to be valid, if possible, the COR will inform the customer of the reason(s) as soon as practical.
- D. Financial health of the contractor will be investigated, if COR receives reports of financial instability.
- E. See paragraph 6.1 for validated negative comments that are true contractual non-conformances. If this non-conformance is a more serious (systemic in nature) or recurring deficiency that could indicate a trend, then the COR should see paragraph 6.2.
- F. The COR will follow up with the customer on the corrective action taken by the contractor, if applicable.

6.3. **Contract Deficiency Reports.** The COR will report more serious (systemic in nature) or recurring deficiencies that could indicate a trend by using the Contract Deficiency Report found in PIEE/SPM. The Contract Discrepancy Report will state the Contract Requirement, the specific contract reference and the specific violation (s) to the requirement. The COR will forward copies of Contract Discrepancy Reports to the KO, in the event that the COR is unable to have the Contractor achieve successful remediation of the deficiency. If the deficiency is elevated to the KO for action, the KO will notify the Contractor and request corrective action to the specific non-conformance, identification of the root cause and corrective action for the root cause with a required suspense date. The KO may require the Contractor to re-perform any services that do not meet contract requirements at no additional cost to the government. The Contractor will formally acknowledge, in writing, the entire list of deficiencies presented by the KO, and in conjunction submit their Corrective Action Plan (CAP) for KO review, approval, and inclusion in the contract/order file. The KO should include the COR in the review of the CAP and re-inspection of services that were found deficient, to ensure the CAP included adequate root cause analysis, included corrective action for the root cause, and was accomplished in the time frame agreed upon.

The KO and COR will not consider a Contract Deficiency Report closed until the deficiency has been corrected and all agreed-upon actions of the CAP have been completed. Contractor's failure to follow through and complete corrective actions will be reported immediately to the KO for further action. (Note: If the COR has to repeatedly perform re-inspection there could be a government re-inspection cost, which could be recovered from the Contractor). The COR will also follow up after the Contractor has completed the corrective action to ensure that the Contractor's corrective action was sufficient to preclude recurrence.

7. Data Analysis

COR Analysis. COR shall perform and document analysis of available data, per the agreed evaluation periodicity or contractual stipulation, and make adjustments to surveillance schedule as required based on results of analysis. Analysis shall be used to look for and document trends in performance, which may indicate shifts in performance risk that could result in increased or reduced surveillance. Data can be based on government observations or contractor observations. Negative trends noted using government observations could result in issuing the contractor a Contract Deficiency Report. Trends noted using contractor data could result in a Contract Deficiency Report if the contractor is not addressing the negative trend. Documentation of data analysis will be recorded in a Monthly COR Activity Report.

8. Acceptance of Services

When all services have been deemed acceptable and there is documented objective quality evidence to support acceptable performance, the COR will accept the services provided and authorize payment upon satisfactory completion of the work.

9. Monthly COR Activity Report

The COR will submit a brief monthly activity report to the KO, which will include the next month's surveillance schedule, summary of inspections performed with results, summary of customer complaints with analysis, summary of contract discrepancies, results of data analysis, recommended adjustments to surveillance, accepted invoices, and any other pertinent contract activities.

10. Quality Assurance Surveillance File

10.1. The Quality Assurance or COR Surveillance file shall contain the following as applicable:

10.2. Memorandum for record of minutes of any meetings, telephone conversations, and discussions with the contractor or others pertaining to the contract or contract performance.

10.3. Names, position titles, and contact information of all key personnel assigned to this contract (government and contractor).

10.4. Records of all inspections performed and the results.

10.5. Monthly surveillance schedules.

10.6. Surveillance Checklists.

10.7. Copy of the COR designation letter from the KO, any changes to that letter, and any termination letters.

10.8. Training Certifications for COR and refresher training.

10.9. Copy of the contract and all contract modifications.

10.10. Copy of the applicable QASP, with attached schedule and checklist.

10.11. Customer Feedback. Documentation pertaining to acceptance of services, reports, or data.

10.12. Copy of the Contractor's QCP.

All correspondence initiated by authorized representatives (Contractor or Government) concerning performance of the contract.

11. Manpower Data Reporting

11.1. Effective in FY 2020, DoD will no longer require contractors to report into the Enterprise-wide Contractor Reporting Application (ECMRA). This rescinds the Office of the Secretary of Defense memorandum, "Enterprise-wide Contractor Manpower Reporting Application," dated November 28, 2012, jointly signed by the Under Secretary of Defense for Acquisition and Sustainment, and Acting Principal Deputy Under Secretary of Defense for Personnel and Readiness.

11.2. For FY 2020, contractors will begin reporting manpower data relating to the performance of services contracts into the System for Award Management (www.sam.gov), consistent with existing service contract reporting requirements under the FAR that is currently applicable only to Federal civilian agencies. The new initiative will allow industry to report all manpower data into a single Federal-wide portal, removing duplicative requirements; one for DoD and another for the rest of the Federal Government, which requires the same data elements to be reported from industry for services contracts performed for both DoD and Federal civilian agencies that essentially perform the same function. The outcome will be a process that is less burdensome on both industry and Government, while improving data integrity and accuracy.

12. QASP Changes

The QASP is a living document and, as such, may be changed as needed. However, the KO must approve changes. The COR will submit recommended changes to the KO for approval.

13. Performance Surveillance Summary

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
1	5	Specific Tasks:	Summary Requirement	N/A	N/A	N/A
2	5.1	Program Management	Summary Requirement	N/A	N/A	N/A
3	5.1.1	The Contractor shall provide overarching program management personnel, processes, and tools under CLINs x008, as necessary to manage and oversee all Contractor activities for the duration of their JWCC Contract within cost, schedule, performance, and quality requirements.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	As required	N/A	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
4	5.1.2	The Contractor shall establish and maintain a formal PMO, which shall coordinate and interface with the JWCC COR and JWCC PMO to ensure the JWCC Contract is being used efficiently, compliant with JWCC requirements, and making use of commercial best practices.	The Government will audit the Contractor's JWCC support organizational structure to assure the critical PoCs for contract success are identified.	As required	N/A	Random Sample
5	5.1.3	The Contractor shall appoint a PM and a DPM empowered to make program and project-level decisions and commit resources necessary to successfully execute courses of action within scope of the JWCC Contract.	The Government will audit the Contractor's proposed JWCC support organizational structure to ascertain if the PM and DPM are clearly identified.	As required	N/A	100% Inspection
6	5.1.4	The Contractor's PM support will facilitate the timely authorization of JWCC infrastructure and offerings Offerings to be included on the JWCC Catalog at all classification levels and ILs, and take all necessary steps to ensure successful integration with the DoD's ATAT provisioning tool with the Contractor's management systems for JWCC, as appropriate.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	As required	N/A	Random Sample
7	5.1.5	The PM and DPM shall have sufficient expertise and authority to execute the following responsibilities: (a) serve as the official central PoC and interface between the Contractor and the COR; (b) be available as needed for interaction with the JWCC COR, JWCC PMO, and JWCC KO; and (c) monitor and report on contract status (CDRL A001) and compliance with the JWCC Contract requirements.	The Government will assess whether the PM and DPM have the necessary authority to act as the single point of contact for all managerial Contractor engagements with regard to the JWCC Contract.	Monthly	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
8	5.1.6	The contractor shall perform the following requirements and provide the following deliverables. All materials shall be provided error free and presented in a professional manner.	Summary Requirement	N/A	N/A	N/A
9	5.1.6.1	<p>The Contractor Program Management Plan (CPMP) (CDRL A021) shall include with sufficient detail such that the Government can assess and understand how the Contractor intends to meet all requirements outlined in the PWS.</p> <p>The CPMP demonstrates the Contractor's approach, timeline, and tools to be used in execution of the Contract. The CPMP should be in both a narrative and graphic format that discusses and displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The CPMP shall be the primary plan and all other plans (e.g. the QCP) required and defined in the PWS will be subordinate to the CPMP. The Contractor shall provide at time of proposal submission the initial CPMP. Once the Government agrees with the CPMP, the finalized copy shall be provided within 10 business days after final Government input(s) are received. The CPMP shall be updated as needed</p>	The Government will assess the CPMP for sufficiency of addressing each requirement of the contract.	Proposal submission, then 10 days after accepted and as needed or annually at a minimum	N/A	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		thereafter, but no less than annually. The CPMP shall, at a minimum, include a description of the management and execution approach to include: all information required under administration and execution of the entirety of 5.1.6				
10	5.1.6.2	The Contract Monthly Progress Report (CDRL A001) is for overall performance under the JWCC Contract and access to all Task Order Monthly Progress Reports (CDRL A012) for PM performance. The Contract Monthly Progress Report shall include, but not be limited to, the following:	The Government will assess the data provided to describe TO execution value and expenditure.	Monthly	The TO has robust data describing every facet of execution, financial, and management aspects.	Random Sample
11	5.1.6.2.1	A full accounting of each TO received, the execution status of the TO, total value of the TO, and funds expended to date on the TO.	The Government will assess if the information provides the Department with insight for JWCC utilization and a full comparison with the commercial and governmental utilization to JWCC use.	Monthly	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.	Random Sample
12	5.1.6.2.2	The report shall include, at a minimum, the JWCC utilization metrics and the percentage as compared to the Contractor's total commercial and non-commercial utilization and capacity. The Contractor/Officer should ensure the information in the report is assessed and appropriately marked with portion markings IAW the DoDM 5200.01. These portion markings shall be limited to 5.1.6.2 and its subsections.	The Government will assess if the information provided is sufficient as required for analysis.	Monthly	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		The report shall be broken out by CSO and CLIN per month, year, and life of the JWCC Contract for the following metrics:				
13	5.1.6.2.2.1	Network. Volume of commercial client traffic, in megabytes, for public internet ingress and egress (at the logical Cloud Boundary outside of availability zones, i.e. in and out of the Contractor's controlled infrastructure) per month and aggregated for the duration of the JWCC Contract to date. This measure and metric shall include a discrete breakdown comparison of the following: commercial traffic, JWCC Contract traffic, TO traffic by availability zone and comprehensively, as both raw volume and the Government's equivalent utilization as a percentile comparison.	The Government will assess if the information provided on Network measures is sufficient as required for analysis.	Monthly	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.	Random Sample
14	5.1.6.2.2.2	Compute. Number of physical (not virtualized) compute (e.g. CPU, GPU, or other processor technology as applicable) cores in use by Application Servers. Application Servers are defined as those physical servers that host the virtualized infrastructure and platform services used by end users (e.g. a server that is hosting JWCC Contract applications is an Application Server, while a network router does not satisfy this definition of Application Server). Additionally, the	The Government will assess if the information provided on Compute measures is sufficient as required for analysis.	Monthly	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		number of physical compute cores that are available for future use (not currently allocated to an Application Server, nor in use by Application Server) both comprehensively and by Availability Zone.				
15	5.1.6.2.2.3	Storage. Data, in megabytes, consumed and available, for each of online, nearline, and offline storage, averaged across the month and aggregated for the life of the JWCC Contract.	The Government will assess if the information provided on Storage measures is sufficient as required for analysis. The Government will assess if units of computation are clearly specified.	Monthly	N/A	Random Sample
16	5.1.6.2.2.4	Additionally, the report shall identify the base (e.g. base 2 or base 10) for all measured values using bytes.	The Government will assess if units of computation are clearly specified.	Monthly	N/A	
17	5.1.6.2.3	An accurate, clear and precise measure and metric for each performance criteria listed in Technical Exhibit 1, Performance Requirements Summary, of the Attachment J-1: JWCC PWS. This shall include monthly and accrued measures and metrics over the life of the JWCC Contract.	The Government will assess if all performance criteria are accounted for regarding metrics and measures from Technical Exhibit 1.	Monthly	Real time analytics will present a continuous reading of the JWCC metrics and measures and the comparison to industry and total Government consumption.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
18	5.1.6.2.4	Progress of the ability to create and deliver the following CDRLs:	Summary Requirement	N/A	N/A	N/A
19	5.1.6.2.4.1	A report on usage, by TO, for any GFP (CDRL A015).	The Government will assess if an accurate accounting of GFP per TO is presented.	365 DAC and Annually	Real time analytics will present a continuous automated tracking of the JWCC GFP on a per TO basis.	Random Sample
20	5.1.6.2.4.2	A report on ordering, by TO, for any TE Offering and any associated TE Devices (CDRL A012).	The Government will assess if TE offerings tracking is managed at the TO level.	30 DATO and Monthly	Real time automated tracking for TE offerings at the TO level.	Random Sample
21	5.1.6.2.4.3	A report of any quality defect findings, regardless of severity, resulting from application of the QCP (CDRL A008) processes, including operationally induced failures, and organized by the associated TO against which the finding was discovered.	The Government will assess if the quality management process sufficiently tracks quality deficiency findings to perform corrective action and prevent future occurrence.	30 DAC and Annually	Application of events to algorithms to resolve quality deficiency findings.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
22	5.1.6.2.4.4	A status of small business allocation of work, by size and category, as required in section 1.5.14 of the JWCC PWS (CDRL A010).	The Government will assess if the portion of Small Business participation is sufficient.	365 DAC and Annually	N/A	Random Sample
23	5.1.6.2.4.5	AA status of both the identification of a financial system and the associated TO for System and Organization Control (SOC 1) Type II reporting as required in section 5.4 of the JWCC PWS and SOC Audit Report (CDRL A014)	The Government will assess if the contractor has sufficient insight to identify any financial system that is supported in the JWCC environment that requires a SOC I Type II report.	Annually	N/A	Random Sample
24	5.1.6.2.5	Any issues, challenges, problems, risk areas, or requests for JWCC COR support.	The Government will assess the contractors process for managing issues, challenges, problems, risk areas, or requests for the JWCC COR.	As required	A fully automated collaboration environment for remediation and mitigation.	100% Inspection
25	5.1.6.3	The Contractor shall attend and participate in meetings arranged, executed, and facilitated by the Government. The Government will coordinate a kickoff meeting for all Contractors receiving an award within 15 calendar days after contract award. The Contractor is responsible for coordinating with the JWCC COR. The kickoff meeting will be conducted in-person with the Contractor's primary staff that will interface with the JWCC PMO and will be held	The Government will assess if the contractor participation and contributions in the meeting is satisfying the goals and objectives of the meeting.	15 DAC and as required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		in the National Capital Region. The kickoff meeting will be conducted with all JWCC Contract holders in attendance at the same time. All JWCC Contract holders will be allowed one-on-one breakout sessions, if requested, for presentation of Contractor materials and any specific questions regarding the JWCC Contract.				
26	5.1.6.4	The Contractor shall arrange, execute, and facilitate meetings when requested by the JWCC PMO, or as required, in support of the JWCC Contract.	The Government will assess if the contractor is able to fully coordinate all Government requested meetings for the JWCC Contract by the JWCC PMO.	As required	N/A	100% Inspection
27	5.1.6.4.1	In-Progress Reviews (IPRs). The Contractor shall arrange, facilitate and execute quarterly IPRs, as well as any additional IPRs at the request of the JWCC KO or JWCC COR. IPRs will be conducted either in-person or virtually at the request of the Government, and the government reserves the right to include virtual attendees for in-person meetings. The Contractor is responsible for providing an agenda, presentation materials, and meeting minutes (CDRL A013) for all IPRs. Minimum content for IPRs shall include, but is not limited to, the following:	The Government will assess if the IPR content provides the Government with sufficient management insight to understand contractor contract performance.	As required	Real time automated tracking dashboard with continuous updates to IPR content.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
28	5.1.6.4.1.1	Overall JWCC Contract execution, management and operating status update;	Summary Requirement	N/A	N/A	N/A
29	5.1.6.4.1.2	Discussion, as necessary, of any upcoming JWCC Catalog changes in offerings (as captured in JWCC Catalog with Change Report (CDRL A022)), including addition, modification, deletion or deprecation;	The Government will assess the veracity of contractor catalog modification management.	On award and As required	N/A	Random Sample
30	5.1.6.4.1.3	Specific recommendations to better optimize JWCC Offerings, operations, and deployment based on empirical evidence, with projections for implementation of those recommendations;	The Government will assess if the Contractor is evaluating empirical data to identify optimization opportunities.	As required	Fully automated dashboard identifying where optimization opportunities exist.	Random Sample
31	5.1.6.4.1.4	Recommendation to improve communication between the Contractor and the JWCC COR;	The Government will assess if the Contractor is providing approaches to improve communications between the Contractor and the JWCC COR.	As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
32	5.1.6.4.1.5	Status of, and any issues regarding, use of and interfacing with ATAT;	The Government will assess if the Contractor is reporting ATAT operational issues consistent with ATAT's operations behavior.	As required	Fully automated dashboard identifying issues in real-time.	100% Inspection
33	5.1.6.4.1.6	Identification of JWCC Contract issues or problems, with regard to management or operations of the JWCC Contract, and the associated risks and mitigation plan;	The Government will assess if the Contractor is identifying issues and problems consistent with identified operating challenges.	As required	Fully automated reporting mechanism identifying issues and problems.	100% Inspection
34	5.1.6.4.1.7	Advising on the utilization of JWCC Contract and how it aligns to the commercial trends and practices;	The Government will assess if the Contractor is proposing commercial terms and practices that would benefit the DoD.	As required	A fully automated optimization model that identifies commercial trends and practices that the DoD would benefit from.	100% Inspection
35	5.1.6.4.1.8	Advising on establishing optimization goals with recommendations to achieve the goals; and for prior goals, a status of progress to achieve the goal and an anticipated completion date;	The Government will assess if the Contractor is assisting the Government with identifying optimization goals for JWCC opportunities.	As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
36	5.1.6.4.1.9	Discussion of any previous quarter C3PO required reports submitted to the JWCC COR;	The Government will assess if C3PO findings are packaged in a quarterly report and discussed with the JWCC COR	As required	N/A	100% Inspection
37	5.1.6.4.1.10	Any Government agenda items provided to the Contractor for inclusion in the scheduled IPR;	The Government will assess if the agenda items are presented in a timely fashion for inclusion in the IPR.	As required	N/A	100% Inspection
38	5.1.6.4.1.11	Report on status of, and any issues regarding, exceptions. (CDRL 0024)	The Government will assess if the Contractor is properly managing existing and new exception requests	As required	N/A	100% Inspection
39	5.1.6.4.2	Technical Exchange Meetings (TEMs). As requested by the JWCC COR, the Contractor shall arrange, facilitate and execute TEMs. TEMs can include discussions of any current or upcoming TOs, any future cloud offerings, JWCC Offerings and Commercial Offerings the Contractor will have available for purchase, and any content/topics determined by the JWCC COR or the JWCC PMO. The Contractor is responsible for providing	The Government will assess if the Contractor is supporting all the requested TEMs.	As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		meeting minutes (CDRL A013) for all TEMs.				
40	5.1.6.4.3	Ad Hoc Reporting/Information Products. The Contractor shall work with the JWCC COR to identify required ad hoc reports or information products related to deployment and utilization of the JWCC Contract. These reports or products will be used to assist the JWCC COR for effective deployment of the JWCC Contract. This reporting is in addition to other reporting requirements mentioned herein.	The Government will assess if the Contractor is responsive to all ad hoc reporting and information requests.	As required	N/A	100% Inspection
41	5.1.6.5	Ordering Guide Inputs.	Summary Requirement	N/A	N/A	N/A
42	5.1.6.5.1	The Contractor shall address, as part of the Contract Ordering Guide Annex (CDRL A007), any specific information that users need to understand how to successfully order JWCC Offerings, TE offerings, cloud support packages, and online JWCC marketplace offerings, to include BYOL offerings, to be included in the JWCC Ordering Guide.	The Government will assess if the ordering guide is complete and useful for a JWCC user to navigate and successful provision from the marketplace.	10 DATO and As required	Fully automated, intuitive navigation and self-help environment that is routinely updated without annex submissions.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
43	5.1.6.5.1.1	Contractor's PoC information and e-mail for contracting related issues.	The Government will assess if email addresses and POCs are accurate.	10 DATO and As required	N/A	100% Inspection
44	5.1.6.5.1.2	Contractor's email address for distribution of TOs (if different from above).	The Government will assess if email addresses and POCs are accurate.	10 DATO and As required	N/A	100% Inspection
45	5.1.6.5.1.3	Link to Contractor's hosting and compute calculators (hereafter referred to as "Calculators") at each classification level for the purpose of Independent Government Cost Estimate development that identifies only those offerings JWCC Offerings that are authorized for DoD consumption under the JWCC Contract.	The Government will assess if the link is accurate and operational at each classification level.	10 DATO and As required	N/A	100% Inspection
46	5.1.6.5.1.4	Any specific process the Contractor may have for requesting TE Offerings that deviates from the normal fulfillment process.	The Government will assess if the non-standard marketplace process maintains appropriate TE offerings fulfillment management.	10 DATO and As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
47	5.1.6.5.1.5	Any specific process the Contractor may have for requesting Cloud Support Packages.	The Government will assess the processes for requesting Cloud Support Packages.	10 DATO and As required	N/A	100% Inspection
48	5.1.6.5.1.6	The Contractor's inputs to the Contract Ordering Guide Annex shall be delivered to the Government (CDRL A007).	The Government will assess if the ordering guide annex sufficiently describes the process.	10 DATO and As required	N/A	100% Inspection
49	5.1.6.6	Contractor Cloud Portal Process. The Contractor shall provide to the JWCC COR the process of establishing initial accounts and Cloud Environments using the Contractor's Portal (both UI and API) and how to fulfill orders and provision/deploy JWCC Offerings from its JWCC Marketplace after the JWCC user account has been established. The Contractor Cloud Portal Process (CDRL A002) shall be delivered to the Government no later than 15 days after contract award and as necessary when changes are made. Only JWCC Offerings that are part of the JWCC Catalog shall be visible and accessible in the JWCC Marketplace. A link (via Internet Protocol address) to the Contractor's Portal will be provided by Contractor for distribution to JWCC users for each classification level and IL.	The Government will assess if the Contractors process for establishing initial accounts and cloud environments meets the JWCC requirements.	15 DAC and As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
50	5.1.6.7	<p>JWCC Catalog. The Contractor shall submit its Commercial Catalog with Change Report and any changes (CDRL A023). The Contractor's Commercial Catalog shall be the basis by which the JWCC Catalog is established. The Contractor shall submit its JWCC Catalog as Attachment J-4: JWCC Catalog Discounts, Premiums, and Fees. For additions or modifications to JWCC Offerings, the Contractor shall follow the process in G11, JWCC Catalog Modifications, and submit the JWCC Catalog with Change Report (CDRL A022). The Contractor shall support the JWCC KO/COR in the maintenance and upkeep of the JWCC Catalog by recording and reporting changes on a periodic basis via JWCC Catalog with Change Report (CDRL A022).</p> <p>JWCC Catalog. The initial JWCC Catalog submission (CDRL A023) shall include all commercial offerings and the current status of DoD Authorization (Provisional Authorization) for each offering and the offering's applicable classification level and IL, which is viewable by DoD user only. (Note: The IC is not part of the DoD for this instruction). The Contractor shall support the JWCC KO/COR in the maintenance and upkeep of the JWCC Catalog by recording and reporting changes on a periodic basis (CDRL A022).</p>	The Government will assess if the Contractors catalog submission meets the requirements of the JWCC contract.	On award and As required	N/A	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
51	5.1.6.8	<p>Quality Control Plan (QCP). The Contractor shall provide a QCP supporting the Government-provided QASP for the JWCC Contract (see Attachment L-6). At a minimum, the QCP shall describe the approach for continuously meeting the performance metrics in Technical Exhibit 1 of the JWCC PWS, throughout the life of the JWCC Contract. The Contractor shall specifically address how all required performance metrics will be assessed, analyzed, and maintained through the life of the JWCC Contract. Cross-referencing between the QCP and PWS is permitted.</p>	<p>The Government will assess if the QCP describes the processes to ensure quality delivery of JWCC offerings.</p>	<p>30 DAC and Annually</p>	<p>N/A</p>	<p>100% Inspection</p>
52	5.1.6.8.1	<p>The Contractor shall provide a PoC as part of the QCP to allow any JWCC user to communicate any issues or failures that arise from an attempt to invoke a JWCC Offering (provisioning) as ordered within a valid JWCC account. The contractor shall provide near-immediate acknowledgement (within 5 minutes of submission). The Contractor will action these communications IAW their QCP and any relevant support package SLAs associated with the JWCC users' identified TO. This PoC shall be available 24 hours a day, 7 days a week, 365 days a year, worldwide without any charges or expense to the Government. The modalities of contact shall include, at a minimum, voice (telephone), web-access (i.e. Contractor's Portal), and e-mail. The e-mail response timeline is within one hour of receipt and a response within five minutes of opening the e-</p>	<p>The Government will assess if the QC PoC information is compliant with the requirement.</p>	<p>As required</p>	<p>N/A</p>	<p>100% Inspection</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		mail. This PoC shall be available for all classification levels and ILs such that JWCC users can communicate the issue at the classification level they are currently operating at.				
53	5.1.6.9	TE Device Loss, Destruction, or Inoperability. Post award, the Contractor shall report on the number of TE Devices that have been lost, destroyed, or rendered inoperable for each device and circumstance and the total for each circumstance. This information shall be reported in the CMPR (CDRL A001) at the JWCC Program level and reported monthly at the TO level.	The Government will assess if the contractor has provided the appropriate information regarding TE Loss, Destruction, or Interoperability.	As required	N/A	Random Sample
54	5.2	Activities to Assess and Authorize Contractor's Cloud Infrastructure and Offerings	Summary Requirement	N/A	N/A	N/A
55	5.2.1	The Contractor shall conduct any activities necessary to receive DoD authorization for all XaaS and TE Offerings at each classification level and IL, for inclusion on the JWCC Catalog.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	As required	N/A	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
56	5.2.2	The Contractor shall maintain any authorization achieved for the duration of the JWCC Contract, and any TO awarded thereunder, to include conducting continuous audit assessments and, as needed, management reviews as requested by the JWCC KO or AO.	The Government will audit all authorizations achieved for the duration of the contract to ensure a continuous authorization state is maintained for qualified services and offerings.	As required	N/A	Random Sample
57	5.2.3	The Contractor shall prepare and submit a sufficiently complete Security Authorization Package (CDRL A009) to demonstrate compliance with all applicable requirements in C3PO, including all invoked references and their requirements.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	As required	N/A	Random Sample
58	5.3	Multi-Cloud Solution Technical Exchange Meetings (TEMs)	Summary Requirement	N/A	N/A	N/A
59	5.3.1	The Contractor shall participate in multi-cloud solution TEMs (including interoperability discussions) with other Federal and DoD contractors, including CSPs, with the goal of exploring novel solutions to optimize and streamline multi-vendor solutions and approaches for the benefit of the DoD, at the TO level. The TEMs will be convened as directed by the TO COR.	The Government will audit if the Contractor is both represented in TEMs and actively participating and contributing.	As required	N/A	100% Inspection
60	5.4	System and Organization Control (SOC 1) Type II Reporting	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
61	5.4.1	The Contractor shall provide a SOC Audit Report (CDRL A014) as listed in the memorandum, "System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers," dated May 2, 2019.	The Government will audit if the SOC Audit Report is compliant with the required content and delivered in a timely manner.	Annually	The SOC Audit Report will be exhaustive in content and delivered in a timely manner.	100% Inspection
62	5.5	JWCC Timeline and Technical Requirements. The Contractor shall provide XaaS for Government consumption at all classification levels and ILs, within the JWCC Catalog (Attachment J-4), discernable by classification level and IL. The requirements in this section are a minimum capability, condition, or attribute of JWCC. All requirements within the PWS are subject to the timelines below and commensurate with their classification level, unless otherwise specified.	Summary Requirement	N/A	N/A	N/A
63	5.5.1	Timeline. Delivery of XaaS, including TE Offerings, will follow the timelines as listed below, unless otherwise specified.	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
64	5.5.1.1	Roadmap//Integrated Master Timeline (CDRL A019). The Contractor shall provide a roadmap and integrated master timeline, or a combined artifact (hereafter referred to as, "Roadmap/Integrated Master Timeline") that has each information set clearly discernible within the single artifact, that contain sufficient detail documenting how and when JWCC requirements will be met. The Roadmap/Integrated Master Timeline shall include indicators for every offering current and potential future Offering to track successful or unsuccessful outcomes presented in the Roadmap/Integrated Master Timeline for delivery and operability.	The Government will assess whether the Roadmap/Integrated Master Timeline (CDRL A019) provides sufficient content and detail and is submitted on time. The measure will be no more than 5% of offerings unaccounted for in the Roadmap/Integrated Master Timeline, including current, deprecated, and removed items.	DAC/DATO and Monthly	The Roadmap/Integrated Master Timeline fully details the duration of the contract with no offerings left unaccounted.	Random Sample
65	5.5.1.2	Unclassified Timeline. The Contractor shall provide its UNCLASSIFIED Offerings at ILs 2, 4, and 5 at immediately upon JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as UNCLASSIFIED Offerings, including UNCLASSIFIED TE offerings. At Offerings. No later than the JWCC Contract award date, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, and submit Security Authorization Package(s) (CDRL A009).	The Government will assess whether all UNCLASSIFIED offerings and TE offerings meet all security requirements as defined in C3PO and are delivered at time of award. The Government will assess whether any UNCLASSIFIED (IL 2, 4, or 5) offerings that have not been previously authorized are delivered to, and include all documentation required by the AO, at JWCC Contract award.	As required	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
66	5.5.1.3	<p>Classified Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the SECRET (IL 6) level, within 60 days after JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as SECRET JWCC Offerings, including SECRET TE Offerings. Within 60 days post-JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254, and submit Security Authorization Package(s) (CDRL A009).</p>	<p>The Government will assess whether CLASSIFIED offerings at the SECRET (IL 6) level and TE offerings meet all security requirements as defined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254. The Government will assess whether CLASSIFIED offerings supporting SECRET (IL 6) level workloads and TE offerings were made available for use/authorization by the DoD within 60 days after JWCC Contract award. The Government will assess whether any SECRET (IL 6) level offerings that have not been previously authorized are delivered to, and include all documentation required by the AO, within 60 days after JWCC Contract award.</p>	As required	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
67	5.5.1.4	<p>Classified Top Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the TOP SECRET (including (TS/SCI)) level, within 180 days after JWCC Contract award, such that DoD will have the ability to deploy and use (immediately upon authorization) these Offerings as TS JWCC Offerings, including TE Offerings (TS and TS/SCI). Within 180 days post-JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization for all TS JWCC Offerings. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, and IC Directive (ICD) 503 (TS and TS/SCI), and submit Security Authorization Package(s) (CDRL A009).</p>	<p>The Government will assess whether CLASSIFIED offerings capable of supporting TS and TS/SCI workloads meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, and IC Directive (ICD) 503 (TS and TS/SCI). The Government will assess whether CLASSIFIED Services supporting TS and TS/SCI workloads and TE offerings were made available for use/authorization by the DoD within 180 days after JWCC Contract award. The Government will assess whether, for any services that have not been previously authorized, all documentation required is delivered to the AO, within 180 days after JWCC Contract award.</p>	As required	<p>The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.</p>	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
68	5.5.1.5	<p>Special Access Programs (SAP) Timeline. The Contractor shall support securely hosting SAP workloads, such that the DoD will have the ability to accomplish SAP missions using Contractor-provided JWCC Offerings IAW DoDD 5205.07, DoDM 5200.01, and the Joint Special Access Program Implementation Guide (JSIG). These JWCC Offerings shall be delivered consistently with the timelines for UNCLASSIFIED, SECRET, and TOP SECRET with documentation and evidence demonstrating compliance with SAP controls. The Contractor shall provide any additional documentation and artifacts as required by the corresponding SAP AO, per SAP workload, and submit Security Authorization Package(s) (CDRL A009).</p>	<p>The Government will assess whether the ability to host SAP workloads meet all security requirements IAW DoDD 5205.07, DoDM 5200.01, and the JSIG at the UNCLASSIFIED, SECRET and TOP SECRET classification levels. The Government will assess whether documentation and evidence demonstrates compliance IAW DoDD 5205.07, DoDM 5200.01, and the JSIG in order to be approved for hosting SAP workloads.</p>	As required	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering.	100% Inspection
69	5.5.1.6	<p>Cross-Domain Solution (CDS) Timeline. The CDSs shall meet the DoD's requirements as described in section 5.5.8.2. The Contractor shall provide CDSs for the Management Plane in conjunction with the associated CLASSIFIED Infrastructure and JWCC Offerings, on or before the delivery of that CLASSIFIED Infrastructure and JWCC Offerings. The CDSs for the Production Plane shall be provided to the DoD within 180 days after the delivery of the associated CLASSIFIED infrastructure and JWCC Offerings. All provided CDSs shall be authorized for use by the DoD Information Security Risk Management</p>	<p>The Government will assess whether a CDS that meets the requirements in 5.5.8.2 was made available to the DoD IAW the timeline required for each classification level as it applies to the management plane and production plane. The Government will assess whether all required documentation is made available to the ISMRC for authorization.</p>	As required	The process for requirements compliance is fully automated and presented in a continuously updated report for each CDS.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		<p>Committee (DoD ISMRC). For any CDS that is not presently authorized, the Contractor shall provide all documentation and artifacts required for CDS authorization to the DoD ISMRC in conjunction with the delivery of the associated CDS, and submit Security Authorization Package(s) (CDRL A009).</p>				
70	5.5.1.7	<p>Advisory and Assistance Services. The Contractor shall provide advisory and assistance services, as part of its Cloud Support Package, available at all classification levels and ILs IAW the service delivery timelines listed above, in order for JWCC users to acquire advisory and assistance services from the Contractor to support use of JWCC Catalog Offerings. The Contractor-provided advisory and assistance services shall meet DoD's requirements as outlined in section 5.5.11.</p>	<p>The Government will assess whether advisory and assistance services are available for the JWCC on the same timeline as the UNCLASSIFIED, SECRET, and TOP SECRET offerings, and whether such services meet the requirements in 5.5.11.</p>	As required	<p>The advisory and assistance services are available prior to offerings (roadmap/timeline based) to enable pre-planning.</p>	Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
71	5.5.2	<p>Available and Resilient Services. The Contractor shall provide Highly Available, resilient CSOs that are reliable, durable, and able to continue operating despite catastrophic failure of portions of the infrastructure. Infrastructure used in the performance of CSOs under JWCC shall be capable of supporting globally dispersed users at all classification levels, including DDIL environments, and Closed-Loop Networks. In order to provide the resiliency and availability required by JWCC users, there must be no fewer than three physical Data Center locations with the ability to operate independently, each including the ability for JWCC users to deploy and manage CSOs at its respective classification level and IL. At least two of the Data Centers must be geographically dispersed by at least 400 miles, utilizing separate power grids, and within the Customs Territory of the United States, as defined in FAR 2.101. UNCLASSIFIED and CLASSIFIED (both SECRET and TOP SECRET) Data Centers may be co-located, as long as the CLASSIFIED Data Center meets FCL requirements IAW C3PO and Attachment J-3: JWCC DD254.</p>	Summary Requirement	N/A	N/A	N/A
72	5.5.2.1	<p>The Contractor shall provide dynamic scalability and resiliency through industry standard mechanisms and activities to ensure the DoD has the ability to maintain continuous operations.</p>	<p>The Government will perform testing of offerings deployed and operating within JWCC for scalability, resiliency,</p>	As required	<p>The offerings will be automatically scalable and resilient.</p>	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			performance, cybersecurity, and cyber survivability.			
73	5.5.2.2	The Contractor shall provide the ability for JWCC users to create system configurations, both manually (i.e. via Contractor Portal (UI)) and through APIs, to provide automated redundancy of storage, networking, and computing systems in the case of catastrophic data center loss or loss of CSOs.	The Contractor will demonstrate at least annually how JWCC users can configure CSOs both manually, via the Contractor's Portal, and via the API, for high availability and resiliency such that it can survive catastrophic data center loss or loss of capabilities.	As required	All CSOs have a native API for high availability and resiliency as well as a single click (per CSO) to enable typical high availability features.	Periodic Sample
74	5.5.2.3	The Contractor shall provide CSOs that are Highly Available and resilient. Accordingly, the Contractor's minimum Data Center capabilities are as follows:	Summary Requirement	N/A	N/A	N/A
75	5.5.2.3.1	Every data center shall be capable of automated replication and failover of CSO(s) within each respective classification level and IL inclusive of the ability to provision, configure, and manage services, such that the DoD is provided Data Center agnostic operations.	The Contractor will demonstrate, at least annually, through design documentation, physical exercise, or any combination thereof, the ability to failover a data center with no lasting impact to Government operations (e.g., browser refresh due to network redirection to a new data center is understandable, but loss of data which should have been synchronized with a secondary	At least annually	All failovers are fully automated and there is no appreciable downtime (99.99999%) for any offering	Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			facility is unacceptable.)			
76	5.5.2.3.2	The Contractor shall, at time of award, provide no fewer than two physical Data Centers offering providing UNCLASSIFIED CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide UNCLASSIFIED CSOs. The Government reserves the right to inspect any facility used to host JWCC workloads.	As required	The Contactor will have at least two data centers for every Contractor defined Operating region and each region is a minimum of 400 miles apart.	100% Inspection
77	5.5.2.3.3	The Contractor shall, upon delivery of SECRET CSOs, provide no fewer than two physical Data Centers offering providing SECRET CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide SECRET CSOs for JWCC. The Government reserves the right to inspect any facility used to host JWCC workloads.	As required	The Contactor will have at least two data centers for every Contractor defined Operating region and each region is a minimum of 400 miles apart.	100% Inspection
78	5.5.2.3.4	The Contractor shall, upon delivery of TS CSOs, provide no fewer than two physical Data Centers offering providing TS CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide TOP	As required	The Contractor will have at least two data centers for every Contractor defined Operating region and each region	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			SECRET CSOs for JWCC. The Government reserves the right to inspect any facility used to host JWCC workloads.		is a minimum of 400 miles apart	
79	5.5.2.3.5	The Contractor shall, no later than 18 months after contract award, provide no fewer than three physical Data Centers offering providing CSOs at each classification levels and ILs. At least two of these three physical Data Centers shall be geographically dispersed by a minimum of 400 miles, by radial measurement, utilizing separate power grids as defined by the Office of Electricity within the U.S. Department of Energy, and within the Customs Territory of the U.S., as defined in FAR 2.101.	The Government will assess whether the locations of the physical data centers are geographically dispersed and utilize separate power grids. The Government reserves the right to inspect any facility used to house JWCC workloads.	As required	All data centers will be serviced using fully independent utility resources.	100% Inspection
80	5.5.2.3.6	The physical data centers at all classification levels and ILs shall strictly comply with all applicable C3PO requirements.	The Government will assess the sufficiency of data center compliance with respect to C3PO will advise the Contractor of any deficiencies for resolution.	As required	All data centers will exceed C3PO standards.	100% Inspection
81	5.5.2.4	The Contractor shall provide, at each classification level and IL, automatic monitoring of resource utilization and events (to include failures and degradation of service) via web interface and documented APIs that are intuitive and easy to use.	The Contractor will demonstrate its monitoring capabilities to the Government, at least annually, at each classification level and IL. In addition, the Government may audit, at any time and via any reasonable method, the Contractor's	The Contractor at least annually, the Government may audit at anytime	All events are fully logged and pre-emptive automated system actions are taken to negate degradation and threat events.	Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			monitoring capabilities.			
82	5.5.3	Globally Accessible. The Contractor shall provide CSOs that are securely accessible worldwide via the Contractor's Portal (UI), at all classification levels and ILs. The CSOs shall provide assured access and enable interoperability between Virtual Enclaves containing applications and data.	Summary Requirement	N/A	N/A	N/A
83	5.5.3.1	The Contractor shall have points of presence on all continents, with the exception of Antarctica, providing a total bandwidth capacity of at least 40 Gigabits per second, using redundant links, to peer with the DoD on each continent. If the DoD adds new locations, the Contractor shall peer with the DoD within 12 months of notification such that the latency between the Contractor's and the DoD's locations is less than 8 milliseconds. The Contractor shall provide documentation that validates the transmission speeds, latency, and bandwidth at each location.	The Government will assess, through review of documentation, site inspection, or any combination thereof, whether the Contractor has points of presence on all continents, with the exception of Antarctica, and that those points of presence have redundant links with a total bandwidth of at least 40 Gigabits per second as measured by network bandwidth tools. The Government will assess the Contractor's peering activities to ensure compliance with the 12 month peering notification requirement.	As required	All Points of Presence support maximal bandwidth capability offered and dynamic automated peering services are available.	100% Inspection and Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
84	5.5.4	<p>Centralized Management and Distributed Control. The Contractor shall permit the DoD to exert necessary oversight and management of CSOs. This oversight and management includes, but is not limited to: the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process. In order to exercise centralized management, the Contractor shall have a mechanism for activating and deactivating any CSO for JWCC workspaces. The Contractor shall provide a mechanism to provision CSOs based on standardized, templated configurations and security policies, as well as a “user friendly” mechanism to deprovision any combination of CSOs (e.g. one, multiple, or all). The Contractor shall also provide as part of its solution object and resource access control management, including data and resource tagging for billing tracking, access control, and technical policy management. The Contractor shall facilitate the automation of central management and distributed control. The Contractor shall provide an actively maintained, versioned, and documented API providing the ability to perform any operation supported by the Contractor’s Portal (UI).</p>	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
85	5.5.4.1	The Contractor shall provide the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process to give the DoD the ability to enforce its policies and security compliance for the JWCC Contract workloads.	The Government will assess whether the Contractor has provided the Government the ability to enforce security policies and standardized configurations in a manual and automated manner.	As required	All policy configurations can be generated and visualized using a Contractor's Portal (UI) tools and the policy application is immediate and comprehensive. Additionally, all compliance can be easily reported and visualized.	Random Sample
86	5.5.4.2	The Contractor shall provide the ability to enable and disable services and restrict parameters within service configurations via both the Contractor's Portal (UI) and API, in a manner that is easy to use such that the JWCC COR and administrative JWCC users within the DoD can properly control service delivery to the greater JWCC user community. This ability to restrict services shall allow for hierarchical subordinated supplemental constraints.	The Contractor will demonstrate, at least annually, the ability to perform the enablement and disablement of services with a sufficient number of parameters via the Contractor's Portal (UI) and API to the JWCC COR and include in their documentation and training material instructions on how to perform these activities. Additionally, the allowance for hierarchical subordinated supplemental constraints must also be demonstrated. The Government will assess the sufficiency of the demonstration and the provided documentation, and may audit, at any time and via any reasonable	As required	The control of services (enable/disable) and all associated parameters can be controlled via a Contractor's Portal (UI), trigger-sensing API, or heads-up UI. The hierarchical inheritance model will be automatically applied.	Periodmethodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			method, the Contractor's ability to enable and disable services.			
87	5.5.4.3	The Contractor shall provide object and resource management capabilities, including data and resource tagging for billing tracking, access control, and technical policy management in order for the DoD to properly administer the JWCC Contract.	The Government will assess whether the Contractor has the ability to provide object and resource management capabilities; including billing trackers, access controls and technical policy mandates that are inherited from the parent organizations. The Government reserves the right to perform periodic testing of these capabilities.	As required	All cloud resources are manageable using API or a Contractor's Portal (UI), in a central and distributed model.	Random Sample
88	5.5.4.4	The Contractor shall provide an API that supports encryption and authentication as defined in C3PO for all JWCC users and sessions, for each XaaS at all classification levels and ILs. The API shall, at a minimum, be capable of the following:	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
89	5.5.4.4.1	IAM controls, including account creation and management in support of the JWCC Contract, token-based and time-limited federated authentication, role-based access control configuration, and specific account permissions.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	Full PBAC is implemented for all offerings	Procedural inspection and Random Sample
90	5.5.4.4.2	Provisioning and management (i.e. IaaS) of network configuration, compute instances, data and object storage including database management systems, and tools for scaling systems (e.g. application server load balancing).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	All cloud configurations have provisioning scripts in a central virtually accessible library that is dynamically populated if a new configuration arises.	Periodic Sample
91	5.5.4.4.3	Storage object lifecycle management (e.g. moving data from online to nearline after a set time period).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	All objects have a parametric tag that is dynamically managed to provide the most appropriate storage type. Additionally the ability to configure objects to change storage type based on AI/ML learning algorithms trained on access and interaction data based on file type, location, other policy information, or any combination thereof.	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
92	5.5.4.4.4	Reading usage data and alerts for compute, storage, and network utilization (e.g. resource/performance monitoring and utilization).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	Automated parametric response triggers are programmatically executed on achieving specific conditions.	Procedural Inspection
93	5.5.4.4.5	Reading accrual, historical billing, and pricing data specified under the entire JWCC Contract to include data for: CSOs, Cloud Support Packages, and workspaces.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	Automated parametric response triggers are programmatically executed on achieving specific conditions.	Procedural Inspection
94	5.5.4.4.6	Setting billing and usage thresholds and adding automated notifications to workspace owners and the TO COR as well as a capability to configure the discontinuation of service upon the billing and usage threshold breach.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	As required	Automated parametric response triggers are programmatically executed on achieving specific conditions.	Procedural Inspection
95	5.5.4.4.7	Accessibility to all JWCC users provided they have the proper access control authorization.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform	As required	Automated parametric response triggers are programmatically executed on achieving specific conditions.	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			periodic testing of these capabilities.			
96	5.5.4.5	The Contractor's APIs, at all classification levels and ILs, shall be actively maintained, versioned, documented, and adhere to industry best practices for modern standards and protocols. API documentation shall contain information on: how to establish a connection, support protocols, security requirements, and capabilities available.	The Government will assess the Contractor's API documentation (e.g. release notes) to ensure sufficient detail and consistency for changes implemented such that the Government can determine the nature of the change, potential impact, actual impact, or any combination thereof, on current operations.	As required	All APIs are fully self-documented. All API changes are both human and machine consumable for automated change analysis.	Random Sample
97	5.5.4.5.1	The Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs, of any change to API capabilities impacting backwards compatibility at least 30 days prior to the change being put into production. Alternately, if the change is to address a critical vulnerability, as designated by the Critical Vulnerability Scoring System, the Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs within 24 hours of the change. Additionally, the Contractor shall make available this same information to all DoD personnel and other authorized JWCC users.	The Government will assess whether the Contractor has adhered to notification time frames for API changes.	As required	All API changes will include full back-compatibility and test spaces are provided which allow for users to perform test calls to the new API prior to its full implementation.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
98	5.5.4.5.2	The Contractor shall provide full API documentation online (to include examples of code). Full API documentation shall be readily discoverable within three clicks from the Contractor's Portal(s) (UI) landing page. API documentation shall also be available on TE Devices operating in DDIL environments.	The Government will assess whether the API online documentation is accessible within the required parameters at all classification levels and ILs to include TE Devices operating in a DDIL environments. Tailoring of the APIs may be necessary across classification levels and ILs, to include TE Devices and the documentation must be tailored to document any changes to the API and its parameters (i.e., if variables, features, or flags deviate from the commercial baseline they must be clearly documented and supported until such time as commercial parity can be established.)	As required	All API documentation is accessible from a fully automated repository that supports dynamic query and retrieval capabilities for both API driven and Contractor Portal (UI) users. Example code would further include tutorials and supporting files/information required to ensure users can fully grasp how to utilize the API.	Random Sample
99	5.5.4.5.3	The Contractor API shall provide the ability to perform any command supported by the Contractor's Portal (UI).	The Government will assess the ability to perform API calls and the corresponding Contractor Portal activity as a part of regular business and inform the Contractor of any deficiencies.	As required	The Contractor will self certify and provide automated tools which can empirically demonstrate compliance with this requirement with less than 1 percent of the API calls being deviant.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
100	5.5.4.6	<p>The Contractor shall provide a fully compliant implementation of the ATAT Multi-Cloud Provisioning API (Attachment J-11) at each classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for test workloads within 15 days of providing JWCC Offerings at the associated classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for production workloads within 30 days of providing JWCC Offerings at the associated classification level and IL. The Contractor implementation shall be pursuant to Attachment J-11: ATAT Multi-Cloud Provisioning API, to enable ATAT to execute calls to the API resulting in standardized mechanisms for:</p> <p>Creation & management of access credentials for accounts and environments in which CSOs can be provisioned.</p> <p>Creation and management of portfolios which manage groups of accounts and environments. The deadline by which the Government expects the portfolio provisioning process to be complete is dictated within the ATAT Multi-Cloud Provisioning API (Attachment J-11).</p> <p>Obtaining actual and projected costs per CLIN, environment, workloads, and portfolio.</p> <p>Setting billing limits with notifications on CLINs,</p>	<p>The Government will assess whether ATAT calls to the Contractor's ATAT Multi-Cloud Provisioning API implementation(s) to create and manage portfolios, accounts, environments, or any combination thereof are successful, that the implementation conforms to the API specifications in J-11, and that the expected outcomes of the API call is achieved in the Contractor's cloud environment. The Government will assess if the implementation conforms to the API specification and that ATAT calls to the Contractor's ATAT Multi-Cloud Provisioning API implementation can obtain actual and projected costs per environment, workload, and portfolio and set billing limits and notifications on environments, workloads, and portfolios.</p>	As required	All ATAT API features are fully implemented and properly working. A fully configured sandbox and test harness exists to emulate a parallel ATAT production instance for robust testing including performance conditions allowing for DevSecOps processes to enable constant iteration and improvement.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		environments, workloads, and portfolios.				
101	5.5.4.7	The Contractor shall update its ATAT Multi-Cloud Provisioning API implementations to the latest version of the ATAT Multi-Cloud Provisioning API definition within 30 days of Government notification for general updates, and within seven days for security updates.	The Government will assess whether the Contractor has implemented the latest version and functionality of the ATAT Multi-Cloud Provisioning API to maintain continued compliance with	As required	The Contractor's implementation is updated within 1 business day for all updates to the ATAT Multi-Cloud Provisioning API with no explicit notification from the Government	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			the published API requirements within the required timelines.		required at all classification levels and ILs.	
102	5.5.4.8	The Contractor's implementation of the ATAT Multi-Cloud Provisioning API shall provide services comparable to the Contractor's other APIs in terms of API service delivery performance.	The Government will test the Contractor API implementation for availability, scalability, and other parameters as part of the Contractor SLA for API services.	As required	The Contractor's API implementation supports continuous operations for scale, and all parametric permutations at all classification levels and ILs.	Random Sample
103	5.5.4.9	The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government has the ability to control any CSO for a subset of the JWCC users or grouping of JWCC users based on individual AO's risk tolerance(s).	The Government will assess, at least annually, whether the Contractor is providing the Government the ability to activate or deactivate, any or all of the Contractor's CSO under the JWCC Contract for an individual workspace	As required	The activation/deactivation is capable of being done from the Contractor's Portal (UI), the API, and current status visualizations from both the Contractor's Portal (UI) and API are available for consumption.	Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
104	5.5.4.10	The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government can activate or deactivate any CSO for all of the JWCC users based on DoD Authorization status or cybersecurity needs.	The Government will assess, at least annually, whether the Contractor is providing the Government the ability to perform activate or deactivate, for all workspaces simultaneously, any cloud service offering being provided by the Contractor under the JWCC Contract.	As required	The activation/deactivation is capable of being done from the Contractor's Portal (UI), the API, and current status visualizations from both the Contractor's Portal (UI) and API are available for consumption.	Periodic Sample
105	5.5.4.11	The Contractor shall provide an IaC CSO, which allows the deployment and provisioning of one or more other CSOs. This IaC CSO will use pre-made standardized configurations and allow for customizable configurations. This IaC CSO shall also include a simple mechanism to deprovision any and all CSOs it deployed or provisioned.	The Government will assess whether the Contractor is providing the Government the ability to deploy a standardized configuration of cloud resources, including security policies, as well as the ability to deprovision in compliance with the configuration specification.	As required	Support for a fully programmable API and a Contractor Portal (UI) is available to deploy and deprovision resources for dynamic configurations and direct input with associated visualizations for current status.	Procedural Inspection
106	5.5.4.12	The Contractor shall not bundle any JWCC Offerings in a manner that restricts a JWCC user's ability to acquire individual JWCC Offerings. Any bundled JWCC Offerings shall also be available as discrete JWCC Offerings.	The Government will assess whether all services that are combined to form a different service offering are available separately, allow the user to acquire each service independently, and are billable as a single item.	As required	All offerings are discretely available and any combination or aggregation permutation is supported.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
107	5.5.4.13	The Contractor shall not require any third-party services that require separate billing, separate licensing, or a combination thereof in order to meet the JWCC requirements or minimum requirements for using any JWCC CSO. Any third-party services that are fully integrated with the Contractor, hosted on the Contractor's infrastructure, and directly supported by, billed through, and licensed by the Contractor are not subject to this requirement.	The Contractor shall certify compliance with this requirement and the Government will assess compliance through the course of doing business with no identified exceptions to this requirement.	As required	The Contractor shall empirically demonstrate compliance to the requirement with comprehensive documentation and self certification.	Random Sample
108	5.5.4.14	The Contractor shall provide prompt notification and follow-up reporting on all service incidents, outages, and other problems (hereafter collectively referred to as, "Service Incident Events") impacting JWCC users or cloud operations. The following minimum requirements apply to all environments, including network and TE Devices:	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
109	5.5.4.14.1	The Contractor shall establish and utilize Service Incident Event management processes, as well as support accessibility and escalation processes, such that the Contractor is able to prioritize and manage response reactions while keeping users informed about Service Incident Event status, remediation schedule, and overall priority amongst all other current Service Incident Events.	<p>The Government will assess whether the Contractor's Service Incident Events management process ensures that each incident is fully traceable through each step of the Contractor's Service Incident Event management process such that:</p> <p>Incident escalation mechanisms are clearly observable and course of action adjustments are captured.</p> <p>Full logging is enabled for each incident and all remediation actions are captured in persistent logs</p>	As required	Service Incident Event Management is fully automated and 100% activity is logged and analyzed for optimization opportunities and auditing for security best practices.	Random Sample
110	5.5.4.14.2	The Contractor shall notify the impacted JWCC users, the JWCC COR, and TO CORs once a Service Incident Event has been detected or discovered. The Contractor shall notify the users, via electronic means, including severity level, for each Service Incident Event. Service Incident Event notifications shall be made IAW the SLA.	The Government will assess the timely delivery of notification for each Service Incident Event.	As required	The notification system is multi-modal and each user is able to select any combination of notification modes for their individual needs.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
111	5.5.4.14.3	<p>The Contractor shall provide updates on Service Incident Event reports to include the impacted JWCC users, the JWCC COR, and TO CORs. The updates shall be provided at intervals IAW the SLO with the SLA, until the Service Incident Event is completely resolved. Updates shall include supplemental Service Incident Event information to aid in understanding the Service Incident Event's scope, severity, and resolution progress, clearly identifying any outage(s) or other significant problems.</p>	<p>The Government will assess whether the Contractor has provided timely updates based on each Service Incident Events evolving status. The Government will assess whether such updates provide sufficient information and are in compliance with the SLOs.</p>	As required	<p>Updates for a Service Incident Event are provided automatically to every impacted user in real-time. Additionally update information is provided to an advanced data analytics CSO for pattern analysis and predictive failure analytics.</p>	Random Sample
112	5.5.4.14.4	<p>The Contractor shall issue a Service Incident Event report to the impacted JWCC users, the JWCC COR, and TO COR when CSOs functionality or cloud operations performance are impacted. The report shall contain, at minimum, a description of the nature of the Service Incident Event, an impact scope statement, the severity level, and the Mean Time to Resolve estimate.</p>	<p>The Government will assess whether:</p> <p>The impact scope statement contents and Service Incident Event severity levels are accurate and complete, such that they inform users and provide sufficient understanding of the event, time horizon to resolve the event and impact to the user.</p> <p>Compliance with Contractor's stated Service Level Objectives (SLO), as stipulated in the Contractor's SLAs, will be analyzed for deviation above the objective thresholds.</p>	As required	<p>The Service Incident Report is exhaustive and updated in real-time as activities transpire. Additionally reports are used as a basis for future chaos engineering tests to improve the cloud resiliency further reducing negative impacts to the DoD hosted capabilities.</p>	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
113	5.5.4.14.5	The Contractor's maintenance activities shall not impact JWCC operations.	The Government will assess whether Contractor maintenance activities have resulted in any observable negative impact to JWCC users.	As required	All maintenance activities are transparent to the users and have zero impact on user activities.	Random Sample
114	5.5.4.14.6	The Contractor shall provide the JWCC KO and JWCC COR with a detailed after-action report on all Service Incident Events within seven days of the Service Incident Event to allow the Government to understand the Service Incident Event's impact and determine appropriate follow-on actions.	The Government will assess whether the Service Incident Event after-action reports are complete and accurate. The Government will also assess whether event report delivery was compliant with the seven-day requirement.	As required	Updates for a Service Incident Event are provided automatically to every impacted user in real-time including after-action reports and analysis.	Random Sample
115	5.5.4.14.7	The Contractor shall securely provide to the Government, human and machine readable cloud service status and Service Incident Event information for all offerings it provides under the JWCC Contract JWCC Offerings.	The Government will assess whether the Contractor securely provides accessible and complete human and machine readable cloud service status and Service Incident Event information for DoD consumption.	As required	All service and Service Incident Event statuses are available in real-time on a centrally managed presentation display or via API query with multiple user selectable display modes.	Random Sample
116	5.5.4.14.8	For disconnected TE Devices, the Contractor shall ensure notification of TE Device specific service outages are provided to any local users at the time of the outage incident and queued for synchronization to cloud services upon re-connection, allowing for centralized reporting and resolution tracking.	The Government will assess whether the notification to local users of a TE Device for any service outage is delivered and if centralized reporting and resolution tracking match when the device	As required	All TE Device and offering notifications are available to all TE enclave users, and automatically captured and stored to a central repository on reconnection. Additionally for situations which	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			completes synchronization.		knock a TE Device off of the core cloud services (i.e. unplanned disconnected operations) the service provides via multiple modes notifications to a set of identified administrators	
117	5.5.4.15	The Contractor shall make available to the Government, standard and easy-to-interpret logs that are both human and machine readable. The Contractor shall ensure logs comply with C3PO and any other Regulatory or Statutory reporting compliance mandates. Such logs shall be generated and available using, at a minimum, either XML or JSON formats, and shall use a structured and verifiable schema. The Contractor shall make available any necessary tools required for log file and schema verification.	The Government will assess whether logs are readable by both human and machine, meet the specified delivery formats, and contain a structured and verifiable schema. Additionally the Government will perform verification of a random sampling of files with the schema using the Contractor provided verification tools.	As required	All logs are created so that humans and machines are equally able to consume the same logs and a Contractor Portal (UI) is available which allows for integrated analytics using customizable queries and visualizations.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
118	5.5.4.15.1	<p>To support DoD’s Defensive Cyber Operations, the Contractor shall provide access to all logs, related to JWCC, that are required for the Contractor’s DoD authorizations which provide an audit trail of all activities and actions (e.g., “Scenarios,” as defined in C3PO) as required under the CC SRG and DoD CIO Memorandum, Department of Defense Cybersecurity Activities Performed for CSO. To provide assurance of the actions of personnel assigned to or supporting an approved Oversight team, as defined in C3PO, for UNCLASSIFIED ILs, the Contractor shall explicitly identify (e.g. tag or separate) logs for all actions, whether direct or indirect, by Contractor personnel working under or as part of an approved oversight team, as defined in C3PO. There shall be no data use charges or transiting charges for accessing the logs stored in the consolidated log location(s).</p>	<p>The Government will assess whether the logs provide an audit trail of all activities and actions IAW C3PO.</p>	<p>As required</p>	<p>The logs will contain all actions executed within the cloud and automatically identify and tag anomalous behavior and behavior which goes against security best practices leading to automated notifications for review of suspicious activity.</p>	<p>Random Sample</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
119	5.5.4.15.2	The Contractor shall provide access to the logs stored in the consolidated log location(s) through a User Interface (UI) and a secure API at each classification level and IL. The Contractor shall participate in collaborative analysis with the DoD, as appropriate. UI and API documentation regarding the logs and associated features shall be accessible from the Contractor's Portal (UI), at each classification level and IL, and include sample code.	The Government will assess whether the Contractor has provided a Contractor Portal (UI) at each classification level and IL for access to consolidated logs and their locations. The Government will assess whether the Contractor has provided API documentation from the Contractor's Portal (UI), at each classification level and IL, and included sample code.	As required	A single Contractor Portal (UI) and API is enabled and the classification boundaries are managed as separable content mechanisms for the respective domains. All logs are also tagged with the origin security domain and associated metadata with the ability to be queried from higher domains for further analytics while maintaining relevant metadata.	Procedural Inspection.
120	5.5.4.16	Financial Analytical Reporting. The Contractor shall provide a comprehensive financial analytical reporting capability at each classification level and IL, capable of providing current and historical data for all one-time and continuing operational costs. Available information shall include all discrete items (smallest JWCC Offering purchasable from the JWCC Catalog) with the ability to aggregate items, using selected filters, across the entire JWCC user period of interest. The reporting capability shall provide users a financial representation of how costs were accrued over the period of interest. Additionally, the reporting capability shall support a projection mode where, based on current	The Government will verify that the provided financial analytical reporting capability produces accurate reporting based on a known configuration at each classification level and IL.	As required	Financial reporting will include the ability to aggregate across all classification levels and ILs, and is only delivered to the appropriate classification levels and ILs.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		behavior bound by a time period, an estimated cost projection can be computed for a future specified period of time.				
121	5.5.4.16.1	The Contractor-provided financial analytical reporting capability shall include the ability to support JWCC user defined queries and interfaces of the financial data and support the following capabilities:	Summary Requirement	N/A	N/A	N/A
122	5.5.4.16.1.1	Direct requester UI that allows for JWCC users to directly input a query and receive commensurate results/outputs.	The Government will assess whether the financial analytical reporting capability provides a Contractor's Portal (UI) to perform queries and present generated results.	As required	The Contractor's Portal (UI) will include tooltips, recommended built in queries, auto complete suggestions and integrated query help to aid users with less experience in the given query language.	Random Sample
123	5.5.4.16.1.2	Scripting capability that allows for repeatable periodic submission, based on a requester-managed file, where the results are delivered to a specified storage location.	The Government will assess whether the scripting capability allows for periodic submissions to a specified storage location.	As required	A fully automated scripting engine that can create and periodically execute scripts and which suggests common queries	Periodic Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
					and destinations based on the individual user, their role, and organization.	
124	5.5.4.16.1.3	An API for automated system-to-system interchange to enable query-response to execute in a dynamic and on-demand, non-human interacted method.	The Government will assess whether the API allows automated system processing with no human intervention, and whether the API is elastic and able to support multiple rapid connections from disparate sources.	As required	The API is able to support parallel processing of simultaneous connections	Procedural Inspection
125	5.5.4.16.1.4	An ability to construct a dashboard from multiple queries at each classification level and IL, such that a JWCC user can view a complete financial picture constructed from multiple queries.	The Government will assess the dashboard presentation and query result accuracy based on a known configuration.	As required	The dashboard is able to autosense classification domains and dynamically redact restricted information.	Procedural Inspection
126	5.5.4.16.1.5	The ability to save and share queries and load query results to dashboards. Once a query is saved to the dashboard, there shall also be an option for an authorized user to read, modify, and delete the query. This ability shall enable users to access, share, and execute a saved query without entering any of the query content and produce routine reports for an overall picture of financial data.	The Government will test the ability to read, modify, delete and save a query, on execution accurately producing the expected results based on a known configuration.	As required	A knowledge based stored query selector based on keyword(s) submission from a user (or API) and the ability to suggest queries based on the individual user, their role, and organization.	Procedural Inspection
127	5.5.4.16.1.6	The ability to display a history of all query activity.	The Government will assess the accuracy of the query history report based on multiple known queries that were executed previously.	As required	The ability to organize query history based on keyword or token submission and then store historical queries as named queries	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
					for future retrieval is provided.	
128	5.5.4.16.1.7	The ability to support reporting to multiple presentation modes (e.g. files, screen displays, etc.) allowing users to indicate one or more output methods for a generated report. At a minimum, this shall include a user accessible dashboard and the file types PDF and CSV. PDF and CSV file types shall be natively available as a presentation mode regardless of the JWCC user's technology (e.g. modern web browser).	The Government will test the query capability to produce the presentation information in multiple modes of output, IAW the minimum output standards described above, and any other output methods available.	As required	The ability to simultaneously report to all modes, selected by the user, of presentation.	Procedural Inspection
129	5.5.4.16.1.8	The query capability shall support discrete reporting down to the smallest unit purchases and aggregate all included costs to present the overall financial picture to the user. This provides users the ability to understand costs down to the smallest units possible.	The Government will assess whether the query tool is capable of showing costs down to the smallest units purchased and aggregate all included costs to present the overall financial picture to the user.	As required	The query capability is able to consume programmed aggregation feeds and reporting structures.	Procedural Inspection and Random Sample
130	5.5.4.16.1.9	The query capability shall support continuous cost accrual reporting to give the ability to report total spend for a given period of time, enabling users to project future budget needs.	The Government will assess whether the query tool includes the ability to see accrued costs for a given period of time.	As required	The ability to create dynamic time-phased reports.	Procedural Inspection and Random Sample
131	5.5.4.16.1.10	The query capability shall support aggregation of collected items that are grouped using tags. This shall allow users to group information based on specific groupings of	The Government will test the query tools ability to group information in a report based on tags.	As required	The tagging engine can deconflict and manage colliding or overlapping tags without double counting	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		information using user-supplied tags.			selected data sets.	
132	5.5.4.16.2	The Contractor shall provide a spend threshold capability to support warning thresholds at each classification level and IL. The spend threshold capability shall support establishment of threshold values by either the Contractor or the Government. The spend threshold capability shall provide a notification alert sent to a specified recipient list, such that Government users are “warned” of approaching spend threshold based on specific user needs.	Summary Requirement	N/A	N/A	N/A
133	5.5.4.16.2.1	The spend threshold capability shall allow each user to set specific threshold trigger values for which the spend threshold capability will execute a specified action, such that each user has the flexibility to specify multiple warning notifications based on unique independent threshold trigger values.	The Government will test, at least annually, whether the capability allows users to set parameters for threshold triggers to execute specific action(s) when that threshold is met.	As required	The ability to identify and arbitrate conflicted trigger events and suggest/select the most appropriate action outcome.	Periodic Sample
134	5.5.4.16.2.2	The spend threshold capability shall include an optional suspension mode, such that the Government avoids Anti-Deficiency Act violations by incurring obligations that are not authorized. If the threshold is achieved, the system will suspend, using a defined process, any additional purchases in a managed manner - both one-time and continuing operational consumption. However, in no case shall the Contractor delete any stored	The Government will assess whether the Contractor has provided the spend threshold capability suspension mode to suspend further spend, at a specified threshold without any compromise on retention of data, at each classification level and IL for	As required	The capability to optionally pre-determine a spend threshold breach exists and an automated “notification” is issued when the computed threshold is encountered and a suspend action is executed.	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		information, including both volatile and non-volatile memory.	one-time and continuing operational consumption. The Government will also assess that this spend threshold capability suspension mode is optional by enabling and then disabling the suspension mode and exceeding the prior set threshold.			
135	5.5.4.16.2.3	The spend threshold capability shall support reinstatement of a suspended CSO such that the CSO can be restored, from the point of suspension, as previously configured.	The Government will assess whether the Contractor has provided the spend threshold capability to restore services, data, and spend authorization, either one-time or continuing operational consumption, once funds verification is provided, without any compromise on retention of data by setting an artificial threshold on a sample workload, invoking the suspension mode and then adjusting the threshold or disabling the mode.	As required	The spend threshold capability is able to auto-sense funds sufficiency and restore operations. This includes a minimum rationale margin tolerance to prevent micro-restart suspend spin lock.	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
136	5.5.4.16.3	The Contractor shall provide the capability to support time-based billing information at each classification level and IL, such that a user can calculate total charges for a specified period of time in support of auditing and budgeting activities.	The Government will assess whether the Contractor has provided the capability to allow the user to set time-based parameters and obtain billing information based on pre-set (day, week, month, etc.), as well as custom time-frames.	As required	The capability will allow for multi-domain computations and auto-redacting information in unauthorized domains, summarizing data according to administrator configurable reporting policies, or any combination thereof.	Procedural Inspection
137	5.5.4.16.4	The Contractor shall provide the capability for JWCC users to plan and estimate one-time and continuing operational costs based on a specified notional resource configuration inputs for a projected operational scenario such that a JWCC user can estimate the projected total cost for a given PoP.	The Government will assess whether the Contractor has provided the capability to support projection of spend based on current configurations, anticipated configurations (user specified), current spend rates applied to both current and anticipated configurations, as well as adjustments to services.	As required	The capability will extrapolate projections based on prior and user estimated behavior patterns (e.g. estimated load, actual load, estimated load based on actual load).	Procedural Inspection
138	5.5.4.16.5	The Contractor shall provide the capability to report balances for remaining funds on accounts, such that users have the ability to track burn rate. This capability shall also project a balance exhaustion date based on consumption activity.	The Government will assess whether the Contractor has provided the capability to present balances of remaining funds on Contractor accounts, including expected timeframe for depletion of	As required	The capability will provide analytics to estimate the rate of consumption plots and trends including variable time resolution down to the minute.	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			current funds in the account(s).			
139	5.5.4.16.6	<p>The Contractor shall provide the capability, at each classification level and IL, to support financial reporting based on logical grouping of charges. Groupings shall include, but are not limited to:</p> <p>a. Reporting based on user/account, organizational structure (i.e. Enterprise, Department, Office, Team), or a combination thereof to determine cloud spend by user/account, organizational structure, or a combination thereof.</p> <p>b. Reporting based on type of services consumed to determine spending based on type of services consumed (e.g. storage, compute, data transfer, security).</p> <p>c. Reporting based on cost to determine services' impacts to spend rate.</p>	The Government will assess whether the Contractor has provided the capability report based on account, organizational structure, type of services consumed, and spend rate.	As required	The capability will provide auto-grouping options that are based on past reports and account based user behavior(s).	Procedural Inspection
140	5.5.4.17	The Contractor shall provide processes and rule-sets that enable the Government, in its utilization of services under the JWCC Contract, to comply with the Freedom of Information Act (FOIA), the Federal Records Act, the DoD Records Management Program, Disposal of Records, Executive Order (EO) 12333, EO 13587, the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), and National Archives Records	The Government will exercise the provided manual and automated processes to ensure the data is managed as prescribed IAW the conditions and mandates of the specific guidance. In the event compound guidance is required, the assessment will apply the	As required	The capability will accommodate all Federal reporting mandates.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		Administration (NARA) regulations.	identified configurations sequentially to assure the outcome is acceptable.			
141	5.5.4.18	The Contractor shall be capable of exporting security control assessment information using the NIST Open Security Controls Assessment Language (OSCAL) for JWCC Catalog Offerings to enable rapid authorization and accreditation of cloud services.	The Contractor will demonstrate the ability to export OSCAL data for their services and a sample workspace within the JWCC at least annually. The Government will assess whether exports are evaluated quarterly through independent testing for sustained compliance and 60 days post-major OSCAL version release.	As required	The capability will implement all OSCAL features including those listed as optional.	Procedural Inspection
142	5.5.5	Ease of Use: The Contractor must provide Self-Service capabilities enabling rapid development and deployment of new applications and advanced capabilities, including services from the JWCC Marketplace, as defined above. Additionally, the Contractor must support the portability of JWCC data and applications both out of and into the cloud. The Contractor shall provide a Portability Plan (CDRL A006) as detailed in sub-section 5.5.5.3.	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
143	5.5.5.1	<p>The Contractor shall provide the Government the ability to rapidly and securely provision/deploy First-Party offeringCSOs and Third-Party offeringCSOs via the Contractor-provided JWCC Marketplace, as defined below, with baseline template configurations, onto JWCC infrastructure at all classification levels and ILs. Third-Party offeringCSOs that are incapable of being deployed, used, or authorized on the Contractor's JWCC infrastructure are outside the scope of this contract.</p>	<p>The Government will assess their ability to provision/deploy offerings via the Contractor-provided JWCC Marketplace with baseline template configurations onto JWCC infrastructure at all classification levels and ILs.</p>	As required	N/A	Procedural Inspection and Random Sample
144	5.5.5.1.1	<p>The Contractor-provided JWCC Marketplace shall support the ability for JWCC users to deploy the first-party offeringCSOs and third-party offeringCSOs listed on the JWCC Catalog. All JWCC Commercial Marketplace Offerings shall undergo accreditation and authorization processes appropriate for their control markings (e.g. classification level and IL, including SAP, SCI, and others as designated) before the Contractor adds them to the JWCC Catalog and makes them available for JWCC users to fulfill orders, provision, or deploy. Commercial Offerings that are not subject to the CC SRG, or other DoD, and/or IC standards must comply with a Government-approved Contractor security processes and standards (CDRL A016) before the Contractor adds them to the JWCC Catalog and makes them available on the JWCC Marketplace. The Contractor shall make all security information and process outputs available for</p>	<p>The Government will audit the information and the processes execution to ensure that all necessary security processes and standards are appropriately managed and applied to all JWCC Marketplace offerings.</p>	30 DAC and then Quarterly	<p>The approved process is created to enable all commercial JWCC Marketplace offerings to obtain a security disposition that allows the DoD AO to grant the necessary security authorization for use with easy to interpret information and online approval based on non-repudiation user input or pre-configured rules.</p>	Procedural Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		Government audit and review.				
145	5.5.5.1.2	The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support centralized/integrated billing. The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support bring your own license (BYOL), where applicable (e.g., where additional licensing is required).	The Government will assess whether all first-party offerings in the JWCC Marketplace support centralized billing, BYOL, or any combination thereof, at each classification level and IL.	As required	The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
146	5.5.5.1.3	<p>The Contractor shall not apply additional cost to any Third-Party Marketplace Offering. This makes all Third-Party offering CSOs price-free from the Contractor, and all pricing shall be derived from the third-party that is providing the Offering in the third-party marketplace. If there is any exception Exceptions to a third-party marketplace offering being price-free, each offering shall this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO. All Third-Party offering CSOs that are available in the JWCC Marketplace shall be offered price-free and BYOL basis as appropriate, excluding the cost of IaaS resources. These JWCC Offerings shall be made available, at all classification levels and ILs, IAW PWS section 5.5.1 and 5.5.6 and their subsections, except as approved by the JWCC KO.</p>	<p>The Government will assess whether all third-party JWCC Marketplace offerings do not have additional cost and are available price-free or BYOL at each classification level and IL.</p>	As required	N/A	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
147	5.5.5.1.3.1	<p>For Third-Party offering CSOs available on a price-free or on a BYOL basis, the Contractor shall not impose additional license terms or conditions on the Government. The Government shall be solely responsible for negotiating the Terms and Conditions of the licenses for any Third-Party offering CSOs available on a price-free or on a BYOL basis that the Government has not previously negotiated Terms and Conditions under a separate contracting vehicle.</p>	<p>The Government will assess whether any BYOL or price-free third-party offering has additional Terms and Conditions beyond the Government provided license.</p>	As required	<p>The Contractor will ultimately take direct responsibility for all offerings, First and Third Party, and provide these offerings in a consistent and compliant manner with the JWCC Terms and Conditions offered by the First Party Contractor. The outcome is that all offerings for the JWCC Contract are now aligned with the JWCC Contract Terms and Conditions, and the First Party Contractor is responsible for ensuring the Government is able to receive all offerings with this contractual provision and no other Term or Condition applies.</p>	Random Sample
148	5.5.5.1.4	<p>The Contractor shall ensure all Third-Party offering CSOs that are available in the JWCC Marketplace support centralized/integrated billing with the Contractor.</p>	<p>The Government will assess whether third-party offering cost accrual is integrated into the workspace billing and does not include licensing costs/fees.</p>	As required	<p>The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.</p>	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
149	5.5.5.1.5	JWCC users' ability to order any discrete JWCC Offering shall be capable of being enabled or disabled at the IDIQ, TO, Cloud Environment, workspace, and JWCC user levels.	The Government will assess whether the ability for a JWCC user to order a sample third-party offering can be disabled at each level.	As required	The ability to establish pool groups for enable/disable single action outcomes across multiple workspaces/organizations/accounts.	Procedural Inspection and Random Sample
150	5.5.5.1.6	The Contractor's JWCC Marketplace shall be available at all classification levels and ILs IAW PWS section 5.5.1 and subsections, and new and modified approved offerings shall be populated within 24 hours of completion of JWCC Catalog Modification process (Section G11) JWCC KO approval. Access to the TS Marketplace shall be restricted to prevent fulfilling orders, provisioning, deploying, cloud operations, schedule non-provisionable or deployable offerings (e.g. Cloud Support Packages) until directed by the JWCC KO.	The Government will determine whether the JWCC Marketplace is available at the appropriate classification levels and ILs and within the stipulated time constraints.	As required	N/A	Procedural Inspection and Random Sample
151	5.5.5.2	The Contractor shall provide, at each classification level and IL, a Calculator reflecting contractually accurate price modeling and projection for any single JWCC Offering, or any combination of JWCC Offerings, at each classification level and IL, to enable authenticated DoD and JWCC users to properly estimate forecasted cloud spending for budgetary planning.	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
152	5.5.5.2.1	The Contractor's Calculator shall present all viable recommendations for available consumption-based pricing and subscription models (e.g. for reserved resources), including any applicable discounts.	The Government will assess whether the Contractor's Calculator is available for use by the DoD and performs cost calculations based on the pricing available to JWCC customers. The Government will also assess whether the output of the calculator presents all viable discounts available based on usage and subscription models (e.g., for reserved resources).	As required	The Calculator will produce a single report of all possible computations for equivalent options based on an initial user input configuration and identify the best priced option.	Procedural Inspection and Random Sample
153	5.5.5.2.2	The Contractor's Calculator shall provide the ability to compute and present projections to support users' long-term (in excess of 12 months) planning needs. The Contractor's Calculator shall provide users the ability to select time frames (e.g. month, quarter, year), as well as allow for custom time frames (e.g. Fiscal Year (FY) 2022 October 22 to FY 2024 January 15), to allow for accurate long-term budgeting.	The Government will assess whether the Contractor's Calculator provides users the ability to do long-term price projections based on user-selected time frames (e.g., month, quarter, year), as well as custom time frames (e.g., FY 2022 Oct 22 to FY 2024 Jan 15).	As required	The Contractor's Calculator is able to dynamically respond to live user entry parameters for time periodicity adjustment projections.	Procedural Inspection and Random Sample
154	5.5.5.2.3	Estimates developed using the Contractor's Calculator shall be made available in various formats, including, but not limited to, on screen, an image report (e.g. PDF document), and exportable/downloadable in a machine readable format that clearly breaks down the pricing by line item for further analytical processing,	The Government will assess whether the Contractor's Calculator provides users the ability to obtain results in the formats described.	As required	The Contractor's Calculator supports a full API for programmatic modeling and projecting scenarios (e.g. AI driven modeling).	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		including by other tools used for analysis and comparison purposes.				

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
155	5.5.5.2.4	<p>The Contractor’s Calculator shall be separately available at each classification level. The Contractor’s Calculator shall use and be consistent with the JWCC Contract pricing and the JWCC Catalog, based on the pricing and availability of all JWCC Offerings to allow for filtering and selecting any single JWCC Offering or any combination of JWCC Offerings at any classification level and IL for estimation. The Contractor’s Calculator shall default JWCC Offerings to the native classification level and IL where the Calculator is used. The Contractor’s Calculator shall be behaviorally and visually consistent at each classification level and IL, such that it provides a single “look and feel” at each classification level and IL (i.e., maintains Commercial Parity).</p>	<p>The Government will perform periodic testing to determine whether the Contractor’s Calculator has consistent and reproducible outcomes using Government predefined order configurations, at each classification level and IL, as well as, its general appearance is uniform across all classification levels and ILs.</p> <p>The Government will also periodically assess whether or not the offerings are defaulting to the native classification level and IL based on the Government user’s environment.</p>	As required	A single Calculator option for multi-classification pricing (i.e.: the Calculator is able to operate at the highest domain and pull data from all lower domains, without exposure of the data or the query).	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
156	5.5.5.3	<p>The JWCC Contract will require information (data, files, and other forms of information) to be transferred both out of the Contractor's Cloud Environment to another environment (cloud or otherwise) of the Government's choosing and into the Contractor's JWCC Cloud Environment from another environment (cloud or otherwise) of the Government's choosing. In accordance with CDRL A006, the Contractor shall provide the Portability Plan to the Government when it is specified in a TO The Portability Plan shall address the following information in the below subsections as specified in individual TOs.</p>	Summary Requirement	N/A	N/A	N/A
157	5.5.5.3.1	<p>The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all, or some, of a JWCC user's data from online, nearline, and offline storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a JWCC code repository, and network configurations. This shall allow the Government to move information (data and files) from the Contractor's JWCC Cloud Environment to another environment (cloud or otherwise) of the Government's choosing.</p>	<p>The Government will assess the Contractor's Portability Plan contents to determine whether the user instructions provide a complete set of processes and procedures that are necessary to extract all, or some, of the JWCC user's: online, nearline, and offline data, all configuration settings, environmental settings, logs and code repository content as well as any other substantive information required to equivalently replicate the</p>	As required	<p>A fully automated capability that targets all user data and prepares an optimized extraction plan for cost and speed and provides cost and time estimates to the user prior to execution. The capability allows the user to deselect items the automated plan identified and add items that are not identified. The plan can execute with a single user action.</p>	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			operational environment.			
158	5.5.5.3.2	<p>The Portability Plan shall include an explanation of how the Contractor will achieve complete purging of all, or some, information as specified by Government direction, which may indicate all, some, or specific user, environment or workspace assets. The Portability Plan shall also include a description for how the Contractor shall prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Contractor's JWCC infrastructure pursuant to the CC SRG and C3PO.</p>	<p>The Government will assess the Contractor's Portability Plan to ensure it includes an explanation of how the successful disposition, wiping and reconfiguration of all, or some, of a JWCC user's system components and data is accomplished, and describe how a JWCC user is able to prevent the re-instantiation of any removed or disposed system, capability, data, or information instances once removed from the Contractor's JWCC infrastructure.</p>	As required	<p>The capability will automatically attempt to access, reinstate, or any combination thereof, all removed items to validate successful disposition after confirming data transfer completion and identify any "success", which indicates eradication failure.</p>	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
159	5.5.5.3.3	<p>The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to import all, or some, of a JWCC user's data from a user specified location (e.g. online, nearline, and offline storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a code repository, network configurations, and on premises implementations) to the Contractor's JWCC cloud. This shall allow the Government to move information (data and files) from their existing environment (cloud or otherwise) to the Contractor's JWCC cloud.</p>	<p>The Government will assess the Contractor's Portability Plan contents to determine whether the user instructions provide a complete set of processes and procedures that are necessary to import all, or some, of a JWCC user's data from a user specified location: online, nearline, and offline data, all configuration settings, environmental settings, logs and code repository content as well as any other substantive information required to equivalently replicate the operational environment</p>	As required	N/A	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
160	5.5.6	<p>Commercial Parity. The Contractor shall establish commercial parity, as defined above, as soon as possible, but no later than 18 months after JWCC Contract award. In addition, the Contractor must submit any new or modified offerings added to the Contractor's commercial catalog after the JWCC Contract award to the DoD for authorization at all classification levels and ILs within 30 days of commercial availability. The new or modified offerings shall be provided at all classification levels and ILs. All new or modified offerings shall be consistent with Contractor's commercial catalog pricing.</p>	Summary Requirement	As required	N/A	N/A
161	5.5.6.1	<p>The Contractor shall ensure the provisioning of each JWCC Offering at each classification level and IL is equal to or faster than the average time computed daily for the provisioning of its equivalent Commercial Offering. The Contractor shall make available performance metrics for each Commercial Offering at each classification level and IL such that the Government can validate provisioning performance for each JWCC Offering (e.g. provisioning a new workspace, user, or service JWCC Offering, or deploying such JWCC Offerings within JWCC) as part of the Contract Monthly Progress Report (CDRL A001).</p>	<p>The Government will periodically assess whether commercial parity has been maintained for provisioning via testing at each classification level and IL.</p>	30 DAC and Monthly	<p>An automated analytics report is generated at a parametrically specified interval to measure provisioning activity against observed (system measures/metrics) and Contractor published performance characteristics. This reporting is also available in a dynamic mode to allow DoD operators to monitor real time operations and service status.</p>	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
162	5.5.6.2	<p>The Contractor shall provide generational replacement and upgrading of all software (inclusive of firmware) and hardware (compute, memory, storage, and networking), at all classification levels and ILs, such that the Contractor's JWCC Offerings are on par with the Contractor's equivalent Commercial Offerings. The Contractor shall provide a Lifecycle Management Plan (CDRL A018) which demonstrates how it will meet this requirement.</p>	<p>The Government will assess the sufficiency of the Lifecycle Management Plan (CDRL A018). The Government will perform a periodic review of hardware replacement and upgrade to verify and validate whether Contractor is adhering to the Lifecycle Management Plan (CDRL A018). The Government will perform periodic inspection of software versions and security patching to verify whether the Contractor is adhering to the Contractor Lifecycle Management Plan (CDRL A018).</p>	30 DAC and Monthly	An automated analytics report is generated at a parametrically specified interval to measure the migration and availability of hardware and network generational replacements and software upgrades as they are produced/occur.	Procedural Inspection and Random Sample
163	5.5.6.3	<p>The Contractor's offerings available under the JWCC Contract, across each classification level and IL, shall achieve commercial parity. Contractor shall achieve Commercial Parity, as soon as possible, but no later than 18 months after the JWCC Contract award. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.</p>	<p>The Government will assess whether the cloud offerings at contract award, less the exception(s) authorized by the JWCC KO and service(s) deprecated by the target date, match the services available for authorization at each IL and classification level 18 months post contract award.</p>	As required	An automated report is generated which compares all offerings in every domain. Parity is achieved in under 6 months and sustained for the duration of the contract.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
164	5.5.6.4	<p>Each Contractor Commercial Offering that becomes available for licensing, purchase, or consumption following the JWCC Contract award, shall be submitted to the Government for authorization, at all classification levels and ILs, according to the following procedures and timelines:</p> <p>For CSOs requiring FedRAMP approval:</p> <ul style="list-style-type: none"> • The Contractor must submit the CSO to the Joint Authorization Board (JAB) for authorization within 30 days of the CSO becoming Commercially Available. • The Contractor must submit the CSO to DISA for authorization within 30 days of FedRAMP approval. <p>For CSOs requiring IC approval:</p> <ul style="list-style-type: none"> • The Contractor must submit the CSO to the cognizant security authority for authorization within 30 days of the CSO becoming Commercially Available. <p>Each Commercial Offering shall be added to the JWCC Catalog IAW G11 at the classification level</p>	<p>The Government will assess whether the Contractor provides the Government a complete authorization package within 30 days of new cloud offering availability, or has an approved exception.</p>	<p>As required</p>	<p>An automated report is generated which identifies all offerings' event history, including authorization lifecycle details. Additionally services are made available the same day.</p>	<p>Random Sample</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		<p>and IL for which it is authorized. If an exception is required the Exception Request must be processed prior to adding it to or modifying it on JWCC Catalog. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.</p> <p>For any offerings that become available after the date of JWCC Contract award, the Contractor shall make such offerings available to the Government for authorization, at all classification levels and ILs, within 30 days of commercial availability. Exceptions to this requirement must be approved by the JWCC KO. Offerings that become commercially available before the availability of classified environments will be automatically provided an exception and remain subject to the JWCC timeline (5.5.1, above).</p>				
165	5.5.6.5	<p>For any of the offerings available under the JWCC Contract JWCC Offerings, across each classification level and IL, the same API calls and Contractor Portal (UI) actions shall result in the same expected behavior, except when restrictions due to classification level or IL prohibit Commercial Parity. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL</p>	<p>The Government may audit at any time during contract performance to determine whether API calls and Contractor Portal (UI) actions result in the expected behavior.</p>	As required	<p>All APIs are available identically across all domains requiring no more than an environment variable and account identification to change between domains.</p>	<p>Procedural Inspection and Random Sample</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		A024) and subsequently approved by the JWCC KO.				
166	5.5.6.6	The Contractor shall provide Commercial Parity of CSOs and specialized hardware availability between Data Centers at each classification level and IL such that workloads are able to scale and migrate horizontally within a classification level and IL. In addition, the Contractor shall ensure that JWCC users have the ability to configure JWCC workloads for “high availability” as defined in NIST SP 800-113. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.	The Government will assess whether data centers are capable of scaling and migrating JWCC workloads horizontally, to the degree to which service parity exists, at each classification level and IL and validate users can configure the services for high availability.	As required	An automated report is generated at a parametrically established interval identifying the maximal scaling and horizontal workload support. Additionally the Contractor makes available features which enable users to test failover between data centers in an easy and repeatable manner to support testing their developed capabilities and contingency operations.	Procedural Inspection and Random Sample
167	5.5.6.7	All JWCC Offerings shall be at or below the Contractor’s Commercial Catalog pricing.	The Government will assess whether pricing provided by the Contractor is consistent with their commercial offerings.	As required	Pricing for offerings that is lower than what is typically commercially available.	Procedural Inspection and Random Sample
168	5.5.6.8	Commercial Offerings which violate the FAR, DFARs, or are otherwise prohibited from DoD consumption are not considered Commercial Offerings for the purposes of Commercial Parity, and, therefore, need not be identified in JWCC	The Government will confirm this is not included in any Exception Requests.	As required	N/A	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		Exception Request (CDRL A024).				
169	5.5.6.9	Third-Party Marketplace Offerings are not considered Commercial Offerings for the purposes of Commercial Parity and, therefore, need not be identified in JWCC Exception Request (CDRL A024).	The Government will confirm this is not included in any Exception Requests.	As required	N/A	Procedural Inspection and Random Sample
170	5.5.7	Modern and Elastic Computing, Storage, and Network Infrastructure. The Contractor must enable self-service automated provisioning of compute, storage, and network infrastructure that is constantly updated -- to include, but not limited to processing architectures, servers, storage options, and platform software -- at scale to meet consumption, rapid development, and deployment in support of mission needs.	Summary Requirement	N/A	N/A	N/A
171	5.5.7.1	The Contractor shall provide all CSOs, including those that are optimized for specific compute-based activities (e.g. evolving GPU and application specific integrated circuits (ASIC) processing architectures, quantum computing applications, and future evolving computational integrated circuit devices).	The Government will assess industry trends in modern scalar compute architectures to determine that the offerings are pacing with commercial parity in both physical hardware and software modernization.	As required	An automated report is generated at a parametrically established interval identifying the trends in industry for cloud capabilities and competitor (boutique, focused and general) comparisons.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
172	5.5.7.2	The Contractor shall provide for durable elastic growth for storage capabilities (e.g. Online, Nearline, and Offline Storage options; object, block, and file-based storage; as well as managed database and NoSQL (non-structured query language) services), at the speed of deployment that is commensurate with Commercial Offering deployment speeds. This shall apply to all classification levels and ILs. Any performance tiering options shall be explicitly identified in the Contractor's JWCC Catalog.	The Government will assess, via audit at the Government's discretion, whether the Contractor's storage and performance behavior characteristics at each classification level and IL, regardless of elastic growth, are commensurate with those of the Contractor's commercial offerings.	As required	An automated report is generated at a parametrically established interval identifying the trends in industry for cloud capabilities and competitor (boutique, focused and general) comparisons.	Random Sample
173	5.5.7.3	The Contractor shall have more than one queryable storage JWCC Offering that can support data on the order of hundreds of Terabytes, intra-Availability Zones, and inter-Availability Zones. The Contractor shall provide at least one storage JWCC Offering that can perform create, read, update, and delete functions on data on the order of hundreds of Terabytes. Create, read, update, and delete operations at all classification levels and ILs shall be commensurate with the Contractor's Commercially available Offerings.	The Government will assess, via audit at the Government's discretion, whether the Contractor's queryable storage and the performance behavior characteristics, at each classification level and IL, are commensurate with the Contractor's commercial offerings.	As required	An automated report is generated at a parametrically established interval identifying the maximal storage capacity, by storage type (on-line, near-line, off-line, other) for each security domain. Additionally, the ability to support operations on the Petabyte scale.	Periodic Sample
174	5.5.7.4	The Contractor shall provide an API Gateway service that allows JWCC users the ability to develop, deploy, secure, manage, and scale the Government's APIs as needed.	The Government will assess whether the Contractor's API Gateway service provided to the Government allows for the ability to develop, deploy, secure, manage, and scale JWCC user-created APIs.	As required	The ability to automatically recommend API parameters, configurations, and optimizations based on historical utilization, available connector information, and	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
					industry best practices.	
175	5.5.7.5	When an authorized user requests a cloud resource within the Contractor's Portal (UI), or via an API, the response time shall be commensurate with the Contractor's Commercially available Offerings.	The Government will assess, via audit at the Government's discretion, whether the response time of each classification level and IL to determine the extent to which the cloud service offerings response times meet commercial parity.	As required	Response times which are quicker than the average commercial response time.	Random Sample
176	5.5.7.6	The Contractor shall provide the ability to generate individual IaaS compute instances, for which the time required to go from stopped state (e.g. powered off) to receiving and processing user instructions (less any operating system boot time) for any individual IaaS compute instance shall be less than 10 seconds.	The Government will assess, via audit at the Government's discretion, whether the time until the IaaS compute instance is capable of processing user instructions at each classification level and IL is less than 10 seconds and commensurate with the Contractor's commercial offering.	As required	The ability to start an instance inclusive of additional software load times (i.e. operating system boot time) which is less than 10 seconds.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
177	5.5.8	Fortified Security: The Contractor must provide fortified security capabilities that enable enhanced cyber defenses for strong IAM and security from the application layer through the data layer. Fortified security capability requirements include continuous monitoring and auditing, automated threat identification, resilience and elasticity, encryption at rest and in transit, secure data transfer capabilities, and an operating environment that meets or exceeds DoD INFOSEC requirements. This security shall be tested regularly and include independent DoD testing, review, and audit.	Summary Requirement	N/A	N/A	N/A
178	5.5.8.1	The Contractor shall provide encryption and logical separation for any of the Contractor's CSOs available under the JWCC Contract, IAW C3PO and the following additional requirements:	Summary Requirement	N/A	N/A	N/A
179	5.5.8.1.1	The Contractor shall ensure that encryption appropriate to the applicable classification level or IL, for data at rest and in transit, is the default setting for all of the Contractor's CSOs available under the JWCC Contract such that the DoD can maintain confidentiality, as defined in the definitions, as the default configuration.	The Government will inspect any data at rest and in transit to ensure that the specified encryption requirements are IAW C3PO. Additionally the Government will assess service offerings to ensure that encryption is configured by default.	As required	All data has multi-layer protection applied, while not impacting the performance profile of the operation.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
180	5.5.8.1.2	<p>The Contractor shall provide multi-layer encryption for all of the Contractor's CSOs such that content, including any at-rest containers, shall remain encrypted until explicitly invoked via executable, and then once again be encrypted when operational processing is complete. The Contractor shall provide multi-layer encryption to maintain data confidentiality and support dual encryption such that it includes two or more independent layers of encryption. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO. The Contractor may request an exception to the above requirement from the JWCC KO and shall include mitigation measures as part of any such request. Prior to submitting such a request, the Contractor shall confer with the JWCC KO, but the decision to grant such a request shall be at the JWCC KO's sole discretion</p>	<p>The Government will assess, via audit at the Government's discretion, whether the Contractor's documentation of multi-layer encryption methodology uses encryption algorithms and procedures as specified in C3PO.</p>	As required	<p>All CSOs, including containers, have multi-layer protection applied which meets CSfC requirements and does not impact the performance profile of the operation.</p>	<p>Procedural Inspection and Random Sample</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
181	5.5.8.1.3	<p>The Contractor shall ensure that all of its CSOs available under the JWCC Contract, at all classification levels and ILs, provide the capability for DoD data to be encrypted at rest, with exclusive DoD control of encryption keys and key management, such that the DoD has the capability to cryptographically erase data, as defined in the definitions. The Contractor shall provide:</p> <ul style="list-style-type: none"> a. JWCC user-managed encryption keys; b. Encryption key management as a service offering available under the JWCC Contract; and c. Support for use of both Contractor-provided and Government-provided Hardware Security Modules (HSMs) (whether in-line, within the Contractor's Cloud Environment, or externally located) for cryptographic operations. 	<p>The Government will assess, via audit at the Government's discretion, whether the key management processes and tools provided by the Contractor are sufficient to ensure that any JWCC user is capable of administering and applying encryption keys independent of the Contractor. The Government will also assess JWCC user-managed encryption keys and cryptographic erasure by attempting to access data encrypted with a deleted key. The Government will assess whether the JWCC user has the capability to use HSMs.</p>	As required	Apply the most modern trusted levels of protection such that the fundamental Government requirement remains fully compliant and operable, with the additional protections applied in concert as a non-interfering or disruptive supplementation.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
182	5.5.8.2	<p>Cross-Domain Solution. The Contractor shall provide a CDS that provides secure and highly deterministic one-way data transfer capability between the Contractor's logical enclaves and environments within the Contractor's cloud service offering CSOs under the JWCC Contract, to external destinations, and across all classification levels, while limiting any threats. The Contractor shall minimally provide CDSs that supports low to high (from a lower impact/classification level to a higher impact/classification level) for both the Management Plane and production plan and high to low (from a higher impact/classification level to a lower impact/classification level) for the Production Plane, per sections 5.5.8.2.1 through 5.5.8.2.5 of this PWS.</p>	Summary Requirement	As required	N/A	N/A
183	5.5.8.2.1	<p>All CDSs provided must be compliant with C3PO and the latest version of Cross-Domain Solution (CDS) Design and Implementation Requirements: 2020 Raise the Bar (RTB) Baseline Release (or current version) and achieve authorization by the DoD ISMRC.</p>	<p>The Government will assess whether the Contractor's provided CDS(s) are compliant with C3PO, 2020 Raise the Bar (RTB) Baseline Release. Additionally, the Government will assess whether the Contractor provides the DoD ISMRC a complete authorization package.</p>	As required	N/A	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
184	5.5.8.2.2	The CDS shall allow specific Government-controlled JWCC role-based accounts to overrule automated security measures to securely transfer information that may be flagged as malicious. This shall allow the specific Government-controlled JWCC role-based accounts-holders to accept risk as appropriate for flagged data transfers.	The Government will assess, via audit at the Government's discretion, whether the CDS, as authorized, allows for role-based accounts to overrule automated security measures.	As required	All CDS offerings have a dynamic control panel with flow management to allow the Government to apply any exception actions in real-time.	Procedural Inspection and Random Sample
185	5.5.8.2.3	The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the management plane to ensure the Contractor can securely migrate security updates to higher classification domains in a timely, consistent, repeatable, and secure manner, and maintain Commercial Parity.	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from low to high between all security domains and classification levels on the management plane.	As required	The Contractor uses the CDS to ensure patching occurs at all levels within hours of release and to ensure service and feature parity through the use of their DevSecOps process.	Procedural Inspection and Random Sample
186	5.5.8.2.4	The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the production plane to support Government data transfer needs, including Development, Security, and Operations (DevSecOps).	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from low to high between all classification levels and ILs on the production plane prior to initial operations.	As required	The CDS offerings support all data traffic regardless of the plane the information natively operates within (e.g. management plane, production plane, or other plane).	Procedural Inspection and Random Sample
187	5.5.8.2.5	The Contractor shall provide a CDS that supports data transfer from high to low between all classification levels and ILs on the production plane to support Government data transfer needs.	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from high to low between all classification levels on the	As required	The CDS offerings support all data traffic regardless of the plane the information natively operates within (e.g. management plane, production	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			production plane prior to initial operations.		plane, or other plane).	
188	5.5.8.3	The Contractor shall provide a secure data transfer capability for deterministic (maintaining integrity and predictable), authenticated, and encrypted, data transfers between the Contractor's logical enclaves and environments within its own cloud infrastructure and Offerings, to external destinations, including multi-environment peering gateways, and across all ILs within a classification level, while limiting any threats.	The Government will assess, via audit at the Government's discretion, whether the JWCC user(s) has the ability to securely transfer data to various endpoints both internal and external to the Contractor.	As required	The capability will seamlessly interoperate with external destinations and dynamically determine the protection posture such that if acceptable it executes the requested process, otherwise it provides a detailed exit report to the requesting user for potential remediation of the failed conditions and terminates the request while also allowing for a manual administrator override.	Procedural Inspection and Random Sample
189	5.5.8.4	Authentication, Authorization, and IAM. With respect to authentication, authorization, and IAM the Contractor shall provide the following:	Summary Requirement	N/A	N/A	N/A
190	5.5.8.4.1	The Contractor shall provide customizable granularity for role-based, identity-based, attribute-based, access control (R-, I-, ABAC) policy configurations within a workspace, including workspace administration, provisioning of new cloud services, management of existing services, and the ability to assign permissions to Contractor pre-defined	The Government will assess, via audit at the Government's discretion, whether granular control access is available for I-, R-, ABAC (collectively referred to as PBAC) across all services, users,	As required	All cloud actions are fully controlled under an exhaustive PBAC model.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		and allow for the creation and assignment of JWCC user specified roles.	data and resources.			
191	5.5.8.4.2	The Contractor shall provide non-repudiation and user-identity confirmation providing the ability to securely verify user identity, including Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI), at all classification levels and ILs pursuant to requirements in C3PO, the CC SRG, and the authorization for each of the Contractor's CSOs under the JWCC Contract.	The Government will assess, via audit at the Government's discretion, whether all users have non-repudiable identities, as well as whether any user exists without identity credentials. The Government will also assess the ability to create users who utilize MFA and PKI at all classification levels and ILs pursuant to the requirements in C3PO and the CC SRG.	As required	The capability denies all actions attempted by a non-authoritatively identified non-repudiable role, and immediately establishes a notification of such an attempt to the appropriate reporting manager (Human, non-human actor).	Procedural Inspection and Random Sample
192	5.5.8.4.3	The Contractor shall provide the ability to generate and issue time-limited, role-based authentication tokens that will allow a JWCC user to assume a set of attributes, roles, or a combination thereof within a specific workspace, the Cloud Environment, or a combination thereof.	The Government will assess, via audit at the Government's discretion, the ability for a JWCC user to establish and use time-limited, role-based authentication tokens within a specific workspace.	As required	The capability will support temporally programmable PBAC (all dimensions, e.g. I-R-ABAC) credentials.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
193	5.5.8.4.4	The Contractor's CSOs shall support modern authentication protocols and methods (e.g. Security Assertion Markup Language (SAML), Open Authorization (OAuth), Fast Identity Online (FIDO2)) such that the Government can integrate/use Federated Identity solutions with the Contractor's CSOs under the JWCC Contract at each classification level and IL.	The Government will assess, via audit at the Government's discretion, whether the Contractor can associate a DoD provided identity to a user within the Contractor's cloud service using modern authentication protocols and methods.	As required	The capability will support all future emerging authentication protocols, while maintaining a fully backward compatible operations posture.	Procedural Inspection and Random Sample
194	5.5.8.5	Automated INFOSEC and Access Control. In conjunction with the requirements established in C3PO, the Contractor shall provide automated tools for INFOSEC and access control with the attributes described below:	Summary Requirement	N/A	N/A	N/A
195	5.5.8.5.1	The Contractor shall provide the capability for the Government to audit both the physical location and logical separation, as defined in C3PO, of any CSO and Government data, at each classification level and IL, to ensure compliance with C3PO.	The Government will assess, via audit at the Government's discretion, whether the Contractor has provided sufficient tools that provide the Government the ability to obtain accurate information regarding the physical location and the logical isolation of selected host services to ensure compliance with C3PO. Optionally the Government will audit the physical location.	As required	The capability will have a persistent mapping of all service physical locations and the specific logical isolation/partitioning that is applied. Additionally visualization tools which support the audit and are able to be dynamically scoped are available for the users/auditors to document and use as part of the audit process.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
196	5.5.8.5.2	The Contractor shall provide automated tools for breach identification, notification, and remediation, to support breach and incident response requirements described in C3PO.	The Government will audit whether the Contractor has provided automated identification, notification, and remediation tools to allow the JWCC user fulfill incident response requirements.	As required	A fully automated programmable breach detection and remediation capability to allow for routine response protocols that optionally utilizes AI/ML services to predict and respond to breaches.	Procedural Inspection and Random Sample
197	5.5.8.5.3	The Contractor shall provide Self-Service and automated tools for handling data spills of CLASSIFIED or other controlled information, at each classification level and IL, to support data spillage activities as described in DoDM 5200.01 and C3PO.	The Government will test the capability at its discretion to assess whether its performance supports data spillage remediation and incident reporting requirements.	As required	A capability to auto alert and notify a designated authority of a potential cloud-based data spillage and provide the ability to suspend the offending action, user, or any combination thereof.	Procedural Inspection and Random Sample
198	5.5.8.5.4	The Contractor shall provide self-service tools, at each classification level and IL, to allow JWCC users to access data and analysis generated by threat detection systems so that JWCC customers, DoD cybersecurity investigators and auditors, including contractor staff serving in those capacities, can review, assess, protect, and defend their deployed and provisioned CSOs.	The Government will assess whether the self-service tools can support the capability to review, assess, protect, and defend deployed/provisioned CSOs as described in C3PO at each classification level and IL.	As required	An automated capability to assess the threat surfaces and exposure points in the cloud environment and present a systematic analysis that can be either programmatically processed or inspected and reviewed by humans.	Procedural Inspection and Random Sample
199	5.5.8.5.5	The Contractor shall provide identification and notification of threats to JWCC users and system owners immediately upon discovery, to support	The Government will assess whether the Contractor provides identification and notification of	As required	An automated capability to present viable remediation techniques to any identified threat for user	Ransom Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		incident response tasks as described in C3PO.	threats immediately upon discovery.		action or configuration for automated remediation.	
200	5.5.9	Advanced Data Analytics. The Contractor shall provide advanced data analytics CSOs, as minimally outlined herein and below, that securely enable data-driven and improved decision making at the strategic level (across security domains) to the TE (within a single security domain). The Contractor shall provide advanced data analytics CSOs that support batch and streaming analytics, predictive analytics, and AI/ML. Advanced data analytics CSOs shall be available at all classification levels and ILs, extensible to the TE, to include DDIL environments and on multiple disparate datasets. Advanced data analytics CSOs shall, at a minimum, be able to import, process, and export streaming and batch data in common data formats.	Summary Requirement	N/A	N/A	N/A
201	5.5.9.1	The Contractor shall provide data analytics CSO's (e.g., streaming analytics, predictive analytics, and AI/ML).	Summary Requirement	N/A	N/A	N/A
202	5.5.9.1.1	The Contractor shall provide data analytics JWCC Offerings capable of operating at all classifications and ILs, and on TE Devices, such that operators can label data, train and develop models, and use model/algorithm outputs in mission relevant environments with mission relevant data, commensurate with the JWCC timeline	The Government will assess whether the Contractor has provided data analytics offering capable of operating at all classifications and ILs and TE Devices, less the exceptions approved by the	As required	A fully equipped AI/ML, and other analytic learning tools, suite of tools, platforms, or any combination thereof, to allow advanced processing of data for insight and findings. All tools are also	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		(5.5.1, above) less exceptions . Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.	KO, and commensurate with the JWCC schedule ref 5.5.1.		available at the tactical edge in connected and disconnected modes.	
203	5.5.9.1.2	The Contractor's advanced data analytics CSOs shall be capable of operating across multiple datasets in disparate workspaces to allow for information sharing and learning across multiple DoD Components/Agencies.	The Government will assess, via audit at the Government's discretion, whether the Contractor has provided advanced data analytics offerings capable of operating across data centers in disparate workspaces by linking multiple disparate data sources (from one or more workspaces) to a single workspace and executing a simple AI/ML pipeline.	As required	A capability to identify all compatible data sets and the specific aligned "data items" (e.g.: data engineering and normalization) across the JWCC data universe. Additionally capabilities which aid data wrangling and suggest likely mappings between disparate data sets for accelerated analysis.	Procedural Inspection and Random Sample
204	5.5.9.1.3	The Contractor shall provide advanced data analytics CSOs able to fully operate with or without network connectivity and in DDIL environments, such that TE Devices shall be capable of continued data analytics activities (including AI/ML) when network connectivity is contested, congested, or unavailable, commensurate with the JWCC timeline (5.5.1, above).	The Government will assess, commensurate with the device's availability under the JWCC schedule (ref. 5.5.1), whether TE Devices have data analytics capabilities (including AI/ML) in varying states of connectivity (e.g., contested, congested, or unavailable). The	As required	A complete cloud stack that can operate in a small footprint TE Device that is in a DDIL mode.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			Government may, at its sole discretion, assess continued capability at any time.			
205	5.5.9.1.4	The Contractor's data analytics JWCC Offerings shall be capable of supporting data import and export in common formats (at minimum these formats shall include CSV, JSON, XML, and streaming data).	The Government will assess, via audit at the Government's discretion, whether the Contractor has met this requirement by using sample data in multiple formats in the Contractor's data analytics offerings. The Contractor's tools will be assessed for data integrity inclusive of the consistency of output of the data structure and content.	As required	A mediated adapter capability that can autosense, or be programmatically patterned, to allow unknown (no prior exposure) data structures and formats to be consumed.	Random Sample
206	5.5.10	Tactical Edge. The Contractor shall provide TE Offerings and TE Devices across the range of military operations while balancing portability, capability, and cost. TE Devices shall operate seamlessly across network connectivity levels, including DDIL environments, at all classification levels and IAs IAW C3PO.	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
207	5.5.10.1	<p>The Contractor shall provide, as a JWCC Offering in the JWCC Catalog, a minimum of one form factor of TE Devices that is man-portable and is capable of being carried by an individual(s), mounted to a vehicle, or both, which the Contractor will have certified as meeting MIL-STD-810H (Environmental Engineering Considerations and Laboratory Tests), such that the form factor of TE Devices enables the use of JWCC resources across the range of military operations (e.g. deployable afloat, aloft, ashore, and globally). This form factor of TE Devices shall be authorized to host data at each classification level and IL.</p>	<p>The Government will assess whether a man-portable TE Device form factor is certified as meeting MIL-STD-810H, is capable of being carried and mounted to a vehicle and is authorized to host data at each (or up to all) classification levels and ILs. The Government will test the TE Devices at its discretion.</p>	As required	<p>A diverse range of MIL-STD-810H TE footprints such as: lightweight (tablet or smaller), highly portable (laptop), small portable (desktop or small luggable 1-person carry) server, moderate non-portable (2+ person movable) server, large human-machine assisted portable (mini, mainframe, vehicle mounted, or facility located), and huge machine (e.g. semi-truck or large container vehicle movable data center).</p>	100% Inspection
208	5.5.10.2	<p>The Contractor shall provide a modular, rapidly deployable data center that can be connected to Government-provided power, connected to Government-provided networking uplinks when available, use Government transportation, and be deployed on U.S. soil, CONUS or OCONUS, or on Government-owned platforms (e.g. aircraft carriers, maritime operations center, airfields, and division headquarters). The deployable data center shall be authorized to host data at each classification level and IL and up to all classification levels and ILs following the physical and logical</p>	<p>The Government will assess whether the modular, rapidly deployable data center is authorized to host data at each classification level and IL, or at all classification levels and ILs in relevant mission environments. The data center will be demonstrated to the Government for acceptance and the Government will test it at its discretion.</p>	As required	<p>A configurator tool is available to generate a known working configuration of a rapidly deployable data center, to include past configuration options and non-existing assemblies that are guaranteed to work.</p>	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		separation requirements in C3PO.				
209	5.5.10.3	The Contractor's TE Offerings shall function in DDIL environments as if connected, with the only features and functionality missing being those that rely on real time interconnection services. TE Offerings shall include the ability to configure and manage any CSO deployed or provisioned on or to the TE Device, and operate using local resources.	The Government will test the TE computing and storage functionality in simulated DDIL environments, at its discretion, to ensure the ability to configure and manage any provisioned CSOs and operate using local resources (e.g., local virtual machines and or containers should continue to operate).	As required	The TE Devices are capable of modular adapter components that can be hot swapped to dynamically change the available service sets for the configuration.	Random Sample
210	5.5.10.4	The Contractor's TE Offerings shall be configurable such that a JWCC user can configure the parameters for synchronization with Contractor-provided services. These parameters shall, at a minimum, include automated or manual, bidirectional or unidirectional synchronization options, the ability to control synchronization priority order, and the ability to throttle use of available	The Government will assess, via audit at the Government's discretion, whether the TE Devices meet the minimum parameters for synchronization to include automated or manual, bidirectional or unidirectional, synchronization options, the	As required	The TE Devices are equipped with programmatic sensing capability that can be threshold triggered to perform synchronization based on complex parametric and algorithmic situations. (e.g. all network traffic is idle and	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		bandwidth for synchronization.	ability to control synchronization priority order and throttle use of available synchronization bandwidth for synchronization.		operational exposure is not a consideration).	
211	5.5.10.5	The Contractor shall provide TE Device and component signature specifications for Electromagnetic (EM), acoustic, thermal, and any other device specific emanations in all operational states to enable the Government to control the magnitude of these signatures (TE Device Specifications, CDRL A017).	The Government will assess whether the Contractor provided TE Device signature data is sufficient and complete. The Government reserves the right to verify the signature specifications against device testing.	90 DAC and As required	The TE Devices will have componentry that can auto generate complete device signature data and can further can control, and/or augment, or any combination thereof, the signature to lowered states without significant impact to performance.	Random Sample
212	5.5.10.6	The Contractor's TE Offerings shall follow the cybersecurity requirements defined in C3PO.	The Government will assess, at its discretion, whether TE offerings and devices meet conformance requirements in C3PO.	As required	The TE Devices will exceed one or more of C3PO requirements.	Random Sample
213	5.5.10.7	The Contractor's TE Offerings shall be capable of both in-band and out-of-band configuration and maintenance for all TE Devices.	The Government will assess whether the TE solutions ability to perform both in-band maintenance and whether the materials are provided for the Government to	As required	All TE configuration and maintenance activities are fully available both in-band and out-of-band.	Procedural Inspection and Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			perform out-of-band configuration and maintenance capabilities without the Contractor's intervention.			
214	5.5.10.8	The Contractor's TE Offerings shall support cryptographic key management, IAW Section 5.5.8.1.3 and C3PO, both on and off the TE Device, at the user's discretion.	The Government will assess tactical edge solutions conformance to support of key management, IAW C3PO, both on and off the device at the discretion of the user will be tested.	As required	N/A	Procedural Inspection and Random Sample
215	5.5.10.9	The Contractor shall provide delivery of TE Devices to CONUS locations only and allow for the Government to pick up TE Device(s) at a Contractor facility in CONUS. Locations for pickup and any services and fees associated with delivery shall be separately identified and priced in the JWCC Catalog.	TE Devices delivered to CONUS locations, and IAW services and fees in the relevant catalog or available for pick up at the defined Contractor's facility.	As required	N/A	Random Sample
216	5.5.10.10	The Contractor shall submit authorization packages for the first unit of all variations of TE Devices for Authorization at each classification level and IL.	The Government will assess the current state of the TE Device authorization. Any TE Devices and services that have not been previously authorized must include all documentation required for the AO to authorize the device(s)/CSO(s) for use.	As required	All TE Devices are pre-qualified with a full authorization, including the first delivery item.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
217	5.5.10.11	For each TE Device the Contractor will offer in the JWCC Catalog, the Contractor shall provide to the JWCC PMO a sample of each TE Device per classification level and IL, with the associated authorization package, such that the Government can perform verification and validation of the device(s) prior to official acceptance as part of the JWCC Catalog. Upon completion of testing, the Government will either order the appropriate TE Offerings(s) from the JWCC Catalog or return all sample TE Devices from the test.	The Government will receive each TE Device submitted, conduct DoD authorization activities. Upon completion of testing, the Government will either order the appropriate TE offering(s) from the JWCC Catalog or return all sample TE Devices from the test.	As required	All TE Devices are pre-qualified with a full authorization, including the first delivery item. This may require pre-coordination with the Government prior to the first order.	100% Inspection
218	5.5.10.12	When TE Devices are returned to the Contractor, the Contractor shall either dispose of the TE Device IAW the CC SRG and the Attachment J-3: JWCC DD254 or follow the procedures and requirements in C3PO for reuse.	The Government will assess the Contractor's ability to dispose of or, wipe and reconfigure TE Devices and to audit management controls surrounding these practices.	As required	N/A	100% Inspection
219	5.5.11	Advisory and Assistance Services. The Contractor shall provide advisory and assistance services under the Cloud Support Package CLINs in the JWCC Contract to advise and assist with cloud architecture, usage, optimization, provisioning, and configuration for all JWCC Offerings, including TE Offerings. Cloud Support Packages shall encompass, but not be limited to, advisory and assistance services, help desk services, training, and documentation support. Cloud Support Packages shall be available for all JWCC Offerings at all classification levels and ILs.	Summary Requirement	N/A	N/A	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
220	5.5.11.1	The Contractor shall provide advisory and assistance services that include integration, aggregation, orchestration, secure design, and troubleshooting of JWCC Offerings and can be applied to all classification levels and ILs.	The Government will assess whether the offered advisory and assistance services ensure coverage of all the Contractor's offered cloud services under the JWCC Contract, inclusive of TE Devices. The Government will assess whether the available advisory and assistance packages can be applied to all security domains, and at each classification and IL and meet the security requirements of the DD254.	As required	All advisory and assistance support packages are equivalent for all security domains, and classification levels and ILs.	100% Inspection

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
221	5.5.11.2	<p>The Contractor shall provide training materials and make training available for all of the CSOs on the JWCC Catalog at all classification levels and ILs. Separate training and documentation are required for TE Offerings. The Contractor shall include, at a minimum:</p> <p>a. Training materials and training for all CSOs provided on the JWCC Catalog at all classification levels and ILs.</p> <p>b. Materials that help users and administrators understand how to successfully provision services and employ best practices for JWCC Offerings on the JWCC Catalog. Users and administrators shall be able to retain such materials upon completion of the training (CDRLs A004 and A005).</p> <p>c. Separate training and training materials shall be provided for each TE Offering, inclusive of supportability training (e.g. end user maintenance, packaging, handling, storage and transportation, infrastructure requirements), at all classification levels and ILs.</p> <p>d. Any training the Contractor provides shall demonstrate, through tabulated results, the relevance, thoroughness, and</p>	<p>The Government will assess whether the offered training and associated materials meet the following criteria:</p> <p>applicability and thoroughness for each service at all classification levels and ILs, including tactical edge.</p> <p>Provide tabulated results on relevance, thoroughness, and efficacy of training.</p>	30 DAC and Annually	All training materials are equivalent between security domains, and classification levels and ILs and are fully comprehensive in content.	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
		<p>efficacy of the training using industry standard methods and tools.</p> <p>e. All training materials shall be current and the Contractor shall provide updated training materials with the release of new versions of any CSO that is made available to JWCC users.</p>				
222	5.5.11.3	<p>If a Cloud Support Package is constrained by the number of hours available to users, the Contractor shall provide a Self-Service mechanism for users to quickly determine how many hours of the available support package have been consumed.</p>	<p>The Government will assess whether the Cloud Support Package services available under the Cloud Support Package line items on the contract for every service offering. The Government</p>	As required	<p>The advisory and assistance services include multi-vendor interoperability solutioning.</p>	Random Sample

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Surveillance	Performance Objective	Monitor Method
			will also assess whether the Contractor provides a self-service resource to determine remaining hours on time constrained services.			
223	5.5.11.4	The Contractor shall provide, as part of the JWCC Catalog, separate options for in-person and remote instructor-led training and support services provided by the Contractor in CONUS and OCONUS locations. All training and support services shall be offered at the locations as described in the JWCC Offering or as required by the TO.	The Government will assess whether the JWCC Catalog for in-person and remote instructor-led training and support services in CONUS are listed independently from those catalog items for training and support services in OCONUS locations.	As required	N/A	Random Sample
224	5.5.11.5	The Contractor shall provide, as part of the JWCC Catalog, an option for self-paced training.	The Government will assess whether the Contractor's catalog has an item for self-paced training.	As required	N/A	Random Sample
225	5.5.11.6	The Contractor shall provide options for equipment repair/replacement and data recovery from TE Device failure or performance degradation, with minimal mission impact, such as the ability to replace failed hardware at the unit level or full TE Device in a manner that is appropriate for the form factor of the device and range of impacted military operations and best effort data recovery.	The Government will evaluate whether the Contractor's offered services under the JWCC Contract include TE data recovery and equipment repair/replacement options.	As required	An immediate replacement/recovery model for TE Devices has no impact on mission operations.	Procedural Inspection and Random Sample

**DEPARTMENT OF DEFENSE
JOINT WARFIGHTING CLOUD CAPABILITY
PERFORMANCE WORK STATEMENT**

(A0012 Update)

Changes within the solicitation and affected attachments have been made using ~~strike through~~ text to reflect information that has been deleted and highlighted text to reflect information that has been changed, so that the new changes are clear. Punctuation and formatting changes that do not change the substantive meaning of the language may not be specially marked.

PART 1
GENERAL

1. **GENERAL:** This is a non-personal services contract to provide the Department of Defense (DoD) of the United States (U.S.) of America with the Joint Warfighting Cloud Capability (JWCC). The Government shall not exercise any supervision or control over the Contractor's personnel performing the services herein. Any individuals providing contract services shall be accountable solely to the Contractor who, in turn, is responsible to the Government.
- 1.1 Description of Services/Introduction: The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary as defined in this Performance Work Statement (PWS) except for those items specified as Government Furnished Property (GFP), Government infrastructure, and Government services. The Contractor shall perform to the standards specified in this contract.
- 1.2 Background: On September 13, 2017, the Deputy Secretary of Defense (DSD) issued a memorandum declaring the initiative to, "Accelerate Enterprise Cloud Adoption" throughout the Department. In it, the DSD stated that, "accelerating the DoD's adoption of Cloud Computing technologies is critical to maintaining our military's technological advantage." On December 22, 2017, the Vice Chairman of the Joint Chiefs of Staff signed and issued Joint Requirements Oversight Council (JROC) Memorandum 135-17, which described, "Joint Characteristics and Considerations for Accelerating to Cloud Architectures and Services." These characteristics and considerations, "guide the Department's efforts in accelerating the DoD's adoption of cloud."

Providing cloud capabilities and services within a single enterprise acquisition solution is "critical in creating a global, resilient, and secure information environment that enables warfighting and mission command, resulting in improved agility, greater lethality, and improved decision-making at all levels." To date, the DoD has acquired, "one-off" cloud capabilities resulting in disconnected and disparate enterprise Cloud Environments for the DoD. The JWCC Indefinite Delivery, Indefinite Quantity (IDIQ) acquisition environment will seek to connect the Defense Information Enterprise in totality, by providing access to globally available Offerings, across all security domains, at all classification levels, from the strategic level to the Tactical Edge (TE), to include Disconnected, Disrupted, Intermittent, and Limited (DDIL) environments, at scale.

This PWS describes the DoD's required Offerings under the JWCC IDIQ acquisition

environment contracts (hereafter the JWCC Contracts). This is inclusive of all “as a Service” Offerings, hereafter referenced as XaaS (i.e. Anything as a Service), that supports current and future DoD business and mission operations.

- 1.3 Scope: JWCC will provide the DoD access to Offerings to support current and future DoD business and mission operations. JWCC users will include all of the DoD as defined in 10 United States Code (U.S.C.) § 111. Other potential users of JWCC will be subject to compliance with all applicable law, statutes, regulations, and policies, and may include other foreign and domestic mission partners when related to the authority, direction, and control of current and future DoD business and mission operations.

JWCC shall provide Cloud Service Provider (CSP) controlled XaaS (e.g. compute, network, storage, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)) across all security domains, and at all classification levels and Impact Levels (ILs). JWCC Offerings shall be available across all classification levels and ILs, from the strategic level to the TE, to include in DDIL environments, as well as Closed-Loop Networks. JWCC Offerings shall meet industry-standard commercial Service Level Agreements (SLAs) and the requirements of this PWS, and the JWCC Contract, regardless of where JWCC Offerings are being delivered.

Unless otherwise annotated, the stated objectives, requirements, and metrics in the PWS apply to Offerings across all security domains, and at all classification levels and ILs. The Government understands that some Contractors may propose functionality beyond what is specified in the PWS as part of their JWCC Offerings, and the PWS should not be interpreted as limiting that functionality, but rather should be considered as a base or minimum. All Performance Metrics listed in the PWS shall apply to all Task Orders (TO), unless otherwise noted in the TO. Migration services are outside the scope of the JWCC Contract.

- 1.4 Period of Performance: The Periods of Performance (PoP) shall consist of one three-year base period, and two one-year option periods to be exercised at the Government’s sole discretion.

Base Period	November 28, 2022 through November 27, 2025
Option Period I	November 28, 2025 through November 27, 2026
Option Period II	November 28, 2026 through November 27, 2027

- 1.5 General Information

- 1.5.1 Quality Control: The Contractor shall develop and maintain an effective quality control program to ensure services are performed In Accordance With (IAW) this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of Defective Services. The Contractor’s Quality Control Plan (QCP) (Contract Data Requirements List (CDRL) A008) is the means by which the Contractor formalizes their quality control program to ensure their work aligns and complies with the requirements of the contract.
- 1.5.2 Quality Assurance: The Government shall evaluate the Contractor’s performance under this contract IAW the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused

on what the Government must do to ensure the Contractor has performed IAW the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.5.3 Recognized Holidays (Reference 5 U.S.C. § 6103):

- New Year's Day – January 1
- Martin Luther King Jr.'s Birthday – the third Monday in January
- President's Day – the third Monday in February
- Memorial Day – the last Monday in May
- Juneteenth National Independence Day – June 19
- Independence Day – July 4
- Labor Day – the first Monday in September
- Columbus Day – the second Monday in October
- Veterans Day – November 11
- Thanksgiving Day – the fourth Thursday in November
- Christmas Day – December 25

1.5.4 Hours of Operation: The Contractor shall, at all times, maintain an adequate workforce for the uninterrupted performance of all tasks and activities defined in the JWCC Contract, and subsequent TOs, such that the clouds and associated JWCC Offerings are available to the Government and are maintained 24 hours a day, 7 days per week, and 365 days a year. In the event an emergency or operational anomaly that impacts normal operations occurs outside of the normal duty hours for Government personnel (Monday through Friday, 8:00 a.m. to 4:30 p.m. Eastern Time), the Contractor shall contact the personnel identified by the Government, below, to notify them of the situation within the hour of emergency or operational anomaly occurrence:

<To be completed for award.>

1.5.5 Place of Performance: The work to be performed under this contract will be performed at the Contractor's facilities for all tasks unless otherwise authorized by the JWCC Contracting Officer (KO) or TO KO. The following are the performance locations approved under this contract:

<To be completed after award.>

1.5.6 Type of Contract: This is a multiple-award IDIQ contract that allows for Firm-Fixed-Price (FFP), Time and Materials (T&M), and hybrid (a mix of FFP and T&M) TOs; travel will only be on a T&M basis.

- 1.5.7 Security Requirements: The Contractor shall perform all tasks and submit all security deliverables (CDRLs A003 and A009) necessary to provide UNCLASSIFIED and CLASSIFIED Infrastructure and Offerings IAW all required Federal and DoD Cybersecurity and Privacy requirements, in time to meet the timeframes under this contract. The Contractor shall be responsible for safeguarding all Government information and GFP provided under this contract. Subsections 1.5.7.1 to 1.5.7.7 supplement Block 13 of the Attachment J-3: JWCC DD254, Contract Security Classification Specification.
- 1.5.7.1 Facility Security Clearance. Work will be performed under this contract and any resultant TOs at up to the TOP SECRET (TS) level and will require Sensitive Compartmented Information (SCI) access eligibility and/or Special Accesses. Therefore, the Contractor must have an interim or final TS Facility Clearance (FCL) from the Defense Counterintelligence and Security Agency (DCSA) FCL Branch, or appropriate accrediting Federal agency, at time of contract award.
- 1.5.7.2 Security Clearance. Personnel performing on this contract, or supporting work under this Contract, shall be U.S. citizens, or as prescribed in the Cloud Computing Cybersecurity Plan for Operations (C3PO) (Attachment J-2). Contractor personnel must possess the interim or final security clearance eligibility necessary to perform the Tasks/Subtasks as delineated in the table below and further identified in the PWS.

Tasks/Subtasks	Clearance Level	Level of CLASSIFIED Access	Justification for Access to CLASSIFIED
JWCC Contract Management	TS/SCI	Personnel supporting the Tasks/Subtasks may require access to: Communications Security (COMSEC), Secret Internet Protocol Router Network (SIPRNet), North Atlantic Treaty Organization (NATO), Joint Worldwide Intelligence Communication System (JWICS), Special Access Program(s) (SAP), etc.	Access is required in support of the oversight and management of the JWCC Contract. Support is required in support of TOs under this contract.

Provide SECRET Cloud Services and Support	SECRET	Personnel supporting the Tasks/Subtasks may require access to: COMSEC, SIPRNet, NATO, SAPs, etc.	Access is required in order to provide and support SECRET JWCC Offerings.
Provide TOP SECRET Cloud Services and Support	TS/SCI	Personnel supporting the Tasks/Subtasks may require access to: COMSEC, SIPRNet, NATO, JWICS, SAPs, etc.	Access is required in order to provide and support of TOP SECRET JWCC Offerings. Access to SCI caveats and information, and SAPs may be required based on the issued TOs.
Tactical Offerings and Edge Support	Up to TS/SCI	Access will be defined based on the TE Device classification	Access is required in order to provide and support CLASSIFIED JWCC Offerings.
Advisory and Assistance Services	Up to TS/SCI	Personnel supporting the Tasks/Subtasks may require access to: COMSEC, SIPRNet, NATO, JWICS, SAPs, etc.	Access is required to advise and assist with cloud architecture design, as well as resource usage, provisioning, and configuration of XaaS.

Cloud Training	Up to TS/SCI	Access will be defined based on the Cloud Training requirements	Access is required in support of cloud training requirements across the contract.
----------------	--------------	---	---

1.5.7.2.1 Individuals supporting PWS Tasks/Subtasks that require(s) a final TS security clearance will, immediately upon hire, require SCI access eligibility adjudicated by the DoD Consolidated Adjudication Facility or another Federal adjudications facility, to perform their duties. Processing for SCI eligibility will be coordinated with the supporting Government Special Security Office (SSO) and/or Security Managers, and will begin immediately upon start of duty performance under any TO issued under this contract.

All SCI work under the JWCC Contract and resultant TOs will be monitored by the relevant Contracting Officer's Representative (COR)/Alternate Contracting Officer's Representative (ACOR). Any COR/ACOR, including those designated in individual TOs, must be indoctrinated into SCI to monitor the SCI work.

1.5.7.3 Investigation Requirements. All personnel requiring TS/SCI access under the JWCC Contract and resultant TOs shall undergo a favorably adjudicated Tier 5 (T5) Investigation (formerly known as a Single Scope Background Investigation) as a minimum requirement. The T5 Investigation will be maintained as current within six years and requests for Tier 5 reinvestigation (T5R; formerly known as Single Scope Background Periodic Reinvestigation) or Phased Periodic Reinvestigation will be initiated prior to the six-year anniversary date of the previous T5R.

1.5.7.3.1 All personnel requiring SECRET access under the JWCC Contract and resultant TOs shall undergo a favorably adjudicated Tier 3 (T3) Investigation (formerly known as a National Agency Check, Local Agency Check, and Credit Check or Access National Agency Check and Inquiries) as a minimum investigation. The T3 Investigation will be maintained within 10 years and requests for SECRET Periodic Reinvestigations will be initiated by submitting a Tier 3 Reinvestigation (T3R) prior to the 10-year anniversary date of the previous T3 Investigation.

1.5.7.3.2 The Contractor is required to have personnel cleared with an interim or final SECRET or TOP SECRET clearance at contract start date. If Contractor personnel are replaced during performance of the contract, replacement personnel should also have interim or final clearance of SECRET or TOP SECRET.

1.5.7.4 Visit Authorization (Visit Authorization Letters (VALs) and Visit Authorization Requests (VARs)). VARs shall be processed and verified through the Defense Information System for Security (DISS) and submitted to Security Management Office (SMO) codes: DKABAA10, DKACCPO, and/or the appropriate SMO. VARs processed through DISS for visits for the JWCC

Contract and resultant TOs are identified as, “Other,” “Temporary Additional Duty,” or “Temporary Duty Travel,” and will include the Contract/Order Number of the contract/order in the, “Additional Information” section. Contractors that do not have access to DISS may submit a VAL by e-mail in a password protected or otherwise encrypted Portable Document Format (PDF) to the COR/ACOR and appropriate SMO designated for the JWCC Contract and applicable TOs. If DISS is not available, the VAL must contain the following information on the Contractor’s company letterhead:

- Company Name, Address, Telephone Number, Facility Security Clearance
- Commercial and Government Entity (CAGE) Code
- Contract/Order Number
- Name, Social Security Number, Date of Birth, Place of Birth, and Country of Citizenship of the personnel intending to visit
- Certification of Personnel Security Clearance and any Special Access authorizations required for the visit (Type of Investigation, Date of Investigation, Adjudication Date, and Agency)
- Name of COR
- Dates or period of time the VAL is to be valid

1.5.7.5 Security Contacts. Defense Information Systems Agency (DISA) Security can be contacted for Industrial Security (INDUSEC) or Personnel Security (PERSEC) related issues at (301) 225-1235 or via mail at the following addresses respectively:

Defense Information Systems Agency Agency ATTN: MP61, Industrial Security Command Building 6910 Cooper Ave. Fort Meade, MD 20755-7088	Defense Information Systems ATTN: MP62, Personnel Security Command Building 6910 Cooper Ave. Fort Meade, MD 20755-7088
---	--

For DISA-specific security related matters, contact the Directorate or Center Security Manager at:

Phone Number: (703) 614-5157
E-mail: ccpo_securitymanagers@ccpo.mil

1.5.7.6 Information Security and Other Miscellaneous Requirements.

1.5.7.6.1 Contractor personnel shall comply with all local security requirements, including entry and exit control for personnel and property at all Government facilities.

1.5.7.6.2 Contractor personnel shall comply with Attachment J-3: JWCC DD254, JWCC Contract PWS, Attachment J-2: Cloud Computing Cybersecurity Plan for Operations (C3PO), and all relevant security clauses of the JWCC Contract. Initial and periodic safety and security training and briefings will be provided by Government security personnel.

Failure to comply with Government security regulations and requirements may, at the Government's sole discretion, require the Contractor to provide the Government with a written remediation/corrective action plan; furthermore, failure to comply with such requirements may be cause for removal, resulting in the individual being unable to provide service on the JWCC Contract or any resultant TO.

- 1.5.7.6.3 Contractor employees whose access to CLASSIFIED information is suspended or revoked will not be permitted to fill positions requiring access to CLASSIFIED information on the JWCC Contract or resulting TOs.
- 1.5.7.6.4 The Contractor shall not disclose any U.S. Government non-public information, regardless of whether the information is UNCLASSIFIED or CLASSIFIED, including, but not limited to, any information about DoD files, data processing activities or functions, user identifications, passwords, to anyone not authorized to have access to such information. In the event that Contractor or Contractor personnel, subcontractor or subcontractor personnel, or affiliates, discloses non-public information, whether purposefully or inadvertently, the Contractor shall report the disclosure to the JWCC KO immediately, but no later than 24 hours after learning of the disclosure. This reporting requirement is in addition to any such reporting and mitigating actions the Contractor must make in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.239-7010 and DFARS clause 252.204-7012.
- 1.5.7.6.5 When at DoD facilities, the Contractor shall observe and comply with all health and security provisions, including the proper attire and display of identification IAW the DoD's facility requirements.
- 1.5.7.6.6 Both the JWCC KO and TO KO retain the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, violate DoD policy(s) or otherwise conflict with the interest of the Government.
- 1.5.7.6.7 In performance on this contract, Contractor personnel may generate or handle documents that contain Controlled Unclassified Information (CUI) at the Contractor's and/or Government's facilities. In performance on this contract, Contractor personnel will generate or handle documents that contain Proprietary, Contract Sensitive, or similarly designated information at the Contractor's facility. In performance on this contract, Contractor personnel will have access to, generate, and handle CLASSIFIED material up to TS only at the location(s) listed in the place of performance section of this document. All Contractor deliverables shall be marked IAW DoD Manual (DoDM) 5200.01, Vol. 3, DoD Information Security Program: Protection of Classified Information; DoD Instruction (DoDI) 5200.48, CUI; and DoDM 5400.07, Freedom of Information Act Program, unless otherwise directed by the Government. The Contractor shall comply with the provisions of the DoD Industrial Security Manual, DoD 5220.22-M - National Industrial Security Program Operating Manual (NISPOM), for handling CLASSIFIED material and producing deliverables.
- 1.5.7.7 The Contractor shall afford the Government access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in performance of this contract and any resultant TO. Access shall be provided to the extent required to carry out a program of

Information Technology (IT) inspection (to include vulnerability testing and any/all internal cybersecurity test data), investigation, and/or audit to safeguard against threats and hazards to the integrity, availability and confidentiality of data, or to the function of IT systems operated on behalf of DISA or DoD, and to preserve evidence of a crime.

- 1.5.7.8 The Contractor shall permit the Government to conduct adversarial cybersecurity assessments, which include mimicking cyber-attacks (such as those that nation-state adversaries are capable of), on both the DoD and Contractor parts of the cloud infrastructure, at times and places of DoD's choosing, from insider, nearsider, and outsider postures, using National Security Agency (NSA) certified red teams. Adversarial cybersecurity assessments will be coordinated with the JWCC Program Management Office (PMO) and Contractor Program Manager (PM) so as to ensure rules of engagement are properly coordinated in advance of any activity that has the potential to disrupt operations.
- 1.5.8 Post-Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post-award conference convened by JWCC PMO or the JWCC KO in accordance with Federal Acquisition Regulation (FAR) Subpart 42.5. In addition, periodic progress meetings will be convened by the JWCC KO, JWCC COR, and other Government personnel, as appropriate, to meet with the Contractor to review the Contractor's performance. At these periodic progress meetings the Government will inform the Contractor how its performance is/has been assessed and the Contractor will inform the Government of issues, if any, it experiences. Appropriate action shall be taken to resolve outstanding issues. These periodic progress meetings shall be at no additional cost to the Government.
- 1.5.9 Contracting Officer's Representative: The JWCC COR and each TO COR will be identified by a separate designation letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is not authorized to change any of the terms and conditions of this contract or any resultant TO.
- 1.5.10 Key Personnel: The Contractor shall provide a PM and a Deputy Program Manager (DPM) as Key Personnel. These individuals shall serve as the Contractor's primary management team and Points of Contact (PoCs). The PM and DPM shall be the Contractor's authorized interface with the JWCC KO and COR. The names of the PM and DPM, who are authorized to act on behalf of the Contractor, shall be designated in writing to the JWCC KO. The PM and DPM are responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising Contractor personnel, and communicating policies, purposes, and goals of the JWCC Contract to subordinates. The PM and DPM are responsible for overall contract performance and shall not serve in any other capacity under this contract. The PM or DPM shall be available between 8:00 a.m. and 4:30 p.m. Eastern Time, Monday through Friday, except on Federal holidays.

Substitution of Key Personnel: The contractor shall ensure the availability of Key Personnel with the requisite skills to perform the work detailed in the PWS, as described in the subsections below. The qualification of substituted key personnel must meet or exceed the key personnel qualification requirements.

- a. The contractor shall notify the JWCC KO prior to making any changes in personnel assigned as Key Personnel. The Government shall review all proposed Key Personnel skill levels prior to acceptance of all substitutions.
- b. During the first 180 days of performance, the Contractor shall make no substitutions of Key Personnel unless authorized by the JWCC KO.
- c. When making a substitution the Contractor shall provide: a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the JWCC KO. The Contractor shall, prior to making any substitution permanent, demonstrate to the satisfaction of the JWCC KO that the qualifications of the proposed substitute personnel meet the requirements described in the subsections below. The JWCC KO will notify the Contractor within 10 calendar days after receipt of all required information of the decision on proposed substitutions.

1.5.10.1 Program Manager:

1.5.10.1.1 The education and experience required for the PM is, at a minimum, a Bachelor of Arts/Bachelor of Science degree in a technical or managerial discipline, a Program Management Professional (PgMP) or Project Management Professional (PMP) certification or at the discretion of the Government, other Program/Project Management certification equivalencies in lieu of PMP, and at least 20 years of experience managing complex IT programs. If the PM has an advanced degree (e.g. Master's degree), the required minimum years of experience is 15 years experience in managing complex IT programs. Additionally no less than 5 years of experience must be met through contiguous practice in a commercial environment, at the minimum credentialed level (i.e. with a Bachelors Degree and PMP certification).

1.5.10.1.2 The PM shall be a U.S. citizen and shall possess (at the time of contract award) a fully adjudicated U.S. TS clearance with SCI eligibility and/or Special Accesses, IAW the Attachment J-3: JWCC DD254, to perform all services required by the JWCC Contract and resultant TOs.

1.5.10.2 Deputy Program Manager:

1.5.10.2.1 The education and experience required for the DPM is, at a minimum, a Bachelor of Arts/Bachelor of Science degree in a technical or managerial discipline, a Program Management Professional (PgMP) or Project Management Professional (PMP) certification or at the discretion of the Government, other Program/Project Management certification equivalencies in lieu of PMP, and at least 15 years of experience managing complex IT programs. If the DPM has an advanced degree (e.g. Master's degree), the required minimum years of experience is 10 years experience in managing complex IT programs. Additionally, no less than 5 years of contiguous practice in a commercial environment, at the minimum credentialed level (i.e. with a Bachelors Degree and PMP certification).

- 1.5.10.2.2 The DPM shall be a U.S. citizen and shall possess (at the time of contract award) a fully adjudicated U.S. TS clearance with SCI eligibility and/or Special Accesses, IAW the JWCC Contract DD254, to perform all services required by the JWCC PWS and resultant TOs.
- 1.5.10.3 The Contractor may provide additional appropriately cleared personnel to receive on-the-job training for any function for which personnel substitution may be anticipated, but in no case shall such training interfere with performance of any service.
- 1.5.11 Identification of Contractor Personnel: All Contractor personnel attending meetings and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as employees of the Contractor to avoid creating an impression in the minds of members of the public that they are Government officials. The Contractor must also ensure that all documents or reports produced by Contractor personnel are suitably marked as Contractor products.
- 1.5.12 Contractor Travel: All travel under the JWCC Contract shall comply with the FAR 31.205-46 Travel Costs unless an explicit waiver is granted from the JWCC KO. All travel must be approved by a Government Official with the requisite authority to approve travel.
- 1.5.13 Organizational Conflicts of Interest: Contractor personnel performing work under this contract, including any subcontractor personnel, may not receive, have access to, or participate in the development of proprietary or source selection information (e.g. cost or pricing information, analyses of budgetary or financial information, specifications or work statements) or perform evaluation services which may create an actual or apparent, current or subsequent, Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the JWCC KO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI, using the form found in Attachment J-10: Organizational Conflicts of Interest Form, and shall promptly submit an OCI plan to the JWCC KO to avoid or mitigate any such OCI. The JWCC KO has the sole discretion to determine whether or not the Contractor's OCI plan is acceptable. In the event the JWCC KO determines that any such OCI cannot be satisfactorily avoided or mitigated, the JWCC KO may take other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements that may be affected by the OCI.
- 1.5.14 Small Business: The Contractor shall implement an Attachment J-7: Small Business Participation Commitment Document (SBPCD). This will assist in the development of capabilities of small businesses and help provide small businesses the maximum practicable opportunity to participate in efficient contract performance for small businesses. The Contractor shall report all small business participation annually to the JWCC KO as for those Contract Line Item Numbers (CLINs) required IAW CDRL A010. Additionally, the Contractor shall report all small business performance under the JWCC Contract IAW Attachment J-6: Small Business Subcontracting Plan, using the electronic Subcontracting Reporting System (eSRS), IAW FAR Subpart 19.704 and CDRL A010.
- 1.5.15 Contractor Control of JWCC Infrastructure

- 1.5.15.1 The Contractor's unimpeded ability to exercise and maintain control over its JWCC infrastructure (other than disconnected TE devices) is critical in order to comply with the Government's security requirements. Within eight hours from initial Government notification, the Contractor shall coordinate and initiate implementation of Government-directed alterations or configuration changes to Contractor-owned/Contractor-operated JWCC infrastructure and capabilities to address critical security vulnerabilities or national security requirements. Such direction may come from the JWCC KO, or the JWCC COR; however, only the JWCC KO may make a change to the terms and conditions of the JWCC Contract.
- 1.5.15.2 Control is defined as:
- a. Unrestricted, uninhibited physical access; and
 - b. The ability to execute directives issued by the JWCC KO or JWCC COR within eight hours of Government notification.
- 1.5.15.3 The Contractor shall maintain Control, as defined above, throughout the entire JWCC Contract's period of performance, over the infrastructure the Contractor is utilizing for all UNCLASSIFIED and CLASSIFIED JWCC environments, including:
- a. Underlying hardware infrastructure, including networking components within Data Centers,
 - b. Underlying software layers, including the hypervisor and networking components,
 - c. Software platform Commercial Offerings and JWCC Offerings (excluding Third-Party Marketplace Offerings),
 - d. Hardware and software components of all Points of Presence, and
 - e. Facilities (inclusive of Sensitive Compartmented Information Facilities (SCIF)).
- 1.5.15.4 If a SCIF supporting the JWCC CLASSIFIED Infrastructure is supporting, or will support, other Government agencies' CLASSIFIED Infrastructure during the performance period of the JWCC contract, the Contractor shall have a fully executed co-use agreement signed by the host and tenant Cognizant Security Authorities (CSAs) as required in Intelligence Community Standard (ICS) 705-02 and follow all applicable Intelligence Community Guidance (e.g. Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities). DISA must be a signatory on the co-use agreement.
- 1.5.15.5 Depending on the urgency of the circumstances, a Government-directed alteration or configuration change may initially be provided verbally from the JWCC KO or JWCC COR. However, to the extent such an alteration or configuration change is deemed a "change" under FAR clause 52.212-4(c), that change will be reflected in writing by the JWCC KO as soon as practicable.
- 1.5.15.6 Contractors who lose Control during performance are subject to termination for cause per FAR 52.212-4, or any other administrative or legal action available to the Government to address the Contractor's default.

1.5.15.7 The Contractor must complete the Self-Certification of Control, as defined in the Solicitation Section H13: Mandatory Addendum to the JWCC Contract: Self-Certification of Control. The Contractor's Self-Certification of Control shall be attached to the JWCC Contract in Attachment J-15: Self-Certification of Control. At any time, and with any frequency throughout the PoP, the Government may request additional documentation to prove compliance with section 1.5.15.

1.5.16 Section 508:

1.5.16.1 IT Accessibility Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (Public Law 105-220), requires that when Federal agencies develop, procure, maintain, or use Information and Communications Technology (ICT), it shall be accessible to people with disabilities. Federal employees who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms, and services delivered pursuant to this PWS that are ICT, or contain ICT, must conform to the Section 508 standards, located at 36 Code of Federal Regulations (C.F.R.) § 1194.1 and Appendices A, C, and D, thereto, available at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>.

1.5.16.2 Unless an exception exists for Section 508 compliance per 36 C.F.R. § 1194.1, at the TO level, the following apply:

1.5.16.2.1 Functional Performance Criteria: The functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Section 508 standards, or when Chapters 4-6 do not address one or more functions of ICT.

1.5.16.2.2 Applicable requirements for software features and components: All Web Content Accessibility Guidelines Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application.

1.5.16.2.3 Applicable requirements for hardware features and components: All requirements apply.

1.5.16.2.4 Applicable support services and documentation: All requirements apply.

1.5.16.3 When providing hosting services for electronic content provided by the Government, the Contractor shall not implement the hosting services in a manner that reduces the existing level of conformance of the electronic content with applicable Section 508 standards.

Throughout the life of the contract, the Government reserves the right to perform testing on the Contractor's hosted solution to verify conformance with this requirement.

PART 2
DEFINITIONS & ACRONYMS

2. DEFINITIONS AND ACRONYMS:

2.1 DEFINITIONS:

2.1.1 ACCOUNT. As defined in C3PO.

2.1.2 ACCOUNT TRACKING AND AUTOMATION TOOL (ATAT). A web-based application that streamlines the cloud onboarding process for DoD and its Mission Partners after a Task Order is awarded. It accomplishes this by:

- a. Providing a simple-to-use interface,
- b. Automating the creation of users and environments, and
- c. Displaying a dashboard with near real-time cloud usage and other metrics

ATAT enables provisioning across multiple vendors and all classification levels.

2.1.3 ADDRESSING. As defined in C3PO.

2.1.4 ADMINISTRATIVE ACCESS. As defined in C3PO.

2.1.5 ALLOCATION. As defined in C3PO.

2.1.6 ANTIFRAGILE. As defined in C3PO.

2.1.7 ANYTHING AS A SERVICE (XaaS). The cloud computing service model that recognizes the vast number of products, tools, and technologies delivered to users as a service over the internet. The capabilities provided by CSPs may fall into the categories of IaaS, PaaS, and SaaS, but allow for the flexibility of the industry to include new and emerging service models such as Functions as a Service, Database as a Service, and others.

2.1.8 APPLICATION PROGRAMMING INTERFACE (API). An API is a set of specifications, definitions, and protocols used in building and integrating application software. It is most commonly used by service accounts or users executing scripts to interact with one or more applications/systems.

2.1.9 APPLICATION. As defined in C3PO.

2.1.10 APPLICATION SERVER. Physical infrastructure into which a user loads a commodity operating system and at least two application runtimes into a virtualized environment hosted on physical servers (e.g. a network router would not satisfy this definition of Application Server).

- 2.1.11 **ARTIFICIAL INTELLIGENCE (AI).** A system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever contextual circumstances it encounters.
- 2.1.12 **AUTHORIZING OFFICIAL (AO).** A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (National Institute of Standards and Technology (NIST) SP 800-37 Revision 2).
- 2.1.13 **AVAILABILITY ZONES/REGIONS.** Availability Zones have independent power and network backbone. A CSP's "region" encompasses multiple Availability Zones such that systems and data in a region with a failed Availability Zone could seamlessly transfer to another Availability Zone and continue operations.
- 2.1.14 **BRING YOUR OWN LICENSE (BYOL).** A model in which a JWCC user provides the license for a Cloud Service Offering (CSO) in whole or in part.
- 2.1.15 **CONTRACTOR COMMERCIAL CATALOG.** A complete listing of the Contractor's current, publicly available Commercial Offerings with associated pricing.
- 2.1.16 **CONTRACTOR PORTAL.** The Contractor Portal is provided by the Contractor as a User Interface (UI) that allows a human or machine user to access the web enabled JWCC Catalog, JWCC Marketplace, and other JWCC cloud resources as provided through the JWCC Contract. The Contractor Portal may also serve as an API endpoint.
- 2.1.17 **CLASSIFIED INFRASTRUCTURE.** As defined in C3PO.
- 2.1.18 **CLOSED-LOOP NETWORK.** A network that is able to operate with no external network connectivity (e.g. the Internet).
- 2.1.19 **CLOSED-LOOP SYSTEM.** System that is able to operate with no external connectivity.
- 2.1.20 **CLOUD.** The practice of pooling physical servers and using them to provide services that can be rapidly provisioned with minimal effort and time, often over the Internet. The term is applied to a variety of different technologies (often without clarifying modifiers), but, for the purpose of this PWS, "cloud" refers to physical computing and storage resources pooled to provide virtual computing, storage, or lighter-level services
- 2.1.21 **CLOUD BOUNDARY.** Physical boundary between JWCC and any external systems or networks.
- 2.1.22 **CLOUD ENVIRONMENT.** A collection of physical and logical assets, provided by a CSP, that minimally supports the hosting and operation of workloads.

- 2.1.23 CLOUD SERVICE OFFERING (CSO). XaaS and cloud services such as those that are sold in the commercial marketplace.
- 2.1.24 CLOUD SERVICE PROVIDER (CSP). An organization that provides cloud services.
- 2.1.25 CLOUD WORKLOAD. A collection of one or more: applications, services, capabilities; or, a specific amount of work in the cloud, all of which consume cloud resources.
- 2.1.26 COMMERCIAL OFFERING. Any Offering in the Contractor's Commercial Catalog that is licensable, consumable, or purchasable by the general public.
- 2.1.27 COMMERCIAL PARITY. The JWCC catalog will consist of every current and future Commercial Offering, including cloud items on the Contractor's Commercial Catalog; and available for DoD consumption at each classification level and IL. JWCC Offerings are, at a minimum, Functionally Equivalent to the hardware, services, interfaces, and capabilities that are Commercial Offerings; use the Contractor's commercial, public cloud pricing model as a basis for pricing all security domains, all classification levels, and all ILs; and are available across all security domains, all classification levels, and all ILs.
- 2.1.28 COMMERCIALY AVAILABLE. An Offering that is of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes, and is offered for sale, lease, or license to the general public.
- 2.1.29 CONFIDENTIALITY. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- 2.1.30 CONTINENTAL UNITED STATES (CONUS). The 48 connected States that make up the United States and the District of Columbia.
- 2.1.31 CONTRACTOR. The supplier or vendor awarded a JWCC Contract.
- 2.1.32 CONTRACTING OFFICER (KO). A U.S. Government representative with authority to enter into, administer, and/or terminate U.S. Government contracts, and make related determinations and findings on behalf of the U.S. Government.
- 2.1.32.1 The JWCC KO is the authorized and warranted individual for the JWCC IDIQ acquisition environment contracts.
- 2.1.32.2 The JWCC TO KO are the authorized and warranted individuals for TOs issued under the JWCC IDIQ acquisition environment contracts.
- 2.1.33 CONTRACTING OFFICER'S REPRESENTATIVE (COR). A Government employee appointed by the KO to assist in administering a contract. The COR is authorized to provide technical direction to the Contractor so long as such direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does

not have authority to change a contract's terms and conditions or to legally bind the Government.

- 2.1.34 CRYPTOGRAPHIC CERTAINTY. As defined in C3PO.
- 2.1.35 CRYPTOGRAPHIC ERASE. Leveraging the encryption of target data by enabling sanitization of the target data's encryption key which leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access. (NIST SP 800-88 Revision 1)
- 2.1.36 DATA CENTER. As defined in C3PO.
- 2.1.37 DAY. Calendar day, unless specified otherwise.
- 2.1.38 DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the JWCC PWS.
- 2.1.39 DELIVERABLE. Any provided response to a requirement or set of requirements that is presented to a customer as work complete.
- 2.1.40 ELASTIC. The ability to quickly expand or contract resources to meet changing demands without worrying about capacity planning and usage loading.
- 2.1.41 FAILOVER. As defined in C3PO.
- 2.1.42 FEDERATED IDENTITY. An assured process that allows for the conveyance of authentication and subscriber attribute information across networked systems, in this case between the CSP's Identity and Access Management (IAM) and DoD systems.
- 2.1.43 FIRST-PARTY CLOUD SERVICE OFFERINGS. CSOs provided directly by the Contractor inclusive of XaaS and subject to the DoD Cloud Computing Security Requirements Guide (CC SRG), therefore requiring Provisional Authorization.
- 2.1.44 FIRST-PARTY MARKETPLACE OFFERINGS. Contractor-owned, Contractor-operated CSO provided directly to the client.
- 2.1.45 FUNCTIONALLY EQUIVALENT. The successful achievement of Commercial Parity, resulting in: (a) individuals trained on the Commercially Available Offerings to be able to utilize JWCC Offerings, at any classification level and IL, and experience a consistent user experience; (b) code to be reused, just as if utilizing the Commercially Available Offering; and (c) all API calls and portal UI actions resulting in the same consistent behavior, except when prohibited by Government restrictions due to classification level or IL.
- 2.1.46 HIGHLY AVAILABLE. A failover feature to ensure availability during device or component interruptions. This availability shall be greater than 99.9% percent and no worse than the

commercial SLA standard for the given service.

- 2.1.47 **HYPERSCALE.** An industry term used to describe CSPs with a global footprint that are able to provide horizontal scalability with high performance, throughput, and redundancy, efficiently leveraging economies of scale to provide low commercial pricing. This scalability is typically in the millions of Central Processing Units (CPUs), Exabytes of storage, and Highly Available services (typically between 99.9% to 99.999% percent uptime).
- 2.1.48 **HYPERVERSOR.** A collection of software modules that provides virtualization of hardware resources (such as CPU/Graphics Processing Unit (GPU), Memory, Network, and Storage) on a single physical host.
- 2.1.49 **IMPACT LEVEL 2 (IL 2).** As defined in C3PO.
- 2.1.50 **IMPACT LEVEL 4 (IL 4).** As defined in C3PO.
- 2.1.51 **IMPACT LEVEL 5 (IL 5).** As defined in C3PO.
- 2.1.52 **IMPACT LEVEL 6 (IL 6).** As defined in the CC SRG.
- 2.1.53 **INDEPENDENT VERIFICATION AND VALIDATION (IV&V).** An independent system assessment that analyzes and tests the target system to: 1) ensure that it performs its intended functions correctly; 2) ensure it performs no unintended functions; and 3) measure its quality and reliability.
- 2.1.54 **INFRASTRUCTURE.** As defined in C3PO.
- 2.1.55 **INFRASTRUCTURE AS A SERVICE (IaaS).** A cloud computing service model wherein the capability is provided to the consumer to provision processing, storage, networks, and other fundamental computing resources allowing the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).
- 2.1.56 **INFRASTRUCTURE AS CODE (IaC).** The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools. (NIST SP 800-172)
- 2.1.57 **INVESTIGATION.** As defined in C3PO.
- 2.1.58 **JWCC CATALOG.** The Contractor provided listing of all its JWCC Offerings, which includes the associated JWCC price for each Offering, the DoD Authorization (Provisional

Authorization) for each Offering, and identifies the applicable classification level and IL for each Offering, viewable only by DoD users.

- 2.1.59 JWCC MARKETPLACE. A mechanism (e.g. portal, console), provided by the Contractor, for fulfilling orders, provisioning, and deploying the approved JWCC Offerings, by classification level and IL, with Policy Based Access Control (PBAC) for fulfilling orders, provisioning, deploying, and cloud operations, and additionally allows a JWCC user to fulfill orders and schedule non-provisionable or deployable JWCC Offerings (e.g. Cloud Support Packages).
- 2.1.60 JWCC OFFERING. Any Offering in the Contractor's JWCC Catalog.
- 2.1.61 LOGICAL SEPARATION. As defined in C3PO.
- 2.1.62 MACHINE LEARNING (ML). The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.
- 2.1.63 MANAGEMENT PLANE. Portion of the Contractor's Cloud Environment that a user has no access to.
- 2.1.64 MEAN TIME TO RESOLVE. A service-level metric that measures the average elapsed time from when an incident is reported until the incident is resolved.
- 2.1.65 MIGRATION. The act of moving an application and/or data from one infrastructure or platform to another infrastructure or platform.
- 2.1.66 MITIGATION. As defined in C3PO.
- 2.1.67 ****RESERVED****
- 2.1.68 MODERN. Relating to the present or recent times as opposed to the remote past or antiquated technology.
- 2.1.69 NEARLINE STORAGE. Storage that is not immediately available, but can be brought online quickly without human intervention.
- 2.1.70 NEARSIDER. An individual that has physical access to the hardware but does not have logical access to the actual data.
- 2.1.71 NETWORK. As defined in C3PO.
- 2.1.72 OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS). All geographical areas outside of the 48 connected states that make up the continental United States and the District of Columbia.

- 2.1.73 **OFFERING.** Any Contractor item (e.g. service offerings, cloud offerings, CSOs, cloud support packages, TE offerings, cloud services, cloud capabilities, advisory and assistance services) available for licensing, purchase, or consumption.
- 2.1.74 **OFFLINE STORAGE.** Storage where the data is not immediately available and typically requires some human or scheduled intervention to become Online or Nearline Storage; Offline Storage is also known as cold storage.
- 2.1.75 **ONLINE STORAGE.** Storage that is immediately accessible to applications without human intervention.
- 2.1.76 **PHYSICAL SECURITY.** Security activities concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
- 2.1.77 **PLATFORM AS A SERVICE (PaaS).** A cloud computing service model wherein the capability provided to the consumer is to deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools onto the cloud infrastructure supported by the Contractor. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- 2.1.78 **POINTS OF PRESENCE.** A demarcation point or interface point between communicating entities. For purposes of JWCC, this is a network access point under the Contractor's control, as defined in section 1.5.15 of the JWCC PWS, where JWCC is accessible to DoD.
- 2.1.79 **PRODUCTION PLANE.** Portion of the Contractor's Cloud Environment infrastructure that a user has access to.
- 2.1.80 **PROVISIONAL AUTHORIZATION.** A pre-acquisition type of Risk Management Framework (RMF) information system authorization used by DoD and the Federal Risk and Authorization Management Program (FedRAMP) to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and information systems.

Provisional Authorizations are to be used by Federal and DoD Cloud Mission Owners during source selection and subsequent system authorization under RMF. (CC SRG)

- 2.1.81 **PROVISIONING.** The act of creating and/or configuring resources in the Cloud Environment (e.g. accounts, compute instances, users, storage mechanisms) using either manual (i.e. via a Contractor's Portal (UI)) or automated (i.e. API) processes.
- 2.1.82 **PURGE.** Apply physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques. (NIST SP 800-88 Revision 1).

- 2.1.83 **QUALITY ASSURANCE.** The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.
- 2.1.84 **QUALITY ASSURANCE SURVEILLANCE PLAN (QASP).** An organized written document specifying the methodology to be used for surveillance of the Contractor's performance.
- 2.1.85 **QUALITY CONTROL.** All necessary measures taken by the Contractor to assure that the quality of an end product or service meets contractual requirements.
- 2.1.86 **RESILIENCE.** The ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and recover to an effective operational posture in a time frame consistent with mission needs. (NIST SP 800-39 under Information System Resilience; and NIST SP 800-53 Revision 4 [Superseded] under Information System Resilience).
- 2.1.87 **RESOURCE POOLING.** Pooling the Contractor's computing resources to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and re-assigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact locations of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or Data Center). Examples of resources include storage, processing, memory, and network bandwidth.
- 2.1.88 **ROBUST INFRASTRUCTURE.** Infrastructure that is responsive, resilient, redundant, and reliable.
- 2.1.89 **ROLE.** A job function, with associated system access privileges, to which people or other system entities may be assigned in a system.
- 2.1.90 **RUGGEDIZED.** System specifically designed to meet or exceed Military Standard (MIL-STD) 810H standards to ensure reliable operations in hard usage conditions. Whether a system needs to be tested and certified as meeting the standard is at the Government's discretion.
- 2.1.91 **SCALABILITY.** The ability to increase or decrease resources commensurate with demand.
- 2.1.92 **SELF-SERVICE.** The ability of a user to access data and perform actions without any human interaction or third-party approval.
- 2.1.93 **SERVER.** As defined in C3PO.
- 2.1.94 **SERVICE MODEL.** The highest-level categorization of cloud services as based on the type of computing capability that is provided. (NIST SP 500-322).

- 2.1.95 **SERVICE LEVEL AGREEMENT (SLA).** A SLA sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems, and the measures by which the effectiveness of the process is monitored and approved.
- 2.1.96 **SERVICE LEVEL OBJECTIVE (SLO):** Within SLAs, SLOs are the objectives that must be achieved, for each service activity, function and process, to provide the best opportunity for service recipient success.
- 2.1.97 **SOFTWARE AS A SERVICE (SaaS).** A cloud computing service model wherein the consumer is provided with the capability to use applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- 2.1.98 **SUBCONTRACTOR.** A party that enters into a contract with the Contractor. The Government does not have privity of contract with subcontractors.
- 2.1.99 **TACTICAL EDGE (TE).** The boundary considered to be everything forward of a deployed tactical network's Defense Information Systems Network (DISN) point-of-presence/Service Delivery Node (SDN). The contours of the TE will vary by service, mission, phase of an operation, bandwidth availability, and other factors (technical and non-technical).
- 2.1.100 **TACTICAL EDGE DEVICE.** Devices that address the needs of disadvantaged users operating at the TE. For the purposes of JWCC, a disadvantaged user experiences DDIL bandwidth that restricts capabilities at the TE. Disadvantaged users may include leaders, warfighters, sensors, platforms, and networked weapon systems not connected with organic communications assets and requiring additional means to acquire network transport and services. Disadvantaged users need to be able to access DoD designated networks and requisite compute resources from wherever they are operating.
- 2.1.101 **TACTICAL EDGE OFFERING.** A subset of Offerings that relate specifically to TE Devices and any Offerings which execute on or support the TE Device(s).
- 2.1.102 **TESTING.** See Independent Verification and Validation and C3PO (as applicable for security requirements).
- 2.1.103 **THIRD-PARTY CLOUD SERVICE OFFERING.** CSOs provided on behalf of a third-party vendor via the Contractor's Marketplace inclusive of XaaS and subject to the CC SRG, therefore requiring no less than Provisional Authorization. Additionally, all licensing

must comply with the terms and conditions of the JWCC Contract regardless of the licensing relationship with the third-party vendor and the Contractor.

- 2.1.104 **THIRD-PARTY MARKETPLACE OFFERINGS.** Third-party-owned, third-party-operated, and third-party-provided CSOs, made available via the Contractor's Portal (UI) and/or provided directly to the client. Additionally, all licensing must comply with the terms and conditions of the JWCC Contract regardless of the licensing relationship with the third-party vendor and the Contractor.
- 2.1.105 **TRAFFIC.** As defined in C3PO.
- 2.1.106 **UNCLASSIFIED INFRASTRUCTURE.** As defined in C3PO.
- 2.1.107 **USER.** Individual, or (system) process acting on behalf of an individual, authorized to access an information system.
- 2.1.108 **VIRTUAL ENCLAVE.** On-demand configurable pool of shared computing and storage resources within a multi-tenant Cloud Environment that is logically isolated from other tenants.
- 2.1.109 **VIRTUAL MACHINE (VM).** Software that emulates a computer's physical hardware.
- 2.1.110 **VULNERABILITY.** As defined in C3PO.
- 2.1.111 **WORK DAY.** The number of hours per day the Contractor provides services IAW the JWCC Contract.
- 2.1.112 **WORK WEEK.** Monday through Friday, unless otherwise specified.
- 2.1.113 **WORKSPACE.** A pool of resources and services within a Cloud Environment that supports a specific project. A workspace, which may be referred to as a cloud services account, can be billed inclusive of the resources and services within the workspace, either singularly or collectively.
- 2.1.114 **DOD.** The DoD as defined in 10 United States Code (U.S.C.) § 111

2.2 **ACRONYMS:**

ABAC	Attribute-Based Access Control
ACOR	Alternate Contracting Officer's Representative
AI	Artificial Intelligence
AO	Authorizing Official
API	Application Programmers Interface
ATAT	Account Tracking and Automation Tool
ATO	Authorization to Operate

BYOL	Bring Your Own License
C3PO	Cloud Computing Cybersecurity Plan for Operations
CAGE	Commercial and Government Entity
CC SRG	Cloud Computing Security Requirements Guide
CDRL	Contract Data Requirements List
CDS	Cross-Domain Solution
C.F.R.	Code of Federal Regulations
CLIN	Contract Line Item Number
CMPR	Contract Monthly Progress Report
COMSEC	Communications Security
CONUS	Continental United States
COR	Contracting Officer's Representative
CPMP	Contractor Program Management Plan
CPU	Central Processing Unit
CSO	Cloud Service Offerings
CSP	Cloud Service Provider
CSV	Comma Separated Values
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DSD	Deputy Secretary of Defense
DevSecOps	Development, Security, and Operations
DD254	Department of Defense Contract Security Classification Specification
DDIL	Disconnected, Disrupted, Intermittent, and Limited
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISS	Defense Information System for Security
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Networks
DoD ISRMC	Department of Defense Information Security Risk Management Committee
DoDM	Department of Defense Manual
DPM	Deputy Program Manager
EM	Electromagnetic
EO	Executive Order
FAR	Federal Acquisition Regulation
FCL	Facility Security Clearance
FFP	Firm-Fixed-Price
FIDO2	Fast Identity Online
FOIA	Freedom of Information Act
FY	Fiscal Year
GFI	Government Furnished Information

GFP	Government Furnished Property
GPU	Graphics Processing Unit
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IAW	In Accordance With
IC	Intelligence Community
ICD	Intelligence Community Directive
ICT	Information and Communications Technology
IDIQ	Indefinite Delivery/Indefinite Quantity
IL	Impact Level
INDUSEC	Industrial Security
INFOSEC	Information Security
IPR	In-Progress Review
IT	Information Technology
JAB	Joint Authorization Board
IUID	Item Unique Identification
JROC	Joint Requirements Oversight Council
JSIG	Joint Special Access Program Implementation Guide
JSON	JavaScript Object Notation
JTR	Joint Travel Regulation
JWCC	Joint Warfighting Cloud Capability
JWICS	Joint Worldwide Intelligence Communication System
KO	Contracting Officer
LiFi	Light Fidelity
MFA	Multi-Factor Authentication
ML	Machine Learning
NARA	National Archives Records Administration
NATO	North Atlantic Treaty Organization
NoSQL	Non-SQL
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAuth	Open Authorization
OCI	Organizational Conflict of Interest
OCONUS	Outside of the Continental United States
OSCAL	Open Security Controls Assessment Language
PaaS	Platform as a Service
PBAC	Policy-Based Access Control
PDF	Portable Document Format
PERSEC	Personnel Security
PgMP	Program Management Professional
PIEE	Procurement Integrated Enterprise Environment
PKI	Public Key Infrastructure

PM	Program Manager
PMO	Program Management Office
PMP	Project Management Professional
PoC	Point of Contact
PoP	Period of Performance
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
RTB	Raise the Bar
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAP	Special Access Program
SBPCD	Small Business Participation Commitment Document
SCI	Sensitive Compartmented Information
SDN	Service Delivery Node
SIPR	Secret Internet Protocol Router
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLO	Service Level Objective
SMO	Security Management Office
SOC	System and Organizational Control
SP	Special Publication
SQL	Structured Query Language
SSO	Special Security Office
T&M	Time and Materials
T3	Tier 3 Investigation
T3R	Tier 3 Reinvestigation
T5	Tier 5 Investigation
T5R	Tier 5 Reinvestigation
TE	Tactical Edge
TEM	Technical Exchange Meeting
TO	Task Order
TPU	Tensor Processing Unit
TS	Top Secret
UI	User Interface
U.S.	United States
U.S.C.	United States Code
VAL	Visit Authorization Letter
XaaS	Anything as a Service
XML	Extensible Markup Language

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

- 3.1 GFP will be provided as indicated in Attachment J-8: GFP included in the solicitation, which will be distributed at award, and incorporated via the GFP module in the Procurement Integrated Enterprise Environment (PIEE). GFP shall be managed IAW the terms of FAR 52.245-1, GFP DFARS clauses, and additional GFP Contractor Management instructions in Section G of the solicitation. Types of GFP anticipated to be provided include: Cryptographic Fill Device(s), Simple Key Loaders, and other DoD-approved encryption hardware.

The Contractor shall accept and/or report provided GFP via the Shipping and Receiving document in the PIEE GFP module (or NSA Equivalent) upon acceptance and/or IAW additional GFP Contractor Management instructions in Section G of the JWCC Contract. Serially managed GFP that is provided to the Contractor by DoD requires all events identified in DFARS 252.211-7007 (and/or any subsequent DFARS, NSA or Agency specific GFP reporting requirements) to be reported by the Contractor. Non-serially managed GFP only requires the GFP receipt to be reported in the PIEE GFP module.

The Contractor, when in possession of GFP, shall provide the JWCC COR and/or TO COR an Annual Report (CDRL A015) of all GFP in its possession, including item description(s), make(s), model(s), serial number(s), Item Unique Identification(s) (IUID), and last inventory date one month prior to the end of base and option period of the contract and/or IAW NSA Guidelines, additional GFP contractor management instructions in Section G of the JWCC contract.

- 3.2 Government Furnished Information (GFI). API interface data for Attachment J-11: ATAT Multi-Cloud Provisioning API and Cross-Domain Solution (CDS) Design and Implementation Requirements: 2020 Raise the Bar (RTB) Baseline Release (or current version) data package are provided as GFI under the JWCC Contract.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

- 4.1 General: The Contractor shall furnish all supplies, equipment, facilities, and services required to perform work under this contract that are not listed under Part 3 of this PWS.

PART 5
REQUIREMENTS

5 Specific Tasks:

5.1 Program Management

- 5.1.1 The Contractor shall provide overarching program management personnel, processes, and tools under CLINs x008, as necessary to manage and oversee all Contractor activities for the duration of their JWCC Contract within cost, schedule, performance, and quality requirements.
- 5.1.2 The Contractor shall establish and maintain a formal PMO, which shall coordinate and interface with the JWCC COR and JWCC PMO to ensure the JWCC Contract is being used efficiently, compliant with JWCC requirements, and making use of commercial best practices.
- 5.1.3 The Contractor shall appoint a PM and a DPM empowered to make program and project-level decisions and commit resources necessary to successfully execute courses of action within scope of the JWCC Contract.
- 5.1.4 The Contractor's PM support will facilitate the timely authorization of JWCC infrastructure and Offerings to be included on the JWCC Catalog at all classification levels and ILs, and take all necessary steps to ensure successful integration with the DoD's ATAT provisioning tool with the Contractor's management systems for JWCC, as appropriate.
- 5.1.5 The PM and DPM shall have sufficient expertise and authority to execute the following responsibilities: (a) serve as the official central PoC and interface between the Contractor and the COR; (b) be available as needed for interaction with the JWCC COR, JWCC PMO, and JWCC KO; and (c) monitor and report on contract status (CDRL A001) and compliance with the JWCC Contract requirements.
- 5.1.6 The Contractor shall perform the following requirements and provide the following deliverables. All materials shall be provided error free and presented in a professional manner.
 - 5.1.6.1 The Contractor Program Management Plan (CPMP) (CDRL A021) shall include with sufficient detail such that the Government can assess and understand how the Contractor intends to meet all requirements outlined in the PWS.

The CPMP demonstrates the Contractor's approach, timeline, and tools to be used in execution of the Contract. The CPMP should be in both a narrative and graphic format that discusses and displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc

data collection reporting requests as identified within the PWS. The CPMP shall be the primary plan and all other plans (e.g. the QCP) required and defined in the PWS will be subordinate to the CPMP. The Contractor shall provide at time of proposal submission the initial CPMP. Once the Government agrees with the CPMP, the finalized copy shall be provided within 10 business days after final Government input(s) are received. The CPMP shall be updated as needed thereafter, but no less than annually.

The CPMP shall, at a minimum, include a description of the management and execution approach to include: all information required under administration and execution of the entirety of 5.1.6.

5.1.6.2 The Contract Monthly Progress Report (CDRL A001) is for overall performance under the JWCC Contract and access to all Task Order Monthly Progress Reports (CDRL A012) for PM performance. The Contract Monthly Progress Report shall include, but not be limited to, the following:

5.1.6.2.1 A full accounting of each TO received, the execution status of the TO, total value of the TO, and funds expended to date on the TO.

5.1.6.2.2 The report shall include, at a minimum, the JWCC utilization metrics and the percentage as compared to the Contractor's total commercial and non-commercial utilization and capacity. The Contractor should ensure the information in the report is assessed and appropriately marked with portion markings IAW the DoDM 5200.01. These portion markings shall be limited to 5.1.6.2 and its subsections.

The report shall be broken out by CSO and CLIN per month, year, and life of the JWCC Contract for the following metrics:

5.1.6.2.2.1 Network. Volume of commercial client traffic, in megabytes, for public internet ingress and egress (at the logical Cloud Boundary outside of Availability Zones, i.e. in and out of the Contractor's controlled infrastructure) per month and aggregated for the duration of the JWCC Contract to date. This measure and metric shall include a discrete breakdown comparison of the following: commercial traffic, JWCC Contract traffic, TO traffic by Availability Zone and comprehensively, as both raw volume and the Government's equivalent utilization as a percentile comparison.

5.1.6.2.2.2 Compute. Number of physical (not virtualized) compute (e.g. CPU, GPU, or other processor technology as applicable) cores in use by Application Servers. Application Servers are defined as those physical servers that host the virtualized infrastructure and platform services used by end users (e.g. a server that is hosting JWCC Contract applications is an Application Server, while a network router does not satisfy this definition of Application Server). Additionally, the number of physical compute cores that are available for future use (not currently allocated to an Application Server, nor in use by Application Server) both comprehensively and by Availability Zone.

- 5.1.6.2.2.3 Storage. Data, in megabytes, consumed and available, for each of online, nearline, and offline storage, averaged across the month and aggregated for the life of the JWCC Contract.
- 5.1.6.2.2.4 Additionally, the report shall identify the base (e.g. base 2 or base 10) for all measured values using bytes.
- 5.1.6.2.3 An accurate, clear and precise measure and metric for each performance criteria listed in Technical Exhibit 1, Performance Requirements Summary, of the Attachment J-1: JWCC PWS. This shall include monthly and accrued measures and metrics over the life of the JWCC Contract.
- 5.1.6.2.4 Progress of the ability to create and deliver the following CDRLs:
- 5.1.6.2.4.1 A report on usage, by TO, for any GFP (CDRL A015).
- 5.1.6.2.4.2 A report on ordering, by TO, for any TE Offering and any associated TE Devices (CDRL A012).
- 5.1.6.2.4.3 A report of any quality defect findings, regardless of severity, resulting from application of the QCP (CDRL A008) processes, including operationally induced failures, and organized by the associated TO against which the finding was discovered.
- 5.1.6.2.4.4 A status of small business allocation of work, by size and category, as required in section 1.5.14 of the JWCC PWS (CDRL A010).
- 5.1.6.2.4.5 A status of both the identification of a financial system and the associated TO for System and Organization Control (SOC 1) Type II reporting as required in section 5.4 of the JWCC PWS and SOC Audit Report (CDRL A014).
- 5.1.6.2.5 Any issues, challenges, problems, risk areas, or requests for JWCC COR support.
- 5.1.6.3 The Contractor shall attend and participate in meetings arranged, executed, and facilitated by the Government. The Government will coordinate a kickoff meeting for all Contractors receiving an award within ~~15~~ 30 calendar days after contract award. The Contractor is responsible for coordinating with the JWCC COR. The kickoff meeting will be conducted in-person with the Contractor's primary staff that will interface with the JWCC PMO and will be held in the National Capital Region. The kickoff meeting will be conducted with all JWCC Contract holders in attendance at the same time. All JWCC Contract holders will be allowed one-on-one breakout sessions, if requested, for presentation of Contractor materials and any specific questions regarding the JWCC Contract.
- 5.1.6.4 The Contractor shall arrange, execute, and facilitate meetings when requested by the JWCC PMO, or as required, in support of the JWCC Contract.

5.1.6.4.1 In-Progress Reviews (IPRs). The Contractor shall arrange, facilitate and execute quarterly IPRs, as well as any additional IPRs at the request of the JWCC KO or JWCC COR. IPRs will be conducted either in-person or virtually at the request of the Government, and the government reserves the right to include virtual attendees for in-person meetings. The Contractor is responsible for providing an agenda, presentation materials, and meeting minutes (CDRL A013) for all IPRs. Minimum content for IPRs shall include, but is not limited to, the following:

- 5.1.6.4.1.1 Overall JWCC Contract execution, management and operating status update;
- 5.1.6.4.1.2 Discussion, as necessary, of any upcoming JWCC Catalog changes (as captured in JWCC Catalog with Change Report (CDRL A022)), including addition, modification, deletion or deprecation;
- 5.1.6.4.1.3 Specific recommendations to better optimize JWCC Offerings, operations, and deployment based on empirical evidence, with projections for implementation of those recommendations;
- 5.1.6.4.1.4 Recommendation to improve communication between the Contractor and the JWCC COR;
- 5.1.6.4.1.5 Status of, and any issues regarding, use of and interfacing with ATAT;
- 5.1.6.4.1.6 Identification of JWCC Contract issues or problems, with regard to management or operations of the JWCC Contract, and the associated risks and mitigation plan;
- 5.1.6.4.1.7 Advising on the utilization of JWCC Contract and how it aligns to the commercial trends and practices;
- 5.1.6.4.1.8 Advising on establishing optimization goals with recommendations to achieve the goals; and for prior goals, a status of progress to achieve the goal and an anticipated completion date;
- 5.1.6.4.1.9 Discussion of any previous quarter C3PO required reports submitted to the JWCC COR;
- 5.1.6.4.1.10 Any Government agenda items provided to the Contractor for inclusion in the scheduled IPR;
- 5.1.6.4.1.11 Report on status of, and any issues regarding, exceptions.

5.1.6.4.2 Technical Exchange Meetings (TEMs). As requested by the JWCC COR, the Contractor shall -arrange, facilitate and execute TEMs. TEMs can include discussions of any current or upcoming TOs, any future JWCC Offerings and Commercial Offerings the Contractor will have available for purchase, and any content/topics determined by the JWCC COR or the

JWCC PMO. The Contractor is responsible for providing meeting minutes (CDRL A013) for all TEMs.

- 5.1.6.4.3 Ad Hoc Reporting/Information Products. The Contractor shall work with the JWCC COR to identify required ad hoc reports or information products related to deployment and utilization of the JWCC Contract. These reports or products will be used to assist the JWCC COR for effective deployment of the JWCC Contract. This reporting is in addition to other reporting requirements mentioned herein.
- 5.1.6.5 Ordering Guide Inputs.
 - 5.1.6.5.1 The Contractor shall address, as part of the Contract Ordering Guide Annex (CDRL A007), any specific information that users need to understand how to successfully order JWCC Offerings, to be included in the JWCC Ordering Guide.
 - 5.1.6.5.1.1 Contractor's PoC information and e-mail for contracting related issues.
 - 5.1.6.5.1.2 Contractor's email address for distribution of TOs (if different from above).
 - 5.1.6.5.1.3 Link to Contractor's hosting and compute calculators (hereafter referred to as "Calculators") at each classification level for the purpose of Independent Government Cost Estimate development that identifies only those JWCC Offerings that are authorized for DoD consumption under the JWCC Contract.
 - 5.1.6.5.1.4 Any specific process the Contractor may have for requesting TE Offerings that deviates from the normal fulfillment process.
 - 5.1.6.5.1.5 Any specific process the Contractor may have for requesting Cloud Support Packages.
 - 5.1.6.5.1.6 The Contractor's inputs to the Contract Ordering Guide Annex shall be delivered to the Government (CDRL A007).
 - 5.1.6.6 Contractor Cloud Portal Process. The Contractor shall provide to the JWCC COR the process of establishing initial accounts and Cloud Environments using the Contractor's Portal (both UI and API) and how to fulfill orders and provision/deploy JWCC Offerings from its JWCC Marketplace after the JWCC user account has been established. The Contractor Cloud Portal Process (CDRL A002) shall be delivered to the Government no later than 15 days after contract award and as necessary when changes are made. Only JWCC Offerings shall be visible and accessible in the JWCC Marketplace. A link (via Internet Protocol address) to the Contractor's Portal will be provided by Contractor for distribution to JWCC users for each classification level and IL.
 - 5.1.6.7 JWCC Catalog. The Contractor shall submit its Commercial Catalog with Change Report (CDRL A023). The Contractor's Commercial Catalog shall be the basis by which the JWCC Catalog is established. The Contractor shall submit its JWCC Catalog as Attachment J-4:

JWCC Catalog Discounts, Premiums, and Fees. For additions or modifications to JWCC Offerings, the Contractor shall follow the process in G11, JWCC Catalog Modifications, and submit the JWCC Catalog with Change Report (CDRL A022). The Contractor shall support the JWCC KO/COR in the maintenance and upkeep of the JWCC Catalog by recording and reporting changes on a periodic basis via the JWCC Catalog with Change Report (CDRL A022).

- 5.1.6.8 Quality Control Plan (QCP). The Contractor shall provide a QCP supporting the Government-provided QASP for the JWCC Contract (see Attachment L-6). At a minimum, the QCP shall describe the approach for continuously meeting the performance metrics in Technical Exhibit 1 of the JWCC PWS, throughout the life of the JWCC Contract. The Contractor shall specifically address how all required performance metrics will be assessed, analyzed, and maintained through the life of the JWCC Contract.

Cross-referencing between the QCP and PWS is permitted.

- 5.1.6.8.1 The Contractor shall provide a PoC as part of the QCP to allow any JWCC user to communicate any issues or failures that arise from an attempt to invoke a JWCC Offering (provisioning) as ordered within a valid JWCC account. The contractor shall provide near-immediate acknowledgement (within 5 minutes of submission). The Contractor will action these communications IAW their QCP and any relevant support package SLAs associated with the JWCC users' identified TO. This PoC shall be available 24 hours a day, 7 days a week, 365 days a year, worldwide without any charges or expense to the Government. The modalities of contact shall include, at a minimum, voice (telephone), web-access (i.e. Contractor's Portal), and e-mail. The e-mail response timeline is within one hour of receipt and a response within five minutes of opening the e-mail. This PoC shall be available for all classification levels and ILs such that JWCC users can communicate the issue at the classification level they are currently operating at.
- 5.1.6.9 TE Device Loss, Destruction, or Inoperability. Post award, the Contractor shall report on the number of TE Devices that have been lost, destroyed, or rendered inoperable for each device and circumstance and the total for each circumstance. This information shall be reported in the CMPR (CDRL A001) at the JWCC Program level and reported monthly at the TO level.

5.2 Activities to Assess and Authorize Contractor's Cloud Infrastructure and Offerings

- 5.2.1 The Contractor shall conduct any activities necessary to receive DoD authorization for all XaaS and TE Offerings at each classification level and IL, for inclusion on the JWCC Catalog.
- 5.2.2 The Contractor shall maintain any authorization achieved for the duration of the JWCC Contract, and any TO awarded thereunder, to include conducting continuous audit assessments and, as needed, management reviews as requested by the JWCC KO or AO.
- 5.2.3 The Contractor shall prepare and submit a sufficiently complete Security Authorization Package (CDRL A009) to demonstrate compliance with all applicable requirements in C3PO, including all invoked references and their requirements.

5.3 Multi-Cloud Solution Technical Exchange Meetings (TEMs)

- 5.3.1 The Contractor shall participate in multi-cloud solution TEMs (including interoperability discussions) with other Federal and DoD contractors, including CSPs, with the goal of exploring novel solutions to optimize and streamline multi-vendor solutions and approaches for the benefit of the DoD, at the TO level. The TEMs will be convened as directed by the TO COR.

5.4 System and Organization Control (SOC 1) Type II Reporting

- 5.4.1 The Contractor shall provide a SOC Audit Report (CDRL A014) in accordance with the memorandum, “System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers,” dated May 2, 2019.

5.5 JWCC Timeline and Technical Requirements

The Contractor shall provide XaaS for Government consumption at all classification levels and ILs, within the JWCC Catalog (Attachment J-4), discernable by classification level and IL. The requirements in this section are a minimum capability, condition, or attribute of JWCC. All requirements within the PWS are subject to the timelines below and commensurate with their classification level, unless otherwise specified.

- 5.5.1 Timeline. Delivery of XaaS, including TE Offerings, will follow the timelines as listed below, unless otherwise specified.
 - 5.5.1.1 Roadmap/Integrated Master Timeline (CDRL A019). The Contractor shall provide a roadmap and integrated master timeline, or a combined artifact (hereafter referred to as, “Roadmap/Integrated Master Timeline”) that has each information set clearly discernible within the single artifact, that contain sufficient detail documenting how and when JWCC requirements will be met. The Roadmap/Integrated Master Timeline shall include indicators for every current and future Offering to track successful or unsuccessful outcomes presented in the Roadmap/Integrated Master Timeline for delivery and operability.
 - 5.5.1.2 Unclassified Timeline. The Contractor shall provide its UNCLASSIFIED Offerings at ILs 2, 4, and 5 immediately upon JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as UNCLASSIFIED Offerings, including UNCLASSIFIED TE Offerings. No later than the JWCC Contract award date, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, and submit Security Authorization Package(s) (CDRL A009).
 - 5.5.1.3 Classified Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the SECRET (IL 6) level, within 60 days after JWCC Contract award, such that DoD will have

the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as SECRET JWCC Offerings, including SECRET TE Offerings. Within 60 days after JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, and submit Security Authorization Package(s) (CDRL A009).

- 5.5.1.4 Classified Top Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the TOP SECRET (including (TS/SCI)) level, within 180 days after JWCC Contract award, such that DoD will have the ability to deploy and use (immediately upon Provisional aAuthorization) these Offerings as TS JWCC Offerings, including TE Offerings (TS and TS/SCI). Within 180 days after JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization for all TS JWCC Offerings. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, IC Directive (ICD) 503 (TS and TS/SCI), and submit Security Authorization Package(s) (CDRL A009).
- 5.5.1.5 Special Access Programs (SAP) Timeline. The Contractor shall support securely hosting SAP workloads, such that the DoD will have the ability to accomplish SAP missions using Contractor-provided JWCC Offerings IAW DoDD 5205.07, DoDM 5200.01, and the Joint Special Access Program Implementation Guide (JSIG). These JWCC Offerings shall be delivered consistently with the timelines for UNCLASSIFIED, SECRET, and TOP SECRET with documentation and evidence demonstrating compliance with SAP controls. The Contractor shall provide any additional documentation and artifacts as required by the corresponding SAP AO, per SAP workload, and submit Security Authorization Package(s) (CDRL A009).
- 5.5.1.6 Cross-Domain Solution (CDS) Timeline. The CDSs shall meet the DoD's requirements as described in section 5.5.8.2. The Contractor shall provide CDSs for the Management Plane in conjunction with the associated CLASSIFIED Infrastructure and JWCC Offerings, on or before the delivery of that CLASSIFIED Infrastructure and JWCC Offerings. The CDSs for the Production Plane shall be provided to the DoD within 180 days after the delivery of the associated CLASSIFIED infrastructure and JWCC Offerings. All provided CDSs shall be authorized for use by the DoD Information Security Risk Management Committee (DoD ISMRC). For any CDS that is not presently authorized, the Contractor shall provide all documentation and artifacts required for CDS authorization to the DoD ISMRC in conjunction with the delivery of the associated CDS, and submit Security Authorization Package(s) (CDRL A009).
- 5.5.1.7 Advisory and Assistance Services. The Contractor shall provide advisory and assistance services, as part of its Cloud Support Package, available at all classification levels and ILs IAW the service delivery timelines listed above, in order for JWCC users to acquire advisory and assistance services from the Contractor to support use of JWCC Offerings. The

Contractor-provided advisory and assistance services shall meet DoD's requirements as outlined in section 5.5.11.

- 5.5.2 Available and Resilient Services. The Contractor shall provide Highly Available, resilient CSOs that are reliable, durable, and able to continue operating despite catastrophic failure of portions of the infrastructure. Infrastructure used in the performance of CSOs under JWCC shall be capable of supporting globally dispersed users at all classification levels, including DDIL environments, and Closed-Loop Networks. In order to provide the resiliency and availability required by JWCC users, there must be no fewer than three physical Data Center locations with the ability to operate independently, each including the ability for JWCC users to deploy and manage CSOs at its respective classification level and IL. At least two of the Data Centers must be geographically dispersed by at least 400 miles, utilizing separate power grids, and within the Customs Territory of the United States, as defined in FAR 2.101. UNCLASSIFIED and CLASSIFIED (both SECRET and TOP SECRET) Data Centers may be co-located, as long as the CLASSIFIED Data Center meets FCL requirements IAW C3PO and Attachment J-3: JWCC DD254.
- 5.5.2.1 The Contractor shall provide dynamic scalability and resiliency through industry standard mechanisms and activities to ensure the DoD has the ability to maintain continuous operations.
- 5.5.2.2 The Contractor shall provide the ability for JWCC users to create system configurations, both manually (i.e. via Contractor Portal (UI)) and through APIs, to provide automated redundancy of storage, networking, and computing systems in the case of catastrophic Data Center loss or loss of CSOs.
- 5.5.2.3 The Contractor shall provide CSOs that are Highly Available and resilient. Accordingly, the Contractor's minimum Data Center capabilities are as follows:
 - 5.5.2.3.1 Every Data Center shall be capable of automated replication and failover of CSO(s) within each respective classification level and IL inclusive of the ability to provision, configure, and manage services, such that the DoD is provided Data Center agnostic operations.
 - 5.5.2.3.2 The Contractor shall, at time of award, provide no fewer than two physical Data Centers providing UNCLASSIFIED CSOs within the Customs Territory of the United States, as defined in FAR 2.101.
 - 5.5.2.3.3 The Contractor shall, upon delivery of SECRET CSOs, provide no fewer than two physical Data Centers providing SECRET CSOs within the Customs Territory of the United States, as defined in FAR 2.101.
 - 5.5.2.3.4 The Contractor shall, upon delivery of TS CSOs, provide no fewer than two physical Data Centers providing TS CSOs within the Customs Territory of the United States, as defined in FAR 2.101.

- 5.5.2.3.5 The Contractor shall, no later than 18 months after contract award, provide no fewer than three physical Data Centers providing CSOs at each classification levels and ILs. At least two of these three physical Data Centers shall be geographically dispersed by a minimum of 400 miles, by radial measurement, utilizing separate power grids as defined by the Office of Electricity within the U.S. Department of Energy, and within the Customs Territory of the U.S., as defined in FAR 2.101.
- 5.5.2.3.6 The physical Data Centers at all classification levels and ILs shall strictly comply with all applicable C3PO requirements.
- 5.5.2.4 The Contractor shall provide, at each classification level and IL, automatic monitoring of resource utilization and events (to include failures and degradation of service) via web interface and documented APIs that are intuitive and easy to use.
- 5.5.3 Globally Accessible. The Contractor shall provide CSOs that are securely accessible worldwide via the Contractor's Portal (UI), at all classification levels and ILs. The CSOs shall provide assured access and enable interoperability between Virtual Enclaves containing applications and data.
- 5.5.3.1 The Contractor shall have Points of Presence on all continents, with the exception of Antarctica, providing a total bandwidth capacity of at least 40 Gigabits per second, using redundant links, to peer with the DoD on each continent. If the DoD adds new locations, the Contractor shall peer with the DoD within 12 months of notification such that the latency between the Contractor's and the DoD's locations is less than 8 milliseconds. The Contractor shall provide documentation that validates the transmission speeds, latency, and bandwidth at each location.
- 5.5.4 Centralized Management and Distributed Control. The Contractor shall permit the DoD to exert necessary oversight and management of CSOs. This oversight and management includes, but is not limited to: the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process. In order to exercise centralized management, the Contractor shall have a mechanism for activating and deactivating any CSO for JWCC workspaces. The Contractor shall provide a mechanism to provision CSOs based on standardized, templated configurations and security policies, as well as a "user friendly" mechanism to deprovision any combination of CSOs (e.g. one, multiple, or all). The Contractor shall also provide as part of its solution object and resource access control management, including data and resource tagging for billing tracking, access control, and technical policy management. The Contractor shall facilitate the automation of central management and distributed control. The Contractor shall provide an actively maintained, versioned, and documented API providing the ability to perform any operation supported by the Contractor's Portal (UI).

- 5.5.4.1 The Contractor shall provide the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process to give the DoD the ability to enforce its policies and security compliance for the JWCC Contract workloads.
- 5.5.4.2 The Contractor shall provide the ability to enable and disable services and restrict parameters within service configurations via both the Contractor's Portal (UI) and API, in a manner that is easy to use such that the JWCC COR and administrative JWCC users within the DoD can properly control service delivery to the greater JWCC user community. This ability to restrict services shall allow for hierarchical subordinated supplemental constraints.
- 5.5.4.3 The Contractor shall provide object and resource management capabilities, including data and resource tagging for billing tracking, access control, and technical policy management in order for the DoD to properly administer the JWCC Contract.
- 5.5.4.4 The Contractor shall provide an API that supports encryption and authentication as defined in C3PO for all JWCC users and sessions, for each XaaS at all classification levels and ILs. The API shall, at a minimum, be capable of the following:
 - 5.5.4.4.1 IAM controls, including account creation and management in support of the JWCC Contract, token-based and time-limited federated authentication, role-based access control configuration, and specific account permissions.
 - 5.5.4.4.2 Provisioning and management (i.e. IaaS) of network configuration, compute instances, data and object storage including database management systems, and tools for scaling systems (e.g. Application Server load balancing).
 - 5.5.4.4.3 Storage object lifecycle management (e.g. moving data from online to nearline after a set time period).
 - 5.5.4.4.4 Reading usage data and alerts for compute, storage, and network utilization (e.g. resource/performance monitoring and utilization).
 - 5.5.4.4.5 Reading accrual, historical billing, and pricing data specified under the entire JWCC Contract to include data for: CSOs, Cloud Support Packages, and workspaces.
 - 5.5.4.4.6 Setting billing and usage thresholds and adding automated notifications to workspace owners and the TO COR as well as a capability to configure the discontinuation of service upon the billing and usage threshold breach.
 - 5.5.4.4.7 Accessibility to all JWCC users provided they have the proper access control authorization.
- 5.5.4.5 The Contractor's APIs, at all classification levels and ILs, shall be actively maintained, versioned, documented, and adhere to industry best practices for modern standards and

protocols. API documentation shall contain information on: how to establish a connection, support protocols, security requirements, and capabilities available.

- 5.5.4.5.1 The Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs, of any change to API capabilities impacting backwards compatibility at least 30 days prior to the change being put into production. Alternately, if the change is to address a critical vulnerability, as designated by the Critical Vulnerability Scoring System, the Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs within 24 hours of the change. Additionally, the Contractor shall make available this same information to all DoD personnel and other authorized JWCC users.
- 5.5.4.5.2 The Contractor shall provide full API documentation online (to include examples of code). Full API documentation shall be readily discoverable within three clicks from the Contractor's Portal(s) (UI) landing page. API documentation shall also be available on TE Devices operating in DDIL environments.
- 5.5.4.5.3 The Contractor API shall provide the ability to perform any command supported by the Contractor's Portal (UI).
- 5.5.4.6 The Contractor shall provide a fully compliant implementation of the ATAT Multi-Cloud Provisioning API (Attachment J-11) at each classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for test workloads within 15 days of providing JWCC Offerings at the associated classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for production workloads within 30 days of providing JWCC Offerings at the associated classification level and IL. The Contractor implementation shall be pursuant to Attachment J-11: ATAT Multi-Cloud Provisioning API, to enable ATAT to execute calls to the API resulting in standardized mechanisms for:
 - a. Creation & management of access credentials for accounts and environments in which CSOs can be provisioned.
 - b. Creation and management of portfolios which manage groups of accounts and environments. The deadline by which the Government expects the portfolio provisioning process to be complete is dictated within the ATAT Multi-Cloud Provisioning API (Attachment J-11).
 - c. Creation of the necessary account for the Contractor's Portal(s) (UI).
 - d. Obtaining actual and projected costs per CLIN, environment, workloads, and portfolio.
 - e. Setting billing limits with notifications on CLINs, environments, workloads, and portfolios.

- 5.5.4.7 The Contractor shall update its ATAT Multi-Cloud Provisioning API implementations to the latest version of the ATAT Multi-Cloud Provisioning API definition within 30 days of Government notification for general updates, and within seven days for security updates. **An extension to these timelines may be granted by the KO on a case by case basis.**
- 5.5.4.8 The Contractor's implementation of the ATAT Multi-Cloud Provisioning API shall provide services comparable to the Contractor's other APIs in terms of API service delivery performance.
- 5.5.4.9 The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government has the ability to control any CSO for a subset of the JWCC users or grouping of JWCC users based on individual AO's risk tolerance(s).
- 5.5.4.10 The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government can activate or deactivate any CSO for all of the JWCC users based on DoD Authorization status or cybersecurity needs.
- 5.5.4.11 The Contractor shall provide an IaC CSO, which allows for the deployment and provisioning of one or more other CSOs. This IaC CSO will use pre-made standardized configurations and allow for customizable configurations. This IaC CSO shall also include a simple mechanism to deprovision any and all CSOs it deployed or provisioned.
- 5.5.4.12 The Contractor shall not bundle any JWCC Offerings in a manner that restricts a JWCC user's ability to acquire individual JWCC Offerings. Any bundled JWCC Offerings shall also be available as discrete JWCC Offerings.
- 5.5.4.13 The Contractor shall not require any third-party services that require separate billing, separate licensing, or a combination thereof in order to meet the JWCC requirements or minimum requirements for using any JWCC CSO. Any third-party services that are fully integrated with the Contractor, hosted on the Contractor's infrastructure, and directly supported by, billed through, and licensed by the Contractor are not subject to this requirement.
- 5.5.4.14 The Contractor shall provide prompt notification and follow-up reporting on all service incidents, outages, and other problems (hereafter collectively referred to as, "Service Incident Events") impacting JWCC users or cloud operations. The following minimum requirements apply to all environments, including network and TE Devices:
- 5.5.4.14.1 The Contractor shall establish and utilize Service Incident Event management processes, as well as support accessibility and escalation processes, such that the Contractor is able to prioritize and manage response reactions while keeping users informed about Service Incident Event status, remediation schedule, and overall priority amongst all other current Service Incident Events.
- 5.5.4.14.2 The Contractor shall notify the impacted JWCC users, the JWCC COR, and TO CORs once a Service Incident Event has been detected or discovered. The Contractor shall notify the users,

via electronic means, including severity level, for each Service Incident Event. Service Incident Event notifications shall be made IAW the SLA.

- 5.5.4.14.3 The Contractor shall provide updates on Service Incident Event reports to include the impacted JWCC users, the JWCC COR, and TO CORs. The updates shall be provided at intervals IAW the SLO with the SLA, until the Service Incident Event is completely resolved. Updates shall include supplemental Service Incident Event information to aid in understanding the Service Incident Event's scope, severity, and resolution progress, clearly identifying any outage(s) or other significant problems.
- 5.5.4.14.4 The Contractor shall issue a Service Incident Event report to the impacted JWCC users, the JWCC COR, and TO COR when CSOs functionality or cloud operations performance are impacted. The report shall contain, at minimum, a description of the nature of the Service Incident Event, an impact scope statement, the severity level, and the Mean Time to Resolve estimate.
- 5.5.4.14.5 The Contractor's maintenance activities shall not impact JWCC operations.
- 5.5.4.14.6 The Contractor shall provide the JWCC KO and JWCC COR with a detailed after-action report on all Service Incident Events within seven days of the Service Incident Event to allow the Government to understand the Service Incident Event's impact and determine appropriate follow-on actions.
- 5.5.4.14.7 The Contractor shall securely provide to the Government, human and machine readable cloud service status and Service Incident Event information for all JWCC Offerings.
- 5.5.4.14.8 For disconnected TE Devices, the Contractor shall ensure notification of TE Device specific service outages are provided to any local users at the time of the outage incident and queued for synchronization to cloud services upon re-connection, allowing for centralized reporting and resolution tracking.
- 5.5.4.15 The Contractor shall make available to the Government, standard and easy-to-interpret logs that are both human and machine readable. The Contractor shall ensure logs comply with C3PO and any other Regulatory or Statutory reporting compliance mandates. Such logs shall be generated and available using, at a minimum, either XML or JSON formats, and shall use a structured and verifiable schema. The Contractor shall make available any necessary tools required for log file and schema verification.
- 5.5.4.15.1 To support DoD's Defensive Cyber Operations, the Contractor shall provide access to all logs, related to JWCC, that are required for the Contractor's DoD authorizations which provide an audit trail of all activities and actions (e.g., "Scenarios," as defined in C3PO) as required under the CC SRG and DoD CIO Memorandum, Department of Defense Cybersecurity Activities Performed for CSO. To provide assurance of the actions of personnel assigned to or supporting an approved Oversight team, as defined in C3PO, for UNCLASSIFIED ILs, the Contractor shall explicitly identify (e.g. tag or separate) logs for all

actions, whether direct or indirect, by Contractor personnel working under or as part of an approved oversight team, as defined in C3PO. There shall be no data use charges or transiting charges for accessing the logs stored in the consolidated log location(s).

5.5.4.15.2 The Contractor shall provide access to the logs stored in the consolidated log location(s) through a User Interface (UI) and a secure API at each classification level and IL. The Contractor shall participate in collaborative analysis with the DoD, as appropriate. UI and API documentation regarding the logs and associated features shall be accessible from the Contractor's Portal (UI), at each classification level and IL, and include sample code.

5.5.4.16 Financial Analytical Reporting. The Contractor shall provide a comprehensive financial analytical reporting capability at each classification level and IL, capable of providing current and historical data for all one-time and continuing operational costs. Available information shall include all discrete items (smallest JWCC Offering purchasable from the JWCC Catalog) with an ability to aggregate items, using selected filters, across the entire JWCC user period of interest. The reporting capability shall provide users a financial representation of how costs were accrued over the period of interest. Additionally, the reporting capability shall support a projection mode where, based on current behavior bound by a time period, an estimated cost projection can be computed for a future specified period of time.

5.5.4.16.1 The Contractor-provided financial analytical reporting capability shall include the ability to support JWCC user defined queries and interfaces of the financial data and support the following capabilities:

5.5.4.16.1.1 Direct requester UI that allows for JWCC users to directly input a query and receive commensurate results/outputs.

5.5.4.16.1.2 Scripting capability that allows for repeatable periodic submission, based on a requester-managed file, where the results are delivered to a specified storage location.

5.5.4.16.1.3 An API for automated system-to-system interchange to enable query-response to execute in a dynamic and on-demand, non-human interacted method.

5.5.4.16.1.4 An ability to construct a dashboard from multiple queries at each classification level and IL, such that a JWCC user can view a complete financial picture constructed from multiple queries.

5.5.4.16.1.5 The ability to save and share queries and load query results to dashboards. Once a query is saved to the dashboard, there shall also be an option for an authorized user to read, modify, and delete the query. This ability shall enable users to access, share, and execute a saved query without entering any of the query content and produce routine reports for an overall picture of financial data.

5.5.4.16.1.6 The ability to display a history of all query activity.

- 5.5.4.16.1.7 The ability to support reporting to multiple presentation modes (e.g. files, screen displays, etc.) allowing users to indicate one or more output methods for a generated report. At a minimum, this shall include a user accessible dashboard and the file types PDF and CSV. PDF and CSV file types shall be natively available as a presentation mode regardless of the JWCC user's technology (e.g. modern web browser).
- 5.5.4.16.1.8 The query capability shall support discrete reporting down to the smallest unit purchases and aggregate all included costs to present the overall financial picture to the user. This provides users the ability to understand costs down to the smallest units possible.
- 5.5.4.16.1.9 The query capability shall support continuous cost accrual reporting to give the ability to report total spend for a given period of time, enabling users to project future budget needs.
- 5.5.4.16.1.10 The query capability shall support aggregation of collected items that are grouped using tags. This shall allow users to group information based on specific groupings of information using user-supplied tags.
- 5.5.4.16.2 The Contractor shall provide a spend threshold capability to support warning thresholds at each classification level and IL. The spend threshold capability shall support establishment of threshold values by either the Contractor or the Government. The spend threshold capability shall provide a notification alert sent to a specified recipient list, such that Government users are "warned" of approaching spend threshold based on specific user needs.
- 5.5.4.16.2.1 The spend threshold capability shall allow each user to set specific threshold trigger values for which the spend threshold capability will execute a specified action, such that each user has the flexibility to specify multiple warning notifications based on unique independent threshold trigger values.
- 5.5.4.16.2.2 The spend threshold capability shall include an optional suspension mode, such that the Government avoids Anti-Deficiency Act violations by incurring obligations that are not authorized. If the threshold is achieved, the system will suspend, using a defined process, any additional purchases in a managed manner - both one-time and continuing operational consumption. However, in no case shall the Contractor delete any stored information, including both volatile and non-volatile memory.
- 5.5.4.16.2.3 The spend threshold capability shall support reinstatement of a suspended CSO such that the CSO can be restored, from the point of suspension, as previously configured.
- 5.5.4.16.3 The Contractor shall provide the capability to support time-based billing information at each classification level and IL, such that a user can calculate total charges for a specified period of time in support of auditing and budgeting activities.
- 5.5.4.16.4 The Contractor shall provide the capability for JWCC users to plan and estimate one-time and continuing operational costs based on a specified notional resource configuration inputs for a

projected operational scenario such that a JWCC user can estimate the projected total cost for a given PoP.

- 5.5.4.16.5 The Contractor shall provide the capability to report balances for remaining funds on accounts, such that users have the ability to track burn rate. This capability shall also project a balance exhaustion date based on consumption activity.
- 5.5.4.16.6 The Contractor shall provide the capability, at each classification level and IL, to support financial reporting based on logical grouping of charges. Groupings shall include, but are not limited to:
- a. Reporting based on user/account, organizational structure (i.e. Enterprise, Department, Office, Team), or a combination thereof to determine cloud spend by user/account organizational structure, or a combination thereof.
 - b. Reporting based on type of services consumed to determine spending based on type of services consumed (e.g. storage, compute, data transfer, security).
 - c. Reporting based on cost to determine services' impacts to spend rate.

5.5.4.17 The Contractor shall provide processes and rulesets that enable the Government, in its utilization of services under the JWCC Contract, to comply with the Freedom of Information Act (FOIA), the Federal Records Act, the DoD Records Management Program, Disposal of Records, Executive Order (EO) 12333, EO 13587, the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), and National Archives Records Administration (NARA) regulations.

5.5.4.18 The Contractor shall be capable of exporting security control assessment information using the NIST Open Security Controls Assessment Language (OSCAL) for JWCC Offerings to enable rapid authorization and accreditation of cloud services.

Additionally, the Contractor shall provide Independent Verification and Validation of its OSCAL exports quarterly and 60 days after major OSCAL version release.

5.5.5 Ease of Use: The Contractor must provide Self-Service capabilities enabling rapid development and deployment of new applications and advanced capabilities, including services from the JWCC Marketplace, as defined above. Additionally, the Contractor must support the portability of JWCC data and applications both out of and into the cloud. The Contractor shall provide a Portability Plan (CDRL A006) as detailed in sub-section 5.5.5.3.

5.5.5.1 The Contractor shall provide the Government the ability to rapidly and securely provision/deploy First-Party CSOs and Third-Party CSOs via the Contractor-provided JWCC Marketplace, as defined below, with baseline template configurations, onto JWCC infrastructure at all classification levels and ILs. Third-

Party CSOs that are incapable of being deployed, used, or authorized on the Contractor's JWCC infrastructure are outside the scope of this contract.

- 5.5.5.1.1 The Contractor-provided JWCC Marketplace shall support the ability for JWCC users to deploy the first-party CSOs and third-party CSOs listed on the JWCC Catalog. All Commercial Offerings shall undergo accreditation and authorization processes appropriate for their control markings (e.g. classification level and IL, including SAP, SCI, and others as designated) before the Contractor adds them to the JWCC Catalog and makes them available for JWCC users to fulfill orders, provision, or deploy. Commercial Offerings that are not subject to the CC SRG, DoD, or IC standards must comply with Government-approved Contractor security processes and standards (CDRL A016) before the Contractor adds them to the JWCC Catalog and makes them available on the JWCC Marketplace. The Contractor shall make all security information and process outputs available for Government audit and review.
- 5.5.5.1.2 The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support centralized/integrated billing. The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support bring your own license (BYOL), where applicable (e.g., where additional licensing is required).
- 5.5.5.1.3 The Contractor shall not apply additional cost to any Third-Party Marketplace Offering. This makes all Third-Party CSOs price-free from the Contractor, and all pricing shall be derived from the third-party that is providing the Offering in the third-party marketplace. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO. All Third-Party CSOs that are available in the JWCC Marketplace shall be offered price-free and BYOL basis as appropriate, excluding the cost of IaaS resources. These JWCC Offerings shall be made available, at all classification levels and ILs, IAW PWS section 5.5.1 and 5.5.6 and their subsections, except as approved by the JWCC KO.
- 5.5.5.1.3.1 For Third-Party CSOs available on a price-free or on a BYOL basis, the Contractor shall not impose additional license terms or conditions on the Government. The Government shall be solely responsible for negotiating the Terms and Conditions of the licenses for any Third-Party CSOs available on a price-free or on a BYOL basis that the Government has not previously negotiated Terms and Conditions under a separate contracting vehicle.
- 5.5.5.1.4 The Contractor shall ensure all Third-Party CSOs that are available in the JWCC Marketplace support centralized/integrated billing with the Contractor.
- 5.5.5.1.5 JWCC users' ability to order any discrete JWCC Offering shall be capable of being enabled or disabled at the IDIQ, TO, Cloud Environment, workspace, and JWCC user levels.
- 5.5.5.1.6 The Contractor's JWCC Marketplace shall be available at all classification levels and ILs IAW PWS section 5.5.1 and subsections, and new and modified Offerings shall be populated

within 24 hours of completion of JWCC Catalog Modification process (Section G11). Access to the TS Marketplace shall be restricted to prevent fulfilling orders, provisioning, deploying, cloud operations, schedule non-provisionable or deployable offerings (e.g. Cloud Support Packages) until directed by the JWCC KO.

- 5.5.5.2 The Contractor shall provide, at each classification level and IL, a Calculator reflecting contractually accurate price modeling and projection for any single JWCC Offering, or any combination of JWCC Offerings, at each classification level and IL, to enable authenticated DoD and JWCC users to properly estimate forecasted cloud spending for budgetary planning.
 - 5.5.5.2.1 The Contractor's Calculator shall present all viable recommendations for available consumption-based pricing and subscription models (e.g. for reserved resources), including any applicable discounts.
 - 5.5.5.2.2 The Contractor's Calculator shall provide the ability to compute and present projections to support users' long-term (in excess of 12 months) planning needs. The Contractor's Calculator shall provide users the ability to select time frames (e.g. month, quarter, year), as well as allow for custom time frames (e.g. Fiscal Year (FY) 2022 October 22 to FY 2024 January 15), to allow for accurate long-term budgeting.
 - 5.5.5.2.3 Estimates developed using the Contractor's Calculator shall be made available in various formats, including, but not limited to, on screen, an image report (e.g. PDF document), and exportable/downloadable in a machine readable format that clearly breaks down the pricing by line item for further analytical processing, including by other tools used for analysis and comparison purposes.
 - 5.5.5.2.4 The Contractor's Calculator shall be separately available at each classification level. The Contractor's Calculator shall use and be consistent with the JWCC Contract pricing and the JWCC Catalog, based on the pricing and availability of all JWCC Offerings to allow for filtering and selecting any single JWCC Offering or any combination of JWCC Offerings at any classification level and IL for estimation. The Contractor's Calculator shall default JWCC Offerings to the native classification level and IL where the Calculator is used. The Contractor's Calculator shall be behaviorally and visually consistent at each classification level and IL, such that it provides a single "look and feel" at each classification level and IL (i.e., maintains Commercial Parity).
- 5.5.5.3 The JWCC Contract will require information (data, files, and other forms of information) to be transferred both out of the Contractor's Cloud Environment to another environment (cloud or otherwise) of the Government's choosing and into the Contractor's JWCC Cloud Environment from another environment (cloud or otherwise) of the Government's choosing. In accordance with CDRL A006, the Contractor shall provide the Portability Plan to the Government when it is specified in a TO. The Portability Plan shall address the following information in the below subsections as specified in individual TOs.

- 5.5.5.3.1 The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all, or some, of a JWCC user's data from Online, Nearline, and Offline Storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a JWCC code repository, and network configurations. This shall allow the Government to move information (data and files) from the Contractor's JWCC Cloud Environment to another environment (cloud or otherwise) of the Government's choosing.
- 5.5.5.3.2 The Portability Plan shall include an explanation of how the Contractor will achieve complete purging of all, or some, information as specified by Government direction, which may indicate all, some, or specific user, environment or workspace assets. The Portability Plan shall also include a description for how the Contractor shall prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Contractor's JWCC infrastructure pursuant to the CC SRG and C3PO.
- 5.5.5.3.3 The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to import all, or some, of a JWCC user's data from a user specified location (e.g. online, nearline, and offline storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a code repository, network configurations, and on premises implementations) to the Contractor's JWCC cloud. This shall allow the Government to move information (data and files) from their existing environment (cloud or otherwise) to the Contractor's JWCC cloud.
- 5.5.6 Commercial Parity.
- 5.5.6.1 The Contractor shall ensure the provisioning of each JWCC Offering at each classification level and IL is equal to or faster than the average time computed daily for the provisioning of its equivalent Commercial Offering. The Contractor shall make available performance metrics for each Commercial Offering at each classification level and IL such that the Government can validate provisioning performance for each JWCC Offering (e.g. provisioning a new workspace, user, or service JWCC Offering, or deploying such JWCC Offerings within JWCC) as part of the Contract Monthly Progress Report (CDRL A001).
- 5.5.6.2 The Contractor shall provide generational replacement and upgrading of all software (inclusive of firmware) and hardware (compute, memory, storage, and networking), at all classification levels and ILs, such that the Contractor's JWCC Offerings are on par with the Contractor's equivalent Commercial Offerings. The Contractor shall provide a Lifecycle Management Plan (CDRL A018) which demonstrates how it will meet this requirement.
- 5.5.6.3 The Contractor shall achieve Commercial Parity, as soon as possible, but no later than 18 months after JWCC Contract award. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.

- 5.5.6.4 Each Contractor Commercial Offering that becomes available for licensing, purchase, or consumption following the JWCC Contract award, shall be submitted to the Government for authorization, at all classification levels and ILs, according to the following procedures and timelines:
- a. For CSOs requiring FedRAMP approval:
 - The Contractor must submit the CSO to the Joint Authorization Board (JAB) for authorization within 30 days of the CSO becoming Commercially Available.
 - The Contractor must submit the CSO to DISA for authorization within 30 days of FedRAMP approval.
 - b. For CSOs requiring IC approval:
 - The Contractor must submit the CSO to the cognizant security authority for authorization within 30 days of the CSO becoming Commercially Available.

Each Commercial Offering shall be added to the JWCC Catalog IAW G11 at the classification level and IL for which it is authorized. If an exception is required the Exception Request must be processed prior to adding it to or modifying it on JWCC Catalog. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.

- 5.5.6.5 For any of the JWCC Offerings, across each classification level and IL, the same API calls and Contractor Portal (UI) actions shall result in the same expected behavior, except when restrictions due to classification level or IL prohibit Commercial Parity. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.
- 5.5.6.6 The Contractor shall provide Commercial Parity of CSOs and specialized hardware availability between Data Centers at each classification level and IL such that workloads are able to scale and migrate horizontally within a classification level and IL. In addition, the Contractor shall ensure that JWCC users have the ability to configure JWCC workloads for “high availability” as defined in NIST SP 800-113. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.
- 5.5.6.7 All JWCC Offerings shall be at or below the Contractor’s Commercial Catalog pricing.
- 5.5.6.8 This requirement number is reserved for ease of administration.
- 5.5.6.9 Third-Party Marketplace Offerings are not considered Commercial Offerings for the purposes of Commercial Parity and, therefore, need not be identified in JWCC Exception Request (CDRL A024).

- 5.5.7 Modern and Elastic Computing, Storage, and Network Infrastructure. The Contractor must enable self-service automated provisioning of compute, storage, and network infrastructure that is constantly updated -- to include, but not limited to processing architectures, servers, storage options, and platform software -- at scale to meet consumption, rapid development, and deployment in support of mission needs.
- 5.5.7.1 The Contractor shall provide all CSOs, including those that are optimized for specific compute-based activities (e.g. evolving GPU and application specific integrated circuits (ASIC) processing architectures, quantum computing applications, and future evolving computational integrated circuit devices).
- 5.5.7.2 The Contractor shall provide for durable elastic growth for storage capabilities (e.g. Online, Nearline, and Offline Storage options; object, block, and file-based storage; as well as managed database and NoSQL (non-structured query language) services), at the speed of deployment that is commensurate with Commercial Offering deployment speeds. This shall apply to all classification levels and ILs. Any performance tiering options shall be explicitly identified in the Contractor's JWCC Catalog.
- 5.5.7.3 The Contractor shall have more than one queryable storage JWCC Offering that can support data on the order of hundreds of Terabytes, intra-Availability Zones, and inter-Availability Zones. The Contractor shall provide at least one storage JWCC Offering that can perform create, read, update, and delete functions on data on the order of hundreds of Terabytes. Create, read, update, and delete operations at all classification levels and ILs shall be commensurate with the Contractor's Commercial Offerings.
- 5.5.7.4 The Contractor shall provide an API Gateway service that allows JWCC users the ability to develop, deploy, secure, manage, and scale the Government's APIs as needed.
- 5.5.7.5 When an authorized user requests a cloud resource within the Contractor's Portal (UI), or via an API, the response time shall be commensurate with the Contractor's Commercial Offerings.
- 5.5.7.6 The Contractor shall provide the ability to generate individual IaaS compute instances, for which the time required to go from stopped state (e.g. powered off) to receiving and processing user instructions (less any operating system boot time) for any individual IaaS compute instance shall be less than 10 seconds.
- 5.5.8 Fortified Security: The Contractor must provide fortified security capabilities that enable enhanced cyber defenses for strong IAM and security from the application layer through the data layer. Fortified security capability requirements include continuous monitoring and auditing, automated threat identification, resilience and elasticity, encryption at rest and in transit, secure data transfer capabilities, and an operating environment that meets or exceeds DoD INFOSEC requirements. This security shall be tested regularly and include independent DoD testing, review, and audit.

- 5.5.8.1 The Contractor shall provide encryption and Logical Separation for any of the Contractor's CSOs available under the JWCC Contract, IAW C3PO and the following additional requirements:
- 5.5.8.1.1 The Contractor shall ensure that encryption appropriate to the applicable classification level or IL, for data at rest and in transit, is the default setting for all of the Contractor's CSOs available under the JWCC Contract such that the DoD can maintain confidentiality, as defined in the definitions, as the default configuration.
- 5.5.8.1.2 The Contractor shall provide multi-layer encryption for all of the Contractor's CSOs such that content, including any at-rest containers, shall remain encrypted until explicitly invoked via executable, and then once again be encrypted when operational processing is complete. The Contractor shall provide multi-layer encryption to maintain data confidentiality and support dual encryption such that it includes two or more independent layers of encryption. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.
- 5.5.8.1.3 The Contractor shall ensure that all of its CSOs available under the JWCC Contract, at all classification levels and ILs, provide the capability for DoD data to be encrypted at rest, with exclusive DoD control of encryption keys and key management, such that the DoD has the capability to cryptographically erase data, as defined in the definitions. The Contractor shall provide:
- a. JWCC user-managed encryption keys;
 - b. Encryption key management as a service; and
 - c. Support for use of both Contractor-provided and Government-provided Hardware Security Modules (HSMs) (whether in-line, within the Contractor's Cloud Environment, or externally located) for cryptographic operations.
- 5.5.8.2 Cross-Domain Solution. The Contractor shall provide a CDS that provides secure and highly deterministic one-way data transfer capability between the Contractor's logical enclaves and environments within the Contractor's CSOs under the JWCC Contract, to external destinations, and across all classification levels, while limiting any threats. The Contractor shall minimally provide CDSs that supports low to high (from a lower impact/classification level to a higher impact/classification level) for both the Management Plane and production plan and high to low (from a higher impact/classification level to a lower impact/classification level) for the Production Plane, per sections 5.5.8.2.1 through 5.5.8.2.5 of this PWS.
- 5.5.8.2.1 All CDSs provided must be compliant with C3PO and the latest version of Cross-Domain Solution (CDS) Design and Implementation Requirements: 2020 Raise the Bar (RTB) Baseline Release (or current version) and achieve authorization by the DoD ISMRC.
- 5.5.8.2.2 The CDS shall allow specific Government-controlled JWCC role-based accounts to overrule automated security measures to securely transfer information that may be

flagged as malicious. This shall allow the specific Government-controlled JWCC role-based accounts-holders to accept risk as appropriate for flagged data transfers.

- 5.5.8.2.3 The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the management plane to ensure the Contractor can securely migrate security updates to higher classification domains in a timely, consistent, repeatable, and secure manner, and maintain Commercial Parity.
- 5.5.8.2.4 The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the Production Plane to support Government data transfer needs, including Development, Security, and Operations (DevSecOps).
- 5.5.8.2.5 The Contractor shall provide a CDS that supports data transfer from high to low between all classification levels and ILs on the Production Plane to support Government data transfer needs.
- 5.5.8.3 The Contractor shall provide a secure data transfer capability for deterministic (maintaining integrity and predictable), authenticated, and encrypted, data transfers between the Contractor's logical enclaves and environments within its own cloud infrastructure and Offerings, to external destinations, including multi-environment peering gateways, and across all ILs within a classification level, while limiting any threats.
- 5.5.8.4 Authentication, Authorization, and IAM. With respect to authentication, authorization, and IAM the Contractor shall provide the following:
 - 5.5.8.4.1 The Contractor shall provide customizable granularity for role-based, identity-based, attribute-based, access control (R-, I-, ABAC) policy configurations within a workspace, including workspace administration, provisioning of new cloud services, management of existing services, and the ability to assign permissions to Contractor pre-defined and allow for the creation and assignment of JWCC user specified roles.
 - 5.5.8.4.2 The Contractor shall provide non-repudiation and user-identity confirmation providing the ability to securely verify user identity, including Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI), at all classification levels and ILs pursuant to requirements in C3PO, the CC SRG, and the authorization for each of the Contractor's CSOs under the JWCC Contract.
 - 5.5.8.4.3 The Contractor shall provide the ability to generate and issue time-limited, role-based authentication tokens that will allow a JWCC user to assume a set of attributes, roles, or a combination thereof within a specific workspace, the Cloud Environment, or a combination thereof.
 - 5.5.8.4.4 The Contractor's CSOs shall support modern authentication protocols and methods (e.g. Security Assertion Markup Language (SAML), Open Authorization (OAuth), Fast Identity Online (FIDO2)) such that the Government can integrate/use Federated Identity solutions with the Contractor's CSOs under the JWCC Contract at each classification level and IL.

- 5.5.8.5 Automated INFOSEC and Access Control. In conjunction with the requirements established in C3PO, the Contractor shall provide automated tools for INFOSEC and access control with the attributes described below:
 - 5.5.8.5.1 The Contractor shall provide the capability for the Government to audit both the physical location and logical separation, as defined in C3PO, of any CSO and Government data, at each classification level and IL, to ensure compliance with C3PO.
 - 5.5.8.5.2 The Contractor shall provide automated tools for breach identification, notification, and remediation, to support breach and incident response requirements described in C3PO.
 - 5.5.8.5.3 The Contractor shall provide Self-Service and automated tools for handling data spills of CLASSIFIED or other controlled information, at each classification level and IL, to support data spillage activities as described in DoDM 5200.01 and C3PO.
 - 5.5.8.5.4 The Contractor shall provide self-service tools, at each classification level and IL, to allow JWCC users to access data and analysis generated by threat detection systems so that JWCC customers, DoD cybersecurity investigators and auditors, including contractor staff serving in those capacities, can review, assess, protect, and defend their deployed and provisioned CSOs.
 - 5.5.8.5.5 The Contractor shall provide identification and notification of threats to JWCC users and system owners immediately upon discovery, to support incident response tasks as described in C3PO.
- 5.5.9 Advanced Data Analytics. The Contractor shall provide advanced data analytics CSOs, as minimally outlined herein and below, that securely enable data-driven and improved decision making at the strategic level (across security domains) to the TE (within a single security domain). The Contractor shall provide advanced data analytics CSOs that support batch and streaming analytics, predictive analytics, and AI/ML. Advanced data analytics CSOs shall be available at all classification levels and ILs, extensible to the TE, to include DDIL environments and on multiple disparate datasets. Advanced data analytics CSOs shall, at a minimum, be able to import, process, and export streaming and batch data in common data formats.
 - 5.5.9.1 The Contractor shall provide data analytics CSO's (e.g., streaming analytics, predictive analytics, and AI/ML).
 - 5.5.9.1.1 The Contractor shall provide data analytics JWCC Offerings capable of operating at all classifications and ILs, and on TE Devices, such that operators can label data, train and develop models, and use model/algorithm outputs in mission relevant environments with mission relevant data, commensurate with the JWCC timeline (5.5.1, above). Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.

- 5.5.9.1.2 The Contractor's advanced data analytics CSOs shall be capable of operating across multiple datasets in disparate workspaces to allow for information sharing and learning across multiple DoD Components/Agencies.
- 5.5.9.1.3 The Contractor shall provide advanced data analytics CSOs able to fully operate with or without network connectivity and in DDIL environments, such that TE Devices shall be capable of continued data analytics activities (including AI/ML) when network connectivity is contested, congested, or unavailable, commensurate with the JWCC timeline (5.5.1, above).
- 5.5.9.1.4 The Contractor's data analytics JWCC Offerings shall be capable of supporting data import and export in common formats (at minimum these formats shall include CSV, JSON, XML, and streaming data).
- 5.5.10 Tactical Edge. The Contractor shall provide TE Offerings and TE Devices across the range of military operations while balancing portability, capability, and cost. TE Devices shall operate seamlessly across network connectivity levels, including DDIL environments, at all classification levels and ILs IAW C3PO.
- 5.5.10.1 The Contractor shall provide, as a JWCC Offering, a minimum of one form factor of TE Devices that is man-portable and is capable of being carried by an individual(s), mounted to a vehicle, or both, which the Contractor will have certified as meeting MIL-STD-810H (Environmental Engineering Considerations and Laboratory Tests), such that the form factor of TE Devices enables the use of JWCC resources across the range of military operations (e.g. deployable afloat, aloft, ashore, and globally). This form factor of TE Devices shall be authorized to host data at each classification level and IL.
- 5.5.10.2 The Contractor shall provide a modular, rapidly deployable Data Center that can be connected to Government-provided power, connected to Government-provided networking uplinks when available, use Government transportation, and be deployed on U.S. soil, CONUS or OCONUS, or on Government-owned platforms (e.g. aircraft carriers, maritime operations center, airfields, and division headquarters). The deployable Data Center shall be authorized to host data at each classification level and IL and up to all classification levels and ILs following the physical and Logical Separation requirements in C3PO.
- 5.5.10.3 The Contractor's TE Offerings shall function in DDIL environments as if connected, with the only features and functionality missing being those that rely on real time interconnection services. TE Offerings shall include the ability to configure and manage any CSO deployed or provisioned on or to the TE Device, and operate using local resources.
- 5.5.10.4 The Contractor's TE Offerings shall be configurable such that a JWCC user can configure the parameters for synchronization with Contractor-provided services. These parameters shall, at a minimum, include automated or manual, bidirectional or unidirectional synchronization options, the ability to control synchronization priority order, and the ability to throttle use of available bandwidth for synchronization.

- 5.5.10.5 The Contractor shall provide TE Device and component signature specifications for Electromagnetic (EM), acoustic, thermal, and any other device specific emanations in all operational states to enable the Government to control the magnitude of these signatures (TE Device Specifications, CDRL A017).
- 5.5.10.6 The Contractor's TE Offerings shall follow the cybersecurity requirements defined in C3PO.
- 5.5.10.7 The Contractor's TE Offerings shall be capable of both in-band and out-of-band configuration and maintenance for all TE Devices.
- 5.5.10.8 The Contractor's TE Offerings shall support cryptographic key management, IAW Section 5.5.8.1.3 and C3PO, both on and off the TE Device, at the user's discretion.
- 5.5.10.9 The Contractor shall provide delivery of TE Devices to CONUS locations only and allow for the Government to pick up TE Device(s) at a Contractor facility in CONUS. Locations for pickup and any services and fees associated with delivery ~~may shall~~ be separately identified and priced in the JWCC Catalog.
- 5.5.10.10 The Contractor shall submit authorization packages for the first unit of all variations of TE Devices for Authorization at each classification level and IL.
- 5.5.10.11 For each TE Device the Contractor will offer in the JWCC Catalog, the Contractor shall provide to the JWCC PMO a sample of each TE Device per classification level and IL, with the associated authorization package, such that the Government can perform verification and validation of the device(s) prior to official acceptance as part of the JWCC Catalog. Upon completion of testing, the Government will either order the appropriate TE Offering(s) from the JWCC Catalog or return all sample TE Devices from the test.
- 5.5.10.12 When TE Devices are returned to the Contractor, the Contractor shall either dispose of the TE Device IAW the CC SRG and the Attachment J-3: JWCC DD254 or follow the procedures and requirements in C3PO for reuse.
- 5.5.11 Advisory and Assistance Services. The Contractor shall provide advisory and assistance services under the Cloud Support Package CLINs in the JWCC Contract to advise and assist with cloud architecture, usage, optimization, provisioning, and configuration for all JWCC Offerings, including TE Offerings. Cloud Support Packages shall encompass, but not be limited to, advisory and assistance services, help desk services, training, and documentation support. Cloud Support Packages shall be available for all JWCC Offerings at all classification levels and ILs.
- 5.5.11.1 The Contractor shall provide advisory and assistance services that include integration, aggregation, orchestration, secure design, and troubleshooting of JWCC Offerings and can be applied to all classification levels and ILs.

5.5.11.2 The Contractor shall provide training materials and make training available for all of the CSOs on the JWCC Catalog at all classification levels and ILs. Separate training and documentation are required for TE Offerings. The Contractor shall include, at a minimum:

- a. Training materials and training for all CSOs provided on the JWCC Catalog at all classification levels and ILs.
- b. Materials that help users and administrators understand how to successfully provision services and employ best practices for JWCC Offerings. Users and administrators shall be able to retain such materials upon completion of the training (CDRLs A004 and A005).
- c. Separate training and training materials shall be provided for each TE Offering, inclusive of supportability training (e.g. end user maintenance, packaging, handling, storage and transportation, infrastructure requirements), at all classification levels and ILs.
- d. Any training the Contractor provides shall demonstrate, through tabulated results, the relevance, thoroughness, and efficacy of the training using industry standard methods and tools.
- e. All training materials shall be current and the Contractor shall provide updated training materials with the release of new versions of any CSO that is made available to JWCC users.

5.5.11.3 If a Cloud Support Package is constrained by the number of hours available to users, the Contractor shall provide a Self-Service mechanism for users to quickly determine how many hours of the available support package have been consumed.

5.5.11.4 The Contractor shall provide, as part of the JWCC Catalog, separate options for in-person and remote instructor-led training and support services provided by the Contractor in CONUS and OCONUS locations. All training and support services shall be offered at the locations as described in the JWCC Offering or as required by the TO.

5.5.11.5 The Contractor shall provide, as part of the JWCC Catalog, an option for self-paced training.

5.5.11.6 The Contractor shall provide options for equipment repair/replacement and data recovery from TE Device failure or performance degradation, with minimal mission impact, such as the ability to replace failed hardware at the unit level or full TE Device in a manner that is appropriate for the form factor of the device and range of impacted military operations and best effort data recovery.

5.6 **Desired Capabilities**

The capabilities outlined below are interest areas for the Government, which it hopes the commercial industry will drive technology toward meeting, and which may be provided under the JWCC Contract.

5.6.1 Advanced Tactical Edge Capabilities

- 5.6.1.1 The Contractor *may* offer additional man-portable TE Devices that deviate from MIL-STD-810H compliance (e.g. quasi-military grade). If a TE Device that deviates from MIL-STD-810H compliance is offered, the Contractor shall document any deviations in their submission of the Tactical Edge Device Specifications (CDRL A017) deviations from MIL-STD-810H.
- 5.6.1.2 TE capabilities that enhance warfighting advantage. For example, new and emerging capabilities that are deployable to land, sea, subsea, air, space, and mobile devices, at all classification levels and ILs.
- 5.6.1.3 Innovative solutions for overcoming logistical challenges in delivering, maintaining, and returning TE Devices capabilities, or any combination thereof.
- 5.6.1.4 Support for the Internet of Things gateways, for both Contractor-hosted services, TE Devices, and Government-provided assets.
- 5.6.1.5 Advanced analytic or algorithm capabilities (e.g. AI/ML) capabilities that enable creation of models, use of developed models, and continuous learning/improvement at the TE.
- 5.6.1.6 New and emerging TE communication methods (e.g. Fifth Generation (5G), Low Earth Orbit Satellite, Light Fidelity (LiFi), Sonic).

5.6.2 Security

- 5.6.2.1 Advanced automated security capabilities, including, but not limited to, the ability to detect and respond to adversaries through AI.
- 5.6.2.2 Automated detection of data spills.
- 5.6.2.3 Emerging cryptographic capabilities (e.g. homomorphic encryption, quantum encryption).

5.6.3 Additional Cloud Support Packages

- 5.6.3.1 Smaller, more incremental levels of support beyond the Contractor's standard Cloud Support Package JWCC Offerings.
- 5.6.3.2 Specialized training support in various modalities, including, but not limited to, classroom, train-the-trainer, certifications, and advising on training package development.
- 5.6.3.3 Self-paced, online, embedded training (e.g. TE Device training that is self-paced and embedded on the device for use in the field), or a combination thereof.

- 5.6.3.4 Self-sensing context adaptive training that provides corrective guidance and training during system operations.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS (CURRENT EDITIONS)

- 6.1 The Contractor shall abide by all applicable regulations, publications, manuals, and local policies and procedures.
 - 6.1.1 Accelerate Enterprise Cloud Adoption, Deputy Secretary of Defense Memorandum, dated September 13, 2017
 - 6.1.2 Cloud Computing Cybersecurity Plan for Operations, dated October 01, 2021
 - 6.1.3 Cross-Domain Solution Design and Implementation Requirements, 2020 Raise the Bar Baseline Release, National Security Agency, dated December 22, 2020
 - 6.1.4 Defense Information Systems Agency Policy Letter, Unauthorized Connections to Network Devices, dated September 11, 2013
 - 6.1.5 Defense Information Systems Agency Form 786, Statement of Information System Use and Acknowledgement of User Responsibilities – Basic User
 - 6.1.6 Defense Information Systems Agency Instruction 240-110-8, Information Security
 - 6.1.7 Defense Information Systems Agency Instruction 240-110-36, Personnel Security
 - 6.1.8 Defense Information Systems Agency Instruction 240-110-38, Industrial Security
 - 6.1.9 Defense Information Systems Agency Instruction 240-110-43, Insider Threat Program
 - 6.1.10 Defense Information Systems Agency Instruction 630-230-19, Cybersecurity
 - 6.1.11 Department of Defense 5220.22-M, National Industrial Security Program Operating Manual, dated May 18, 2016
 - 6.1.12 Department of Defense Chief Information Officer Memorandum, Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings, dated November 15, 2017
 - 6.1.13 Department of Defense Manual 5105.21, Sensitive Compartmented Information Administrative Security Manual: Administration of Information and Information Systems Security, dated September 14, 2020

- 6.1.14 Department of Defense Manual 5200.01, Volume(s) 1-3 Information Security Program, dated February 24, 2012
- 6.1.15 Department of Defense Manual 5200.02, Procedures for the Department of Defense Personnel Security Program, dated April 3, 2017
- 6.1.16 Department of Defense Manual 5205.07, Special Access Program Security Manual, dated September 20, 2020
- 6.1.17 Department of Defense Manual 5400.07, Freedom of Information Act Program, dated January 25, 2017
- 6.1.18 Department of Defense Instruction 5200.48, Controlled Unclassified Information, dated March 6, 2020
- 6.1.19 Intelligence Community Directive 503, Intelligence Community Information Technology Systems Security Risk Management Certification and Accreditation, dated September 15, 2008
- 6.1.20 Interconnections, Office of Electricity, Department of Energy.
<https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0>
- 6.1.21 Joint Special Access Program Implementation Guide, dated April 11, 2016
- 6.1.22 Joint Requirements Oversight Council Memorandum 135-17, dated December 22, 2017
- 6.1.23 Joint Travel Regulations, dated November 01, 2021
- 6.1.24 Military Standard 810H, Department of Defense Test Method Standard: Environmental Engineering Considerations and Laboratory Tests, dated January 31, 2019
- 6.1.25 National Institute of Standards and Technology SP-800-113, Recommendations of the National Institute of Standards and Technology, dated July 2008
- 6.1.26 National Institute of Standards and Technology SP-800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, dated January 16, 2020
- 6.1.27 System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers, dated May 2, 2019

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING

- 7. **Attachment/Technical Exhibit List:**
- 7.1 Attachment 1/Technical Exhibit 1 – Performance Requirements Summary
- 7.2 Attachment 2/Technical Exhibit 2 – Deliverables Schedule

TECHNICAL EXHIBIT 1

Performance Requirements Summary

The Contractor's service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
1	5	Specific Tasks:	Summary Requirement	N/A
2	5.1	Program Management	Summary Requirement	N/A
3	5.1.1	The Contractor shall provide overarching program management personnel, processes, and tools under CLINs x008, as necessary to manage and oversee all Contractor activities for the duration of their JWCC Contract within cost, schedule, performance, and quality requirements.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	N/A
4	5.1.2	The Contractor shall establish and maintain a formal PMO, which shall coordinate and interface with the JWCC COR and JWCC PMO to ensure the JWCC Contract is being used efficiently, compliant with JWCC requirements, and making use of commercial best practices.	The Government will audit the Contractor's JWCC support organizational structure to assure the critical PoCs for contract success are identified.	N/A
5	5.1.3	The Contractor shall appoint a PM and a DPM empowered to make program and project-level decisions and commit resources necessary to successfully execute courses of action within scope of the JWCC Contract.	The Government will audit the Contractor's proposed JWCC support organizational structure to ascertain if the PM and DPM are clearly identified.	N/A
6	5.1.4	The Contractor's PM support will facilitate the timely authorization of JWCC infrastructure and Offerings to be included on the JWCC Catalog at all classification levels and ILs, and take all necessary steps to ensure successful integration with the DoD's ATAT provisioning tool with the Contractor's management systems for JWCC, as appropriate.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
7	5.1.5	The PM and DPM shall have sufficient expertise and authority to execute the following responsibilities: (a) serve as the official central PoC and interface between the Contractor and the COR; (b) be available as needed for interaction with the JWCC COR, JWCC PMO, and JWCC KO; and (c) monitor and report on contract status (CDRL A001) and compliance with the JWCC Contract requirements.	The Government will assess whether the PM and DPM have the necessary authority to act as the single point of contact for all managerial Contractor engagements with regard to the JWCC Contract.	N/A
8	5.1.6	The contractor shall perform the following requirements and provide the following deliverables. All materials shall be provided error free and presented in a professional manner.	Summary Requirement	N/A
9	5.1.6.1	<p>The Contractor Program Management Plan (CPMP) (CDRL A021) shall include with sufficient detail such that the Government can assess and understand how the Contractor intends to meet all requirements outlined in the PWS.</p> <p>The CPMP demonstrates the Contractor’s approach, timeline, and tools to be used in execution of the Contract. The CPMP should be in both a narrative and graphic format that discusses and displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The CPMP shall be the primary plan and all other plans (e.g. the QCP) required and defined in the PWS will be subordinate to the CPMP. The Contractor shall provide at time of proposal submission the initial CPMP. Once the Government agrees with the CPMP, the finalized copy shall be provided within 10 business days after final Government input(s) are received. The CPMP shall be updated as needed thereafter, but no less than annually.</p> <p>The CPMP shall, at a minimum, include a description of the management and execution approach to include: all information required under administration and execution of the entirety of 5.1.6</p>	The Government will assess the CPMP for sufficiency of addressing each requirement of the contract.	N/A
10	5.1.6.2	The Contract Monthly Progress Report (CDRL A001) is for overall performance under the JWCC Contract and access to all Task Order Monthly Progress Reports (CDRL A012) for PM performance. The Contract Monthly Progress Report shall include, but not be limited to, the following:	The Government will assess the data provided to describe TO execution value and expenditure.	The TO has robust data describing every facet of execution, financial, and management aspects.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
11	5.1.6.2.1	A full accounting of each TO received, the execution status of the TO, total value of the TO, and funds expended to date on the TO.	The Government will assess if the information provides the Department with insight for JWCC utilization and a full comparison with the commercial and governmental utilization to JWCC use.	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.
12	5.1.6.2.2	The report shall include, at a minimum, the JWCC utilization metrics and the percentage as compared to the Contractor's total commercial and non-commercial utilization and capacity. The Contractor should ensure the information in the report is assessed and appropriately marked with portion markings IAW the DoDM 5200.01. These portion markings shall be limited to 5.1.6.2 and its subsections. The report shall be broken out by CSO and CLIN per month, year, and life of the JWCC Contract for the following metrics:	The Government will assess if the information provided is sufficient as required for analysis.	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.
13	5.1.6.2.2.1	Network. Volume of commercial client traffic, in megabytes, for public internet ingress and egress (at the logical Cloud Boundary outside of availability zones, i.e. in and out of the Contractor's controlled infrastructure) per month and aggregated for the duration of the JWCC Contract to date. This measure and metric shall include a discrete breakdown comparison of the following: commercial traffic, JWCC Contract traffic, TO traffic by availability zone and comprehensively, as both raw volume and the Government's equivalent utilization as a percentile comparison.	The Government will assess if the information provided on Network measures is sufficient as required for analysis.	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.
14	5.1.6.2.2.2	Compute. Number of physical (not virtualized) compute (e.g. CPU, GPU, or other processor technology as applicable) cores in use by Application Servers. Application Servers are defined as those physical servers that host the virtualized infrastructure and platform services used by end users (e.g. a server that is hosting JWCC Contract applications is an Application Server, while a network router does not satisfy this definition of Application Server). Additionally, the number of physical compute cores that are available for future use (not currently allocated to an Application Server, nor in use by Application Server) both comprehensively and by Availability Zone.	The Government will assess if the information provided on Compute measures is sufficient as required for analysis.	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.
15	5.1.6.2.2.3	Storage. Data, in megabytes, consumed and available, for each of online, nearline, and offline storage, averaged across the month and aggregated for the life of the JWCC Contract.	The Government will assess if the information provided on Storage measures is sufficient as required for analysis. The Government will assess if units	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			of computation are clearly specified.	
16	5.1.6.2.2.4	Additionally, the report shall identify the base (e.g. base 2 or base 10) for all measured values using bytes.	The Government will assess if units of computation are clearly specified.	N/A
17	5.1.6.2.3	An accurate, clear and precise measure and metric for each performance criteria listed in Technical Exhibit 1, Performance Requirements Summary, of the Attachment J-1: JWCC PWS. This shall include monthly and accrued measures and metrics over the life of the JWCC Contract.	The Government will assess if all performance criteria are accounted for regarding metrics and measures from Technical Exhibit 1.	Real time analytics will present a continuous reading of the JWCC metrics and measures and the comparison to industry and total Government consumption.
18	5.1.6.2.4	Progress of the ability to create and deliver the following CDRLs:	Summary Requirement	N/A
19	5.1.6.2.4.1	A report on usage, by TO, for any GFP (CDRL A015).	The Government will assess if an accurate accounting of GFP per TO is presented.	Real time analytics will present a continuous automated tracking of the JWCC GFP on a per TO basis.
20	5.1.6.2.4.2	A report on ordering, by TO, for any TE Offering and any associated TE Devices (CDRL A012).	The Government will assess if TE offerings tracking is managed at the TO level.	Real time automated tracking for TE offerings at the TO level.
21	5.1.6.2.4.3	A report of any quality defect findings, regardless of severity, resulting from application of the QCP (CDRL A008) processes, including operationally induced failures, and organized by the associated TO against which the finding was discovered.	The Government will assess if the quality management process sufficiently tracks quality deficiency findings to perform corrective action and prevent future occurrence.	Application of events to algorithms to resolve quality deficiency findings.
22	5.1.6.2.4.4	A status of small business allocation of work, by size and category, as required in section 1.5.14 of the JWCC PWS (CDRL A010).	The Government will assess if the portion of Small Business participation is sufficient.	N/A
23	5.1.6.2.4.5	AA status of both the identification of a financial system and the associated TO for System and Organization Control (SOC 1) Type II reporting as required in section 5.4 of the JWCC PWS and SOC Audit Report (CDRL A014).	The Government will assess if the contractor has sufficient insight to identify any financial system that is supported in the JWCC environment that requires a SOC I Type II report.	N/A
24	5.1.6.2.5	Any issues, challenges, problems, risk areas, or requests for JWCC COR support.	The Government will assess the contractors process for managing issues, challenges, problems, risk areas, or requests for the JWCC COR.	A fully automated collaboration environment for remediation and mitigation.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
25	5.1.6.3	The Contractor shall attend and participate in meetings arranged, executed, and facilitated by the Government. The Government will coordinate a kickoff meeting for all Contractors receiving an award within 45 30 calendar days after contract award. The Contractor is responsible for coordinating with the JWCC COR. The kickoff meeting will be conducted in-person with the Contractor's primary staff that will interface with the JWCC PMO and will be held in the National Capital Region. The kickoff meeting will be conducted with all JWCC Contract holders in attendance at the same time. All JWCC Contract holders will be allowed one-on-one breakout sessions, if requested, for presentation of Contractor materials and any specific questions regarding the JWCC Contract.	The Government will assess if the contractor participation and contributions in the meeting is satisfying the goals and objectives of the meeting.	N/A
26	5.1.6.4	The Contractor shall arrange, execute, and facilitate meetings when requested by the JWCC PMO, or as required, in support of the JWCC Contract.	The Government will assess if the contractor is able to fully coordinate all Government requested meetings for the JWCC Contract by the JWCC PMO.	N/A
27	5.1.6.4.1	In-Progress Reviews (IPRs). The Contractor shall arrange, facilitate and execute quarterly IPRs, as well as any additional IPRs at the request of the JWCC KO or JWCC COR. IPRs will be conducted either in-person or virtually at the request of the Government, and the government reserves the right to include virtual attendees for in-person meetings. The Contractor is responsible for providing an agenda, presentation materials, and meeting minutes (CDRL A013) for all IPRs. Minimum content for IPRs shall include, but is not limited to, the following:	The Government will assess if the IPR content provides the Government with sufficient management insight to understand contractor contract performance.	Real time automated tracking dashboard with continuous updates to IPR content.
28	5.1.6.4.1.1	Overall JWCC Contract execution, management and operating status update;	Summary Requirement	N/A
29	5.1.6.4.1.2	Discussion, as necessary, of any upcoming JWCC Catalog changes (as captured in JWCC Catalog with Change Report (CDRL A022)), including addition, modification, deletion or deprecation;	The Government will assess the veracity of contractor catalog modification management.	N/A
30	5.1.6.4.1.3	Specific recommendations to better optimize JWCC Offerings, operations, and deployment based on empirical evidence, with projections for implementation of those recommendations;	The Government will assess if the Contractor is evaluating empirical data to identify optimization opportunities.	Fully automated dashboard identifying where optimization opportunities exist.
31	5.1.6.4.1.4	Recommendation to improve communication between the Contractor and the JWCC COR;	The Government will assess if the Contractor is providing approaches to improve communications between the Contractor and the JWCC COR.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
32	5.1.6.4.1.5	Status of, and any issues regarding, use of and interfacing with ATAT;	The Government will assess if the Contractor is reporting ATAT operational issues consistent with ATAT's operations behavior.	Fully automated dashboard identifying issues in real-time.
33	5.1.6.4.1.6	Identification of JWCC Contract issues or problems, with regard to management or operations of the JWCC Contract, and the associated risks and mitigation plan;	The Government will assess if the Contractor is identifying issues and problems consistent with identified operating challenges.	Fully automated reporting mechanism identifying issues and problems.
34	5.1.6.4.1.7	Advising on the utilization of JWCC Contract and how it aligns to the commercial trends and practices;	The Government will assess if the Contractor is proposing commercial terms and practices that would benefit the DoD.	A fully automated optimization model that identifies commercial trends and practices that the DoD would benefit from.
35	5.1.6.4.1.8	Advising on establishing optimization goals with recommendations to achieve the goals; and for prior goals, a status of progress to achieve the goal and an anticipated completion date;	The Government will assess if the Contractor is assisting the Government with identifying optimization goals for JWCC opportunities.	N/A
36	5.1.6.4.1.9	Discussion of any previous quarter C3PO required reports submitted to the JWCC COR;	The Government will assess if C3PO findings are packaged in a quarterly report and discussed with the JWCC COR	N/A
37	5.1.6.4.1.10	Any Government agenda items provided to the Contractor for inclusion in the scheduled IPR;	The Government will assess if the agenda items are presented in a timely fashion for inclusion in the IPR.	N/A
38	5.1.6.4.1.11	Report on status of, and any issues regarding, exceptions. (CDRL 0024)	The Government will assess if the Contractor is properly managing existing and new exception requests	N/A
39	5.1.6.4.2	Technical Exchange Meetings (TEMs). As requested by the JWCC COR, the Contractor shall arrange, facilitate and execute TEMs. TEMs can include discussions of any current or upcoming TOs, any future JWCC Offerings and Commercial Offerings the Contractor will have available for purchase, and any content/topics determined by the JWCC COR or the JWCC PMO. The Contractor is responsible for providing meeting minutes (CDRL A013) for all TEMs.	The Government will assess if the Contractor is supporting all the requested TEMs.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
40	5.1.6.4.3	Ad Hoc Reporting/Information Products. The Contractor shall work with the JWCC COR to identify required ad hoc reports or information products related to deployment and utilization of the JWCC Contract. These reports or products will be used to assist the JWCC COR for effective deployment of the JWCC Contract. This reporting is in addition to other reporting requirements mentioned herein.	The Government will assess if the Contractor is responsive to all ad hoc reporting and information requests.	N/A
41	5.1.6.5	Ordering Guide Inputs.	Summary Requirement	N/A
42	5.1.6.5.1	The Contractor shall address, as part of the Contract Ordering Guide Annex (CDRL A007), any specific information that users need to understand how to successfully order JWCC Offerings, to be included in the JWCC Ordering Guide.	The Government will assess if the ordering guide is complete and useful for a JWCC user to navigate and successful provision from the marketplace.	Fully automated, intuitive navigation and self-help environment that is routinely updated without annex submissions.
43	5.1.6.5.1.1	Contractor's PoC information and e-mail for contracting related issues.	The Government will assess if email addresses and POCs are accurate.	N/A
44	5.1.6.5.1.2	Contractor's email address for distribution of TOs (if different from above).	The Government will assess if email addresses and POCs are accurate.	N/A
45	5.1.6.5.1.3	Link to Contractor's hosting and compute calculators (hereafter referred to as "Calculators") at each classification level for the purpose of Independent Government Cost Estimate development that identifies only those JWCC Offerings that are authorized for DoD consumption under the JWCC Contract.	The Government will assess if the link is accurate and operational at each classification level.	N/A
46	5.1.6.5.1.4	Any specific process the Contractor may have for requesting TE Offerings that deviates from the normal fulfillment process.	The Government will assess if the non-standard marketplace process maintains appropriate TE offerings fulfillment management.	N/A
47	5.1.6.5.1.5	Any specific process the Contractor may have for requesting Cloud Support Packages.	The Government will assess the processes for requesting Cloud Support Packages.	N/A
48	5.1.6.5.1.6	The Contractor's inputs to the Contract Ordering Guide Annex shall be delivered to the Government (CDRL A007).	The Government will assess if the ordering guide annex sufficiently describes the process.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
49	5.1.6.6	<p>Contractor Cloud Portal Process. The Contractor shall provide to the JWCC COR the process of establishing initial accounts and Cloud Environments using the Contractor's Portal (both UI and API) and how to fulfill orders and provision/deploy JWCC Offerings from its JWCC Marketplace after the JWCC user account has been established. The Contractor Cloud Portal Process (CDRL A002) shall be delivered to the Government no later than 15 days after contract award and as necessary when changes are made. Only JWCC Offerings shall be visible and accessible in the JWCC Marketplace. A link (via Internet Protocol address) to the Contractor's Portal will be provided by Contractor for distribution to JWCC users for each classification level and IL.</p>	<p>The Government will assess if the Contractors process for establishing initial accounts and cloud environments meets the JWCC requirements.</p>	N/A
50	5.1.6.7	<p>JWCC Catalog. The Contractor shall submit its Commercial Catalog with Change Report-(CDRL A023). The Contractor's Commercial Catalog shall be the basis by which the JWCC Catalog is established. The Contractor shall submit its JWCC Catalog as Attachment J-4: JWCC Catalog Discounts, Premiums, and Fees. For additions or modifications to JWCC Offerings, the Contractor shall follow the process in G11, JWCC Catalog Modifications, and submit the JWCC Catalog with Change Report (CDRL A022). The Contractor shall support the JWCC KO/COR in the maintenance and upkeep of the JWCC Catalog by recording and reporting changes on a periodic basis via JWCC Catalog with Change Report (CDRL A022).</p>	<p>The Government will assess if the Contractors catalog submission meets the requirements of the JWCC contract.</p>	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
51	5.1.6.8	Quality Control Plan (QCP). The Contractor shall provide a QCP supporting the Government-provided QASP for the JWCC Contract (see Attachment L-6). At a minimum, the QCP shall describe the approach for continuously meeting the performance metrics in Technical Exhibit 1 of the JWCC PWS, throughout the life of the JWCC Contract. The Contractor shall specifically address how all required performance metrics will be assessed, analyzed, and maintained through the life of the JWCC Contract. Cross-referencing between the QCP and PWS is permitted.	The Government will assess if the QCP describes the processes to ensure quality delivery of JWCC offerings.	N/A
52	5.1.6.8.1	The Contractor shall provide a PoC as part of the QCP to allow any JWCC user to communicate any issues or failures that arise from an attempt to invoke a JWCC Offering (provisioning) as ordered within a valid JWCC account. The contractor shall provide near-immediate acknowledgement (within 5 minutes of submission). The Contractor will action these communications IAW their QCP and any relevant support package SLAs associated with the JWCC users' identified TO. This PoC shall be available 24 hours a day, 7 days a week, 365 days a year, worldwide without any charges or expense to the Government. The modalities of contact shall include, at a minimum, voice (telephone), web-access (i.e. Contractor's Portal), and e-mail. The e-mail response timeline is within one hour of receipt and a response within five minutes of opening the e-mail. This PoC shall be available for all classification levels and ILs such that JWCC users can communicate the issue at the classification level they are currently operating at.	The Government will assess if the QC PoC information is compliant with the requirement.	N/A
53	5.1.6.9	TE Device Loss, Destruction, or Inoperability. Post award, the Contractor shall report on the number of TE Devices that have been lost, destroyed, or rendered inoperable for each device and circumstance and the total for each circumstance. This information shall be reported in the CMPR (CDRL A001) at the JWCC Program level and reported monthly at the TO level.	The Government will assess if the contractor has provided the appropriate information regarding TE Loss, Destruction, or Interoperability.	N/A
54	5.2	Activities to Assess and Authorize Contractor's Cloud Infrastructure and Offerings	Summary Requirement	N/A
55	5.2.1	The Contractor shall conduct any activities necessary to receive DoD authorization for all XaaS and TE Offerings at each classification level and IL, for inclusion on the JWCC Catalog.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			providing the expected outcomes.	
56	5.2.2	The Contractor shall maintain any authorization achieved for the duration of the JWCC Contract, and any TO awarded thereunder, to include conducting continuous audit assessments and, as needed, management reviews as requested by the JWCC KO or AO.	The Government will audit all authorizations achieved for the duration of the contract to ensure a continuous authorization state is maintained for qualified services and offerings.	N/A
57	5.2.3	The Contractor shall prepare and submit a sufficiently complete Security Authorization Package (CDRL A009) to demonstrate compliance with all applicable requirements in C3PO, including all invoked references and their requirements.	The Government will audit the items and services delivered to ascertain whether the overarching program management personnel, control processes and tools are providing the expected outcomes.	N/A
58	5.3	Multi-Cloud Solution Technical Exchange Meetings (TEMs)	Summary Requirement	N/A
59	5.3.1	The Contractor shall participate in multi-cloud solution TEMs (including interoperability discussions) with other Federal and DoD contractors, including CSPs, with the goal of exploring novel solutions to optimize and streamline multi-vendor solutions and approaches for the benefit of the DoD, at the TO level. The TEMs will be convened as directed by the TO COR.	The Government will audit if the Contractor is both represented in TEMs and actively participating and contributing.	N/A
60	5.4	System and Organization Control (SOC 1) Type II Reporting	Summary Requirement	N/A
61	5.4.1	The Contractor shall provide a SOC Audit Report (CDRL A014) as listed in the memorandum, "System and Organization Control Report Requirement for Audit Impacting Cloud/Data Center Hosting Organizations and Application Service Providers," dated May 2, 2019.	The Government will audit if the SOC Audit Report is compliant with the required content and delivered in a timely manner.	The SOC Audit Report will be exhaustive in content and delivered in a timely manner.
62	5.5	JWCC Timeline and Technical Requirements. The Contractor shall provide XaaS for Government consumption at all classification levels and ILs, within the JWCC Catalog (Attachment J-4), discernable by classification level and IL. The requirements in this section are a minimum capability, condition, or attribute of JWCC. All requirements within the PWS are subject to the timelines below and commensurate with their classification level, unless otherwise specified.	Summary Requirement	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
63	5.5.1	Timeline. Delivery of XaaS, including TE Offerings, will follow the timelines as listed below, unless otherwise specified.	Summary Requirement	N/A
64	5.5.1.1	Roadmap/Integrated Master Timeline (CDRL A019). The Contractor shall provide a roadmap and integrated master timeline, or a combined artifact (hereafter referred to as, "Roadmap/Integrated Master Timeline") that has each information set clearly discernible within the single artifact, that contain sufficient detail documenting how and when JWCC requirements will be met. The Roadmap/Integrated Master Timeline shall include indicators for every current and future Offering to track successful or unsuccessful outcomes presented in the Roadmap/Integrated Master Timeline for delivery and operability.	The Government will assess whether the Roadmap/Integrated Master Timeline (CDRL A019) provides sufficient content and detail and is submitted on time. The measure will be no more than 5% of offerings unaccounted for in the Roadmap/Integrated Master Timeline, including current, future, deprecated, and removed items.	The Roadmap/Integrated Master Timeline fully details the duration of the contract with no offerings left unaccounted.
65	5.5.1.2	Unclassified Timeline. The Contractor shall provide its UNCLASSIFIED Offerings at ILs 2, 4, and 5 immediately upon JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as UNCLASSIFIED Offerings, including UNCLASSIFIED TE Offerings. No later than the JWCC Contract award date, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, and submit Security Authorization Package(s) (CDRL A009).	The Government will assess whether all UNCLASSIFIED offerings and TE offerings meet all security requirements as defined in C3PO and are delivered at time of award. The Government will assess whether any UNCLASSIFIED (IL 2, 4, or 5) offerings that have not been previously authorized are delivered to, and include all documentation required by the AO, at JWCC Contract award.	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.
66	5.5.1.3	Classified Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the SECRET (IL 6) level, within 60 days after JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) these Offerings as SECRET JWCC Offerings, including SECRET TE Offerings. Within 60 days post-JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254, and submit Security Authorization Package(s) (CDRL A009).	The Government will assess whether CLASSIFIED offerings at the SECRET (IL 6) level and TE offerings meet all security requirements as defined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254. The Government will assess whether CLASSIFIED offerings supporting SECRET (IL 6) level workloads and TE offerings were made available for use/authorization by the DoD within 60 days after JWCC Contract award. The Government will assess whether any SECRET (IL 6) level offerings that have not been previously authorized are delivered to, and include all documentation required by the	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			AO, within 60 days after JWCC Contract award.	
67	5.5.1.4	Classified Top Secret Timeline. The Contractor shall provide its CLASSIFIED Offerings at the TOP SECRET (including (TS/SCI)) level, within 180 days after JWCC Contract award, such that DoD will have the ability to deploy and use (immediately upon authorization) these Offerings as TS JWCC Offerings, including TE Offerings (TS and TS/SCI). Within 180 days post-JWCC Contract award, the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization for all TS JWCC Offerings. The Contractor shall ensure all JWCC Offerings meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, and IC Directive (ICD) 503 (TS and TS/SCI), and submit Security Authorization Package(s) (CDRL A009).	The Government will assess whether CLASSIFIED offerings capable of supporting TS and TS/SCI workloads meet all security requirements outlined in C3PO, DoDM 5200.01, the Attachment J-3: JWCC DD254, and IC Directive (ICD) 503 (TS and TS/SCI). The Government will assess whether CLASSIFIED Services supporting TS and TS/SCI workloads and TE offerings were made available for use/authorization by the DoD within 180 days after JWCC Contract award. The Government will assess whether, for any services that have not been previously authorized, all documentation required is delivered to the AO, within 180 days after JWCC Contract award.	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering with the ability to perform analysis.
68	5.5.1.5	Special Access Programs (SAP) Timeline. The Contractor shall support securely hosting SAP workloads, such that the DoD will have the ability to accomplish SAP missions using Contractor-provided JWCC Offerings IAW DoDD 5205.07, DoDM 5200.01, and the Joint Special Access Program Implementation Guide (JSIG). These JWCC Offerings shall be delivered consistently with the timelines for UNCLASSIFIED, SECRET, and TOP SECRET with documentation and evidence demonstrating compliance with SAP controls. The Contractor shall provide any additional documentation and artifacts as required by the corresponding SAP AO, per SAP	The Government will assess whether the ability to host SAP workloads meet all security requirements IAW DoDD 5205.07, DoDM 5200.01, and the JSIG at the UNCLASSIFIED, SECRET and TOP SECRET classification levels. The Government will assess whether documentation and evidence demonstrates compliance IAW DoDD 5205.07, DoDM 5200.01, and	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
		workload, and submit Security Authorization Package(s) (CDRL A009).	the JSIG in order to be approved for hosting SAP workloads.	
69	5.5.1.6	Cross-Domain Solution (CDS) Timeline. The CDSs shall meet the DoD's requirements as described in section 5.5.8.2. The Contractor shall provide CDSs for the Management Plane in conjunction with the associated CLASSIFIED Infrastructure and JWCC Offerings, on or before the delivery of that CLASSIFIED Infrastructure and JWCC Offerings. The CDSs for the Production Plane shall be provided to the DoD within 180 days after the delivery of the associated CLASSIFIED infrastructure and JWCC Offerings. All provided CDSs shall be authorized for use by the DoD Information Security Risk Management Committee (DoD ISMRC). For any CDS that is not presently authorized, the Contractor shall provide all documentation and artifacts required for CDS authorization to the DoD ISMRC in conjunction with the delivery of the associated CDS, and submit Security Authorization Package(s) (CDRL A009).	The Government will assess whether a CDS that meets the requirements in 5.5.8.2 was made available to the DoD IAW the timeline required for each classification level as it applies to the management plane and production plane. The Government will assess whether all required documentation is made available to the ISMRC for authorization.	The process for requirements compliance is fully automated and presented in a continuously updated report for each CDS.
70	5.5.1.7	Advisory and Assistance Services. The Contractor shall provide advisory and assistance services, as part of its Cloud Support Package, available at all classification levels and ILs IAW the service delivery timelines listed above, in order for JWCC users to acquire advisory and assistance services from the Contractor to support use of JWCC Offerings. The Contractor-provided advisory and assistance services shall meet DoD's requirements as outlined in section 5.5.11.	The Government will assess whether advisory and assistance services are available for the JWCC on the same timeline as the UNCLASSIFIED, SECRET, and TOP SECRET offerings, and whether such services meet the requirements in 5.5.11.	The advisory and assistance services are available prior to offerings (roadmap/timeline based) to enable pre-planning.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
71	5.5.2	Available and Resilient Services. The Contractor shall provide Highly Available, resilient CSOs that are reliable, durable, and able to continue operating despite catastrophic failure of portions of the infrastructure. Infrastructure used in the performance of CSOs under JWCC shall be capable of supporting globally dispersed users at all classification levels, including DDIL environments, and Closed-Loop Networks. In order to provide the resiliency and availability required by JWCC users, there must be no fewer than three physical Data Center locations with the ability to operate independently, each including the ability for JWCC users to deploy and manage CSOs at its respective classification level and IL. At least two of the Data Centers must be geographically dispersed by at least 400 miles, utilizing separate power grids, and within the Customs Territory of the United States, as defined in FAR 2.101. UNCLASSIFIED and CLASSIFIED (both SECRET and TOP SECRET) Data Centers may be co-located, as long as the CLASSIFIED Data Center meets FCL requirements IAW C3PO and Attachment J-3: JWCC DD254.	Summary Requirement	N/A
72	5.5.2.1	The Contractor shall provide dynamic scalability and resiliency through industry standard mechanisms and activities to ensure the DoD has the ability to maintain continuous operations.	The Government will perform testing of offerings deployed and operating within JWCC for scalability, resiliency, performance, cybersecurity, and cyber survivability.	The offerings will be automatically scalable and resilient.
73	5.5.2.2	The Contractor shall provide the ability for JWCC users to create system configurations, both manually (i.e. via Contractor Portal (UI)) and through APIs, to provide automated redundancy of storage, networking, and computing systems in the case of catastrophic data center loss or loss of CSOs.	The Contractor will demonstrate at least annually how JWCC users can configure CSOs both manually, via the Contractor's Portal, and via the API, for high availability and resiliency such that it can survive catastrophic data center loss or loss of capabilities.	All CSOs have a native API for high availability and resiliency as well as a single click (per CSO) to enable typical high availability features.
74	5.5.2.3	The Contractor shall provide CSOs that are Highly Available and resilient. Accordingly, the Contractor's minimum Data Center capabilities are as follows:	Summary Requirement	N/A
75	5.5.2.3.1	Every data center shall be capable of automated replication and failover of CSO(s) within each respective classification level and IL inclusive of the ability to provision, configure, and manage services, such that the DoD is provided Data Center agnostic operations.	The Contractor will demonstrate, at least annually, through design documentation, physical exercise, or any combination thereof, the ability to failover a data center with no lasting impact to Government operations (e.g., browser refresh due to network redirection to a	All failovers are fully automated and there is no appreciable downtime (99.99999%) for any offering

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			new data center is understandable, but loss of data which should have been synchronized with a secondary facility is unacceptable.)	
76	5.5.2.3.2	The Contractor shall, at time of award, provide no fewer than two physical Data Centers providing UNCLASSIFIED CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide UNCLASSIFIED CSOs. The Government reserves the right to inspect any facility used to host JWCC workloads.	The Contactor will have at least two data centers for every Contractor defined Operating region and each region is a minimum of 400 miles apart.
77	5.5.2.3.3	The Contractor shall, upon delivery of SECRET CSOs, provide no fewer than two physical Data Centers providing SECRET CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide SECRET CSOs for JWCC. The Government reserves the right to inspect any facility used to host JWCC workloads.	The Contactor will have at least two data centers for every Contractor defined Operating region and each region is a minimum of 400 miles apart.
78	5.5.2.3.4	The Contractor shall, upon delivery of TS CSOs, provide no fewer than two physical Data Centers providing TS CSOs within the Customs Territory of the United States, as defined in FAR 2.101.	The Government will assess whether the Contractor has at least two data centers meeting the requirements above that provide TOP SECRET CSOs for JWCC. The Government reserves the right to inspect any facility used to host JWCC workloads.	The Contractor will have at least two data centers for every Contractor defined Operating region and each region is a minimum of 400 miles apart
79	5.5.2.3.5	The Contractor shall, no later than 18 months after contract award, provide no fewer than three physical Data Centers providing CSOs at each classification levels and ILs. At least two of these three physical Data Centers shall be geographically dispersed by a minimum of 400 miles, by radial measurement, utilizing separate power grids as defined by the Office of Electricity within the U.S. Department of Energy, and within the Customs Territory of the U.S., as defined in FAR 2.101.	The Government will assess whether the locations of the physical data centers are geographically dispersed and utilize separate power grids. The Government reserves the right to inspect any facility used to house JWCC workloads.	All data centers will be serviced using fully independent utility resources.
80	5.5.2.3.6	The physical data centers at all classification levels and ILs shall strictly comply with all applicable C3PO requirements.	The Government will assess the sufficiency of data center compliance with respect to C3PO will advise the Contractor of any deficiencies for resolution.	All data centers will exceed C3PO standards.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
81	5.5.2.4	The Contractor shall provide, at each classification level and IL, automatic monitoring of resource utilization and events (to include failures and degradation of service) via web interface and documented APIs that are intuitive and easy to use.	The Contractor will demonstrate its monitoring capabilities to the Government, at least annually, at each classification level and IL. In addition, the Government may audit, at any time and via any reasonable method, the Contractor's monitoring capabilities.	All events are fully logged and pre-emptive automated system actions are taken to negate degradation and threat events.
82	5.5.3	Globally Accessible. The Contractor shall provide CSOs that are securely accessible worldwide via the Contractor's Portal (UI), at all classification levels and ILs. The CSOs shall provide assured access and enable interoperability between Virtual Enclaves containing applications and data.	Summary Requirement	N/A
83	5.5.3.1	The Contractor shall have points of presence on all continents, with the exception of Antarctica, providing a total bandwidth capacity of at least 40 Gigabits per second, using redundant links, to peer with the DoD on each continent. If the DoD adds new locations, the Contractor shall peer with the DoD within 12 months of notification such that the latency between the Contractor's and the DoD's locations is less than 8 milliseconds. The Contractor shall provide documentation that validates the transmission speeds, latency, and bandwidth at each location.	The Government will assess, through review of documentation, site inspection, or any combination thereof, whether the Contractor has points of presence on all continents, with the exception of Antarctica, and that those points of presence have redundant links with a total bandwidth of at least 40 Gigabits per second as measured by network bandwidth tools. The Government will assess the Contractor's peering activities to ensure compliance with the 12 month peering notification requirement.	All Points of Presence support maximal bandwidth capability offered and dynamic automated peering services are available.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
84	5.5.4	<p>Centralized Management and Distributed Control. The Contractor shall permit the DoD to exert necessary oversight and management of CSOs. This oversight and management includes, but is not limited to: the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process. In order to exercise centralized management, the Contractor shall have a mechanism for activating and deactivating any CSO for JWCC workspaces. The Contractor shall provide a mechanism to provision CSOs based on standardized, templated configurations and security policies, as well as a “user friendly” mechanism to deprovision any combination of CSOs (e.g. one, multiple, or all). The Contractor shall also provide as part of its solution object and resource access control management, including data and resource tagging for billing tracking, access control, and technical policy management. The Contractor shall facilitate the automation of central management and distributed control. The Contractor shall provide an actively maintained, versioned, and documented API providing the ability to perform any operation supported by the Contractor’s Portal (UI).</p>	Summary Requirement	N/A
85	5.5.4.1	<p>The Contractor shall provide the ability to apply security policies, monitor network security compliance and service usage, promulgate standardized service configurations, and automate and distribute the account provisioning process to give the DoD the ability to enforce its policies and security compliance for the JWCC Contract workloads.</p>	<p>The Government will assess whether the Contractor has provided the Government the ability to enforce security policies and standardized configurations in a manual and automated manner.</p>	<p>All policy configurations can be generated and visualized using a Contractor’s Portal (UI) tools and the policy application is immediate and comprehensive. Additionally, all compliance can be easily reported and visualized.</p>
86	5.5.4.2	<p>The Contractor shall provide the ability to enable and disable services and restrict parameters within service configurations via both the Contractor’s Portal (UI) and API, in a manner that is easy to use such that the JWCC COR and administrative JWCC users within the DoD can properly control service delivery to the greater JWCC user community. This ability to restrict services shall allow for hierarchical subordinated supplemental constraints.</p>	<p>The Contractor will demonstrate, at least annually, the ability to perform the enablement and disablement of services with a sufficient number of parameters via the Contractor’s Portal (UI) and API to the JWCC COR and include in their documentation and training material instructions on how to perform these activities. Additionally, the allowance for hierarchical subordinated supplemental constraints must</p>	<p>The control of services (enable/disable) and all associated parameters can be controlled via a Contractor’s Portal (UI), trigger-sensing API, or heads-up UI. The hierarchical inheritance model will be automatically applied.</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			also be demonstrated. The Government will assess the sufficiency of the demonstration and the provided documentation, and may audit, at any time and via any reasonable method, the Contractor's ability to enable and disable services.	
87	5.5.4.3	The Contractor shall provide object and resource management capabilities, including data and resource tagging for billing tracking, access control, and technical policy management in order for the DoD to properly administer the JWCC Contract.	The Government will assess whether the Contractor has the ability to provide object and resource management capabilities; including billing trackers, access controls and technical policy mandates that are inherited from the parent organizations. The Government reserves the right to perform periodic testing of these capabilities.	All cloud resources are manageable using API or a Contractor's Portal (UI), in a central and distributed model.
88	5.5.4.4	The Contractor shall provide an API that supports encryption and authentication as defined in C3PO for all JWCC users and sessions, for each XaaS at all classification levels and ILs. The API shall, at a minimum, be capable of the following:	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	N/A
89	5.5.4.4.1	IAM controls, including account creation and management in support of the JWCC Contract, token-based and time-limited federated authentication, role-based access control configuration, and specific account permissions.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	Full PBAC is implemented for all offerings
90	5.5.4.4.2	Provisioning and management (i.e. IaaS) of network configuration, compute instances, data and object storage including database management systems, and tools for scaling systems (e.g. application server load balancing).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	All cloud configurations have provisioning scripts in a central virtually accessible library that is dynamically populated if a new configuration arises.
91	5.5.4.4.3	Storage object lifecycle management (e.g. moving data from online to nearline after a set time period).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	All objects have a parametric tag that is dynamically managed to provide the most appropriate storage type. Additionally the ability to configure objects to

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				change storage type based on AI/ML learning algorithms trained on access and interaction data based on file type, location, other policy information, or any combination thereof.
92	5.5.4.4.4	Reading usage data and alerts for compute, storage, and network utilization (e.g. resource/performance monitoring and utilization).	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	Automated parametric response triggers are programmatically executed on achieving specific conditions.
93	5.5.4.4.5	Reading accrual, historical billing, and pricing data specified under the entire JWCC Contract to include data for: CSOs, Cloud Support Packages, and workspaces.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	Automated parametric response triggers are programmatically executed on achieving specific conditions.
94	5.5.4.4.6	Setting billing and usage thresholds and adding automated notifications to workspace owners and the TO COR as well as a capability to configure the discontinuation of service upon the billing and usage threshold breach.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	Automated parametric response triggers are programmatically executed on achieving specific conditions.
95	5.5.4.4.7	Accessibility to all JWCC users provided they have the proper access control authorization.	The Government will assess the sufficiency of the API to support all of the requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	Automated parametric response triggers are programmatically executed on achieving specific conditions.
96	5.5.4.5	The Contractor's APIs, at all classification levels and ILs, shall be actively maintained, versioned, documented, and adhere to industry best practices for modern standards and protocols. API documentation shall contain information on: how to establish a connection, support protocols, security requirements, and capabilities available.	The Government will assess the Contractor's API documentation (e.g. release notes) to ensure sufficient detail and consistency for changes implemented such that the Government can determine the nature of the change, potential impact, actual impact, or any combination thereof, on current operations.	All APIs are fully self-documented. All API changes are both human and machine consumable for automated change analysis.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
97	5.5.4.5.1	<p>The Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs, of any change to API capabilities impacting backwards compatibility at least 30 days prior to the change being put into production. Alternately, if the change is to address a critical vulnerability, as designated by the Critical Vulnerability Scoring System, the Contractor shall notify all JWCC administrative users, the JWCC COR, and TO CORs within 24 hours of the change. Additionally, the Contractor shall make available this same information to all DoD personnel and other authorized JWCC users.</p>	<p>The Government will assess whether the Contractor has adhered to notification time frames for API changes.</p>	<p>All API changes will include full back-compatibility and test spaces are provided which allow for users to perform test calls to the new API prior to its full implementation.</p>
98	5.5.4.5.2	<p>The Contractor shall provide full API documentation online (to include examples of code). Full API documentation shall be readily discoverable within three clicks from the Contractor's Portal(s) (UI) landing page. API documentation shall also be available on TE Devices operating in DDIL environments.</p>	<p>The Government will assess whether the API online documentation is accessible within the required parameters at all classification levels and ILs to include TE Devices operating in a DDIL environments. Tailoring of the APIs may be necessary across classification levels and ILs, to include TE Devices and the documentation must be tailored to document any changes to the API and its parameters (i.e., if variables, features, or flags deviate from the commercial baseline they must be clearly documented and supported until such time as commercial parity can be established.)</p>	<p>All API documentation is accessible from a fully automated repository that supports dynamic query and retrieval capabilities for both API driven and Contractor Portal (UI) users. Example code would further include tutorials and supporting files/information required to ensure users can fully grasp how to utilize the API.</p>
99	5.5.4.5.3	<p>The Contractor API shall provide the ability to perform any command supported by the Contractor's Portal (UI).</p>	<p>The Government will assess the ability to perform API calls and the corresponding Contractor Portal activity as a part of regular business and inform the Contractor of any deficiencies.</p>	<p>The Contractor will self certify and provide automated tools which can empirically demonstrate compliance with this requirement with less than 1 percent of the API calls being deviant.</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
100	5.5.4.6	<p>The Contractor shall provide a fully compliant implementation of the ATAT Multi-Cloud Provisioning API (Attachment J-11) at each classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for test workloads within 15 days of providing JWCC Offerings at the associated classification level and IL. The Contractor shall provide an API endpoint per classification level and IL for production workloads within 30 days of providing JWCC Offerings at the associated classification level and IL. The Contractor implementation shall be pursuant to Attachment J-11: ATAT Multi-Cloud Provisioning API, to enable ATAT to execute calls to the API resulting in standardized mechanisms for:</p> <p>Creation & management of access credentials for accounts and environments in which CSOs can be provisioned.</p> <p>Creation and management of portfolios which manage groups of accounts and environments. The deadline by which the Government expects the portfolio provisioning process to be complete is dictated within the ATAT Multi-Cloud Provisioning API (Attachment J-11).</p> <p>Obtaining actual and projected costs per CLIN, environment, workloads, and portfolio.</p> <p>Setting billing limits with notifications on CLINs, environments, workloads, and portfolios.</p>	<p>The Government will assess whether ATAT calls to the Contractor's ATAT Multi-Cloud Provisioning API implementation(s) to create and manage portfolios, accounts, environments, or any combination thereof are successful, that the implementation conforms to the API specifications in J-11, and that the expected outcomes of the API call is achieved in the Contractor's cloud environment. The Government will assess if the implementation conforms to the API specification and that ATAT calls to the Contractor's ATAT Multi-Cloud Provisioning API implementation can obtain actual and projected costs per environment, workload, and portfolio and set billing limits and notifications on environments, workloads, and portfolios.</p>	<p>All ATAT API features are fully implemented and properly working. A fully configured sandbox and test harness exists to emulate a parallel ATAT production instance for robust testing including performance conditions allowing for DevSecOps processes to enable constant iteration and improvement.</p>
101	5.5.4.7	<p>The Contractor shall update its ATAT Multi-Cloud Provisioning API implementations to the latest version of the ATAT Multi-Cloud Provisioning API definition within 30 days of Government notification for general updates, and within seven days for security updates. An extension to these timelines may be granted by the KO on a case by case basis.</p>	<p>The Government will assess whether the Contractor has implemented the latest version and functionality of the ATAT Multi-Cloud Provisioning API to maintain continued compliance with the published API requirements within the required timelines.</p>	<p>The Contractor's implementation is updated within 1 business day for all updates to the ATAT Multi-Cloud Provisioning API with no explicit notification from the Government required at all classification levels and ILs.</p>
102	5.5.4.8	<p>The Contractor's implementation of the ATAT Multi-Cloud Provisioning API shall provide services comparable to the Contractor's other APIs in terms of API service delivery performance.</p>	<p>The Government will test the Contractor API implementation for availability, scalability, and other parameters as part of the Contractor SLA for API services.</p>	<p>The Contractor's API implementation supports continuous operations for scale, and all parametric permutations at all classification levels and ILs.</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
103	5.5.4.9	The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government has the ability to control any CSO for a subset of the JWCC users or grouping of JWCC users based on individual AO's risk tolerance(s).	The Government will assess, at least annually, whether the Contractor is providing the Government the ability to activate or deactivate, any or all of the Contractor's CSO under the JWCC Contract for an individual workspace	The activation/deactivation is capable of being done from the Contractor's Portal (UI), the API, and current status visualizations from both the Contractor's Portal (UI) and API are available for consumption.
104	5.5.4.10	The Contractor shall provide a mechanism for activating and deactivating any JWCC CSO such that the Government can activate or deactivate any CSO for all of the JWCC users based on DoD Authorization status or cybersecurity needs.	The Government will assess, at least annually, whether the Contractor is providing the Government the ability to perform activate or deactivate, for all workspaces simultaneously, any cloud service offering being provided by the Contractor under the JWCC Contract.	The activation/deactivation is capable of being done from the Contractor's Portal (UI), the API, and current status visualizations from both the Contractor's Portal (UI) and API are available for consumption.
105	5.5.4.11	The Contractor shall provide an IaC CSO, which allows the deployment and provisioning of one or more other CSOs. This IaC CSO will use pre-made standardized configurations and allow for customizable configurations. This IaC CSO shall also include a simple mechanism to deprovision any and all CSOs it deployed or provisioned.	The Government will assess whether the Contractor is providing the Government the ability to deploy a standardized configuration of cloud resources, including security policies, as well as the ability to deprovision in compliance with the configuration specification.	Support for a fully programmable API and a Contractor Portal (UI) is available to deploy and deprovision resources for dynamic configurations and direct input with associated visualizations for current status.
106	5.5.4.12	The Contractor shall not bundle any JWCC Offerings in a manner that restricts a JWCC user's ability to acquire individual JWCC Offerings. Any bundled JWCC Offerings shall also be available as discrete JWCC Offerings.	The Government will assess whether all services that are combined to form a different service offering are available separately, allow the user to acquire each service independently, and are billable as a single item.	All offerings are discretely available and any combination or aggregation permutation is supported.
107	5.5.4.13	The Contractor shall not require any third-party services that require separate billing, separate licensing, or a combination thereof in order to meet the JWCC requirements or minimum requirements for using any JWCC CSO. Any third-party services that are fully integrated with the Contractor, hosted on the Contractor's infrastructure, and directly supported by, billed through, and licensed by the Contractor are not subject to this requirement.	The Contractor shall certify compliance with this requirement and the Government will assess compliance through the course of doing business with no identified exceptions to this requirement.	The Contractor shall empirically demonstrate compliance to the requirement with comprehensive documentation and self certification.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
108	5.5.4.14	The Contractor shall provide prompt notification and follow-up reporting on all service incidents, outages, and other problems (hereafter collectively referred to as, "Service Incident Events") impacting JWCC users or cloud operations. The following minimum requirements apply to all environments, including network and TE Devices:	Summary Requirement	N/A
109	5.5.4.14.1	The Contractor shall establish and utilize Service Incident Event management processes, as well as support accessibility and escalation processes, such that the Contractor is able to prioritize and manage response reactions while keeping users informed about Service Incident Event status, remediation schedule, and overall priority amongst all other current Service Incident Events.	<p>The Government will assess whether the Contractor's Service Incident Events management process ensures that each incident is fully traceable through each step of the Contractor's Service Incident Event management process such that:</p> <p>Incident escalation mechanisms are clearly observable and course of action adjustments are captured.</p> <p>Full logging is enabled for each incident and all remediation actions are captured in persistent logs</p>	Service Incident Event Management is fully automated and 100% activity is logged and analyzed for optimization opportunities and auditing for security best practices.
110	5.5.4.14.2	The Contractor shall notify the impacted JWCC users, the JWCC COR, and TO CORs once a Service Incident Event has been detected or discovered. The Contractor shall notify the users, via electronic means, including severity level, for each Service Incident Event. Service Incident Event notifications shall be made IAW the SLA.	The Government will assess the timely delivery of notification for each Service Incident Event.	The notification system is multi-modal and each user is able to select any combination of notification modes for their individual needs.
111	5.5.4.14.3	The Contractor shall provide updates on Service Incident Event reports to include the impacted JWCC users, the JWCC COR, and TO CORs. The updates shall be provided at intervals IAW the SLO with the SLA, until the Service Incident Event is completely resolved. Updates shall include supplemental Service Incident Event information to aid in understanding the Service Incident Event's scope, severity, and resolution progress, clearly identifying any outage(s) or other significant problems.	The Government will assess whether the Contractor has provided timely updates based on each Service Incident Events evolving status. The Government will assess whether such updates provide sufficient information and are in compliance with the SLOs.	Updates for a Service Incident Event are provided automatically to every impacted user in real-time. Additionally update information is provided to an advanced data analytics CSO for pattern analysis and predictive failure analytics.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
112	5.5.4.14.4	The Contractor shall issue a Service Incident Event report to the impacted JWCC users, the JWCC COR, and TO COR when CSOs functionality or cloud operations performance are impacted. The report shall contain, at minimum, a description of the nature of the Service Incident Event, an impact scope statement, the severity level, and the Mean Time to Resolve estimate.	<p>The Government will assess whether:</p> <p>The impact scope statement contents and Service Incident Event severity levels are accurate and complete, such that they inform users and provide sufficient understanding of the event, time horizon to resolve the event and impact to the user.</p> <p>Compliance with Contractor's stated Service Level Objectives (SLO), as stipulated in the Contractor's SLAs, will be analyzed for deviation above the objective thresholds.</p>	The Service Incident Report is exhaustive and updated in real-time as activities transpire. Additionally reports are used as a basis for future chaos engineering tests to improve the cloud resiliency further reducing negative impacts to the DoD hosted capabilities.
113	5.5.4.14.5	The Contractor's maintenance activities shall not impact JWCC operations.	The Government will assess whether Contractor maintenance activities have resulted in any observable negative impact to JWCC users.	All maintenance activities are transparent to the users and have zero impact on user activities.
114	5.5.4.14.6	The Contractor shall provide the JWCC KO and JWCC COR with a detailed after-action report on all Service Incident Events within seven days of the Service Incident Event to allow the Government to understand the Service Incident Event's impact and determine appropriate follow-on actions.	The Government will assess whether the Service Incident Event after-action reports are complete and accurate. The Government will also assess whether event report delivery was compliant with the seven-day requirement.	Updates for a Service Incident Event are provided automatically to every impacted user in real-time including after-action reports and analysis.
115	5.5.4.14.7	The Contractor shall securely provide to the Government, human and machine readable cloud service status and Service Incident Event information for all JWCC Offerings.	The Government will assess whether the Contractor securely provides accessible and complete human and machine readable cloud service status and Service Incident Event information for DoD consumption.	All service and Service Incident Event statuses are available in real-time on a centrally managed presentation display or via API query with multiple user selectable display modes.
116	5.5.4.14.8	For disconnected TE Devices, the Contractor shall ensure notification of TE Device specific service outages are provided to any local users at the time of the outage incident and queued for synchronization to cloud services upon re-connection, allowing for centralized reporting and resolution tracking.	The Government will assess whether the notification to local users of a TE Device for any service outage is delivered and if centralized reporting and resolution tracking match when the device completes synchronization.	All TE Device and offering notifications are available to all TE enclave users, and automatically captured and stored to a central repository on reconnection. Additionally for situations which knock a TE Device off of the

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				core cloud services (i.e. unplanned disconnected operations) the service provides via multiple modes notifications to a set of identified administrators
117	5.5.4.15	The Contractor shall make available to the Government, standard and easy-to-interpret logs that are both human and machine readable. The Contractor shall ensure logs comply with C3PO and any other Regulatory or Statutory reporting compliance mandates. Such logs shall be generated and available using, at a minimum, either XML or JSON formats, and shall use a structured and verifiable schema. The Contractor shall make available any necessary tools required for log file and schema verification.	The Government will assess whether logs are readable by both human and machine, meet the specified delivery formats, and contain a structured and verifiable schema. Additionally the Government will perform verification of a random sampling of files with the schema using the Contractor provided verification tools.	All logs are created so that humans and machines are equally able to consume the same logs and a Contractor Portal (UI) is available which allows for integrated analytics using customizable queries and visualizations.
118	5.5.4.15.1	To support DoD's Defensive Cyber Operations, the Contractor shall provide access to all logs, related to JWCC, that are required for the Contractor's DoD authorizations which provide an audit trail of all activities and actions (e.g., "Scenarios," as defined in C3PO) as required under the CC SRG and DoD CIO Memorandum, Department of Defense Cybersecurity Activities Performed for CSO. To provide assurance of the actions of personnel assigned to or supporting an approved Oversight team, as defined in C3PO, for UNCLASSIFIED ILs, the Contractor shall explicitly identify (e.g. tag or separate) logs for all actions, whether direct or indirect, by Contractor personnel working under or as part of an approved oversight team, as defined in C3PO. There shall be no data use charges or transiting charges for accessing the logs stored in the consolidated log location(s).	The Government will assess whether the logs provide an audit trail of all activities and actions IAW C3PO.	The logs will contain all actions executed within the cloud and automatically identify and tag anomalous behavior and behavior which goes against security best practices leading to automated notifications for review of suspicious activity.
119	5.5.4.15.2	The Contractor shall provide access to the logs stored in the consolidated log location(s) through a User Interface (UI) and a secure API at each classification level and IL. The Contractor shall participate in collaborative analysis with the DoD, as appropriate. UI and API documentation regarding the logs and associated features shall be accessible from the Contractor's Portal (UI), at each classification level and IL, and include sample code.	The Government will assess whether the Contractor has provided a Contractor Portal (UI) at each classification level and IL for access to consolidated logs and their locations. The Government will assess whether the Contractor has provided API documentation from the Contractor's Portal (UI), at each classification level and IL, and included sample code.	A single Contractor Portal (UI) and API is enabled and the classification boundaries are managed as separable content mechanisms for the respective domains. All logs are also tagged with the origin security domain and associated metadata with the ability to be queried from higher domains for further analytics while

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				maintaining relevant metadata.
120	5.5.4.16	Financial Analytical Reporting. The Contractor shall provide a comprehensive financial analytical reporting capability at each classification level and IL, capable of providing current and historical data for all one-time and continuing operational costs. Available information shall include all discrete items (smallest JWCC Offering purchasable from the JWCC Catalog) with an ability to aggregate items, using selected filters, across the entire JWCC user period of interest. The reporting capability shall provide users a financial representation of how costs were accrued over the period of interest. Additionally, the reporting capability shall support a projection mode where, based on current behavior bound by a time period, an estimated cost projection can be computed for a future specified period of time.	The Government will verify that the provided financial analytical reporting capability produces accurate reporting based on a known configuration at each classification level and IL.	Financial reporting will include the ability to aggregate across all classification levels and ILs, and is only delivered to the appropriate classification levels and ILs.
121	5.5.4.16.1	The Contractor-provided financial analytical reporting capability shall include the ability to support JWCC user defined queries and interfaces of the financial data and support the following capabilities:	Summary Requirement	N/A
122	5.5.4.16.1.1	Direct requester UI that allows for JWCC users to directly input a query and receive commensurate results/outputs.	The Government will assess whether the financial analytical reporting capability provides a Contractor's Portal (UI) to perform queries and present generated results.	The Contractor's Portal (UI) will include tooltips, recommended built in queries, auto complete suggestions and integrated query help to aid users with less experience in the given query language.
123	5.5.4.16.1.2	Scripting capability that allows for repeatable periodic submission, based on a requester-managed file, where the results are delivered to a specified storage location.	The Government will assess whether the scripting capability allows for periodic submissions to a specified storage location.	A fully automated scripting engine that can create and periodically execute scripts and which suggests common queries and destinations based on the individual user, their role, and organization.
124	5.5.4.16.1.3	An API for automated system-to-system interchange to enable query-response to execute in a dynamic and on-demand, non-human interacted method.	The Government will assess whether the API allows automated system processing	The API is able to support parallel processing of

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			with no human intervention, and whether the API is elastic and able to support multiple rapid connections from disparate sources.	simultaneous connections
125	5.5.4.16.1.4	An ability to construct a dashboard from multiple queries at each classification level and IL, such that a JWCC user can view a complete financial picture constructed from multiple queries.	The Government will assess the dashboard presentation and query result accuracy based on a known configuration.	The dashboard is able to autosense classification domains and dynamically redact restricted information.
126	5.5.4.16.1.5	The ability to save and share queries and load query results to dashboards. Once a query is saved to the dashboard, there shall also be an option for an authorized user to read, modify, and delete the query. This ability shall enable users to access, share, and execute a saved query without entering any of the query content and produce routine reports for an overall picture of financial data.	The Government will test the ability to read, modify, delete and save a query, on execution accurately producing the expected results based on a known configuration.	A knowledge based stored query selector based on keyword(s) submission from a user (or API) and the ability to suggest queries based on the individual user, their role, and organization.
127	5.5.4.16.1.6	The ability to display a history of all query activity.	The Government will assess the accuracy of the query history report based on multiple known queries that were executed previously.	The ability to organize query history based on keyword or token submission and then store historical queries as named queries for future retrieval is provided.
128	5.5.4.16.1.7	The ability to support reporting to multiple presentation modes (e.g. files, screen displays, etc.) allowing users to indicate one or more output methods for a generated report. At a minimum, this shall include a user accessible dashboard and the file types PDF and CSV. PDF and CSV file types shall be natively available as a presentation mode regardless of the JWCC user's technology (e.g. modern web browser).	The Government will test the query capability to produce the presentation information in multiple modes of output, IAW the minimum output standards described above, and any other output methods available.	The ability to simultaneously report to all modes, selected by the user, of presentation.
129	5.5.4.16.1.8	The query capability shall support discrete reporting down to the smallest unit purchases and aggregate all included costs to present the overall financial picture to the user. This provides users the ability to understand costs down to the smallest units possible.	The Government will assess whether the query tool is capable of showing costs down to the smallest units purchased and aggregate all included costs to present the overall financial picture to the user.	The query capability is able to consume programmed aggregation feeds and reporting structures.
130	5.5.4.16.1.9	The query capability shall support continuous cost accrual reporting to give the ability to report total spend for a given period of time, enabling users to project future budget needs.	The Government will assess whether the query tool includes the ability to see accrued costs for a given period of time.	The ability to create dynamic time-phased reports.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
131	5.5.4.16.1.10	The query capability shall support aggregation of collected items that are grouped using tags. This shall allow users to group information based on specific groupings of information using user-supplied tags.	The Government will test the query tools ability to group information in a report based on tags.	The tagging engine can deconflict and manage colliding or overlapping tags without double counting selected data sets.
132	5.5.4.16.2	The Contractor shall provide a spend threshold capability to support warning thresholds at each classification level and IL. The spend threshold capability shall support establishment of threshold values by either the Contractor or the Government. The spend threshold capability shall provide a notification alert sent to a specified recipient list, such that Government users are “warned” of approaching spend threshold based on specific user needs.	Summary Requirement	N/A
133	5.5.4.16.2.1	The spend threshold capability shall allow each user to set specific threshold trigger values for which the spend threshold capability will execute a specified action, such that each user has the flexibility to specify multiple warning notifications based on unique independent threshold trigger values.	The Government will test, at least annually, whether the capability allows users to set parameters for threshold triggers to execute specific action(s) when that threshold is met.	The ability to identify and arbitrate conflicted trigger events and suggest/select the most appropriate action outcome.
134	5.5.4.16.2.2	The spend threshold capability shall include an optional suspension mode, such that the Government avoids Anti-Deficiency Act violations by incurring obligations that are not authorized. If the threshold is achieved, the system will suspend, using a defined process, any additional purchases in a managed manner - both one-time and continuing operational consumption. However, in no case shall the Contractor delete any stored information, including both volatile and non-volatile memory.	The Government will assess whether the Contractor has provided the spend threshold capability suspension mode to suspend further spend, at a specified threshold without any compromise on retention of data, at each classification level and IL for one-time and continuing operational consumption. The Government will also assess that this spend threshold capability suspension mode is optional by enabling and then disabling the suspension mode and exceeding the prior set threshold.	The capability to optionally pre-determine a spend threshold breach exists and an automated “notification” is issued when the computed threshold is encountered and a suspend action is executed.
135	5.5.4.16.2.3	The spend threshold capability shall support reinstatement of a suspended CSO such that the CSO can be restored, from the point of suspension, as previously configured.	The Government will assess whether the Contractor has provided the spend threshold capability to restore services, data, and spend authorization, either one-time or continuing operational consumption, once funds verification is provided, without any compromise on retention of data by setting an artificial threshold on a sample workload, invoking the	The spend threshold capability is able to auto-sense funds sufficiency and restore operations. This includes a minimum rationale margin tolerance to prevent micro-restart suspend spin lock.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			suspension mode and then adjusting the threshold or disabling the mode.	
136	5.5.4.16.3	The Contractor shall provide the capability to support time-based billing information at each classification level and IL, such that a user can calculate total charges for a specified period of time in support of auditing and budgeting activities.	The Government will assess whether the Contractor has provided the capability to allow the user to set time-based parameters and obtain billing information based on pre-set (day, week, month, etc.), as well as custom time-frames.	The capability will allow for multi-domain computations and auto-redacting information in unauthorized domains, summarizing e-data according to administrator configurable reporting policies, or any combination thereof.
137	5.5.4.16.4	The Contractor shall provide the capability for JWCC users to plan and estimate one-time and continuing operational costs based on a specified notional resource configuration inputs for a projected operational scenario such that a JWCC user can estimate the projected total cost for a given PoP.	The Government will assess whether the Contractor has provided the capability to support projection of spend based on current configurations, anticipated configurations (user specified), current spend rates applied to both current and anticipated configurations, as well as adjustments to services.	The capability will extrapolate projections based on prior and user estimated behavior patterns (e.g. estimated load, actual load, estimated load based on actual load).
138	5.5.4.16.5	The Contractor shall provide the capability to report balances for remaining funds on accounts, such that users have the ability to track burn rate. This capability shall also project a balance exhaustion date based on consumption activity.	The Government will assess whether the Contractor has provided the capability to present balances of remaining funds on Contractor accounts, including expected timeframe for depletion of current funds in the account(s).	The capability will provide analytics to estimate the rate of consumption plots and trends including variable time resolution down to the minute.
139	5.5.4.16.6	<p>The Contractor shall provide the capability, at each classification level and IL, to support financial reporting based on logical grouping of charges. Groupings shall include, but are not limited to:</p> <p>a. Reporting based on user/account, organizational structure (i.e. Enterprise, Department, Office, Team), or a combination thereof to determine cloud spend by user/account, organizational structure, or a combination thereof.</p> <p>b. Reporting based on type of services consumed to determine spending based on type of services consumed (e.g. storage, compute, data transfer, security).</p>	The Government will assess whether the Contractor has provided the capability report based on account, organizational structure, type of services consumed, and spend rate.	The capability will provide auto-grouping options that are based on past reports and account based user behavior(s).

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
		c. Reporting based on cost to determine services' impacts to spend rate.		
140	5.5.4.17	The Contractor shall provide processes and rule-sets that enable the Government, in its utilization of services under the JWCC Contract, to comply with the Freedom of Information Act (FOIA), the Federal Records Act, the DoD Records Management Program, Disposal of Records, Executive Order (EO) 12333, EO 13587, the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), and National Archives Records Administration (NARA) regulations.	The Government will exercise the provided manual and automated processes to ensure the data is managed as prescribed IAW the conditions and mandates of the specific guidance. In the event compound guidance is required, the assessment will apply the identified configurations sequentially to assure the outcome is acceptable.	The capability will accommodate all Federal reporting mandates.
141	5.5.4.18	The Contractor shall be capable of exporting security control assessment information using the NIST Open Security Controls Assessment Language (OSCAL) for JWCC Offerings to enable rapid authorization and accreditation of cloud services.	The Contractor will demonstrate the ability to export OSCAL data for their services and a sample workspace within the JWCC at least annually. The Government will assess whether exports are evaluated quarterly through independent testing for sustained compliance and 60 days post-major OSCAL version release.	The capability will implement all OSCAL features including those listed as optional.
142	5.5.5	Ease of Use: The Contractor must provide Self-Service capabilities enabling rapid development and deployment of new applications and advanced capabilities, including services from the JWCC Marketplace, as defined above. Additionally, the Contractor must support the portability of JWCC data and applications both out of and into the cloud. The Contractor shall provide a Portability Plan (CDRL A006) as detailed in sub-section 5.5.5.3.	Summary Requirement	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
143	5.5.5.1	The Contractor shall provide the Government the ability to rapidly and securely provision/deploy First-Party CSOs and Third-Party CSOs via the Contractor-provided JWCC Marketplace, as defined below, with baseline template configurations, onto JWCC infrastructure at all classification levels and ILs. Third-Party CSOs that are incapable of being deployed, used, or authorized on the Contractor's JWCC infrastructure are outside the scope of this contract.	The Government will assess their ability to provision/deploy offerings via the Contractor-provided JWCC Marketplace with baseline template configurations onto JWCC infrastructure at all classification levels and ILs.	N/A
144	5.5.5.1.1	The Contractor-provided JWCC Marketplace shall support the ability for JWCC users to deploy the first-party CSOs and third-party CSOs listed on the JWCC Catalog. All Commercial Offerings shall undergo accreditation and authorization processes appropriate for their control markings (e.g. classification level and IL, including SAP, SCI, and others as designated) before the Contractor adds them to the JWCC Catalog and makes them available for JWCC users to fulfill orders, provision, or deploy. Commercial Offerings that are not subject to the CC SRG, DoD, or IC standards must comply with-Government-approved Contractor security processes and standards (CDRL A016) before the Contractor adds them to the JWCC Catalog and makes them available on the JWCC Marketplace. The Contractor shall make all security information and process outputs available for Government audit and review.	The Government will audit the information and the processes execution to ensure that all necessary security processes and standards are appropriately managed and applied to all JWCC Marketplace offerings.	The approved process is created to enable all commercial JWCC Marketplace offerings to obtain a security disposition that allows the DoD AO to grant the necessary security authorization for use with easy to interpret information and online approval based on non-repudiation user input or pre-configured rules.
145	5.5.5.1.2	The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support centralized/integrated billing. The Contractor shall ensure all First-Party CSOs that are available in the JWCC Marketplace support bring your own license (BYOL), where applicable (e.g., where additional licensing is required).	The Government will assess whether all first-party offerings in the JWCC Marketplace support centralized billing, BYOL, or any combination thereof, at each classification level and IL.	The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
146	5.5.5.1.3	<p>The Contractor shall not apply additional cost to any Third-Party Marketplace Offering. This makes all Third-Party CSOs price-free from the Contractor, and all pricing shall be derived from the third-party that is providing the Offering in the third-party marketplace. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO. All Third-Party CSOs that are available in the JWCC Marketplace shall be offered price-free and BYOL basis as appropriate, excluding the cost of IaaS resources. These JWCC Offerings shall be made available, at all classification levels and ILs, IAW PWS section 5.5.1 and 5.5.6 and their subsections, except as approved by the JWCC KO.</p>	<p>The Government will assess whether all third-party JWCC Marketplace offerings do not have additional cost and are available price-free or BYOL at each classification level and IL.</p>	N/A
147	5.5.5.1.3.1	<p>For Third-Party CSOs available on a price-free or on a BYOL basis, the Contractor shall not impose additional license terms or conditions on the Government. The Government shall be solely responsible for negotiating the Terms and Conditions of the licenses for any Third-Party CSOs available on a price-free or on a BYOL basis that the Government has not previously negotiated Terms and Conditions under a separate contracting vehicle.</p>	<p>The Government will assess whether any BYOL or price-free third-party offering has additional Terms and Conditions beyond the Government provided license.</p>	<p>The Contractor will ultimately take direct responsibility for all offerings, First and Third Party, and provide these offerings in a consistent and compliant manner with the JWCC Terms and Conditions offered by the First Party Contractor. The outcome is that all offerings for the JWCC Contract are now aligned with the JWCC Contract Terms and Conditions, and the First Party Contractor is responsible for ensuring the Government is able to receive all offerings with this contractual provision and no other Term or Condition applies.</p>
148	5.5.5.1.4	<p>The Contractor shall ensure all Third-Party CSOs that are available in the JWCC Marketplace support centralized/integrated billing with the Contractor.</p>	<p>The Government will assess whether third-party offering cost accrual is integrated into the workspace billing and does not include licensing costs/fees.</p>	<p>The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
149	5.5.5.1.5	JWCC users' ability to order any discrete JWCC Offering shall be capable of being enabled or disabled at the IDIQ, TO, Cloud Environment, workspace, and JWCC user levels.	The Government will assess whether the ability for a JWCC user to order a sample third-party offering can be disabled at each level.	The ability to establish pool groups for enable/disable single action outcomes across multiple workspaces/organization s/accounts.
150	5.5.5.1.6	The Contractor's JWCC Marketplace shall be available at all classification levels and ILs IAW PWS section 5.5.1 and subsections, and new and modified Offerings shall be populated within 24 hours of completion of JWCC Catalog Modification process (Section G11). Access to the TS Marketplace shall be restricted to prevent fulfilling orders, provisioning, deploying, cloud operations, schedule non-provisionable or deployable offerings (e.g. Cloud Support Packages) until directed by the JWCC KO.	The Government will determine whether the JWCC Marketplace is available at the appropriate classification levels and ILs and within the stipulated time constraints.	N/A
151	5.5.5.2	The Contractor shall provide, at each classification level and IL, a Calculator reflecting contractually accurate price modeling and projection for any single JWCC Offering, or any combination of JWCC Offerings, at each classification level and IL, to enable authenticated DoD and JWCC users to properly estimate forecasted cloud spending for budgetary planning.	Summary Requirement	N/A
152	5.5.5.2.1	The Contractor's Calculator shall present all viable recommendations for available consumption-based pricing and subscription models (e.g. for reserved resources), including any applicable discounts.	The Government will assess whether the Contractor's Calculator is available for use by the DoD and performs cost calculations based on the pricing available to JWCC customers. The Government will also assess whether the output of the calculator presents all viable discounts available based on usage and subscription models (e.g., for reserved resources).	The Calculator will produce a single report of all possible computations for equivalent options based on an initial user input configuration and identify the best priced option.
153	5.5.5.2.2	The Contractor's Calculator shall provide the ability to compute and present projections to support users' long-term (in excess of 12 months) planning needs. The Contractor's Calculator shall provide users the ability to select time frames (e.g. month, quarter, year), as well as allow for custom time frames (e.g. Fiscal Year (FY) 2022 October 22 to FY 2024 January 15), to allow for accurate long-term budgeting.	The Government will assess whether the Contractor's Calculator provides users the ability to do long-term price projections based on user-selected time frames (e.g., month, quarter, year), as well as custom time frames (e.g., FY 2022 Oct 22 to FY 2024 Jan 15).	The Contractor's Calculator is able to dynamically respond to live user entry parameters for time periodicity adjustment projections.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
154	5.5.5.2.3	Estimates developed using the Contractor’s Calculator shall be made available in various formats, including, but not limited to, on screen, an image report (e.g. PDF document), and exportable/downloadable in a machine readable format that clearly breaks down the pricing by line item for further analytical processing, including by other tools used for analysis and comparison purposes.	The Government will assess whether the Contractor’s Calculator provides users the ability to obtain results in the formats described.	The Contractor’s Calculator supports a full API for programmatic modeling and projecting scenarios (e.g. AI driven modeling).
155	5.5.5.2.4	The Contractor’s Calculator shall be separately available at each classification level. The Contractor’s Calculator shall use and be consistent with the JWCC Contract pricing and the JWCC Catalog, based on the pricing and availability of all JWCC Offerings to allow for filtering and selecting any single JWCC Offering or any combination of JWCC Offerings at any classification level and IL for estimation. The Contractor’s Calculator shall default JWCC Offerings to the native classification level and IL where the Calculator is used. The Contractor’s Calculator shall be behaviorally and visually consistent at each classification level and IL, such that it provides a single “look and feel” at each classification level and IL (i.e., maintains Commercial Parity).	<p>The Government will perform periodic testing to determine whether the Contractor’s Calculator has consistent and reproducible outcomes using Government predefined order configurations, at each classification level and IL, as well as, its general appearance is uniform across all classification levels and ILs.</p> <p>The Government will also periodically assess whether or not the offerings are defaulting to the native classification level and IL based on the Government user’s environment.</p>	A single Calculator option for multi-classification pricing (i.e.: the Calculator is able to operate at the highest domain and pull data from all lower domains, without exposure of the data or the query).
156	5.5.5.3	The JWCC Contract will require information (data, files, and other forms of information) to be transferred both out of the Contractor’s Cloud Environment to another environment (cloud or otherwise) of the Government’s choosing and into the Contractor’s JWCC Cloud Environment from another environment (cloud or otherwise) of the Government’s choosing. In accordance with CDRL A006, the Contractor shall provide the Portability Plan to the Government when it is specified in a TO The Portability Plan shall address the following information in the below subsections as specified in individual TOs.	Summary Requirement	N/A
157	5.5.5.3.1	The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all, or some, of a JWCC user’s data from online, nearline, and offline storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a JWCC code repository, and network configurations. This shall allow the Government to move information (data and files) from the Contractor’s JWCC Cloud Environment to another environment (cloud or otherwise) of the Government’s choosing.	The Government will assess the Contractor’s Portability Plan contents to determine whether the user instructions provide a complete set of processes and procedures that are necessary to extract all, or some, of the JWCC user’s: online, nearline, and offline data, all configuration settings, environmental settings, logs and code repository content as well as any other substantive	A fully automated capability that targets all user data and prepares an optimized extraction plan for cost and speed and provides cost and time estimates to the user prior to execution. The capability allows the user to deselect items the automated plan identified and add items that are not

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			information required to equivalently replicate the operational environment.	identified. The plan can execute with a single user action.
158	5.5.5.3.2	The Portability Plan shall include an explanation of how the Contractor will achieve complete purging of all, or some, information as specified by Government direction, which may indicate all, some, or specific user, environment or workspace assets. The Portability Plan shall also include a description for how the Contractor shall prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Contractor's JWCC infrastructure pursuant to the CC SRG and C3PO.	The Government will assess the Contractor's Portability Plan to ensure it includes an explanation of how the successful disposition, wiping and reconfiguration of all, or some, of a JWCC user's system components and data is accomplished, and describe how a JWCC user is able to prevent the re-instantiation of any removed or disposed system, capability, data, or information instances once removed from the Contractor's JWCC infrastructure.	The capability will automatically attempt to access, reinstate, or any combination thereof, all removed items to validate successful disposition after confirming data transfer completion and identify any "success", which indicates eradication failure.
159	5.5.5.3.3	The Portability Plan shall specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to import all, or some, of a JWCC user's data from a user specified location (e.g. online, nearline, and offline storage locations, including, but not limited to: databases, object and file storage, system configurations, cloud activity logs, source code hosted in a code repository, network configurations, and on premises implementations) to the Contractor's JWCC cloud. This shall allow the Government to move information (data and files) from their existing environment (cloud or otherwise) to the Contractor's JWCC cloud.	The Government will assess the Contractor's Portability Plan contents to determine whether the user instructions provide a complete set of processes and procedures that are necessary to import all, or some, of a JWCC user's data from a user specified location: online, nearline, and offline data, all configuration settings, environmental settings, logs and code repository content as well as any other substantive information required to equivalently replicate the operational environment	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
160	5.5.6	Commercial Parity.	Summary Requirement	N/A
161	5.5.6.1	The Contractor shall ensure the provisioning of each JWCC Offering at each classification level and IL is equal to or faster than the average time computed daily for the provisioning of its equivalent Commercial Offering. The Contractor shall make available performance metrics for each Commercial Offering at each classification level and IL such that the Government can validate provisioning performance for each JWCC Offering (e.g. provisioning a new workspace, user, or service JWCC Offering, or deploying such JWCC Offerings within JWCC) as part of the Contract Monthly Progress Report (CDRL A001).	The Government will periodically assess whether commercial parity has been maintained for provisioning via testing at each classification level and IL.	An automated analytics report is generated at a parametrically specified interval to measure provisioning activity against observed (system measures/metrics) and Contractor published performance characteristics. This reporting is also available in a dynamic mode to allow DoD operators to monitor real time operations and service status.
162	5.5.6.2	The Contractor shall provide generational replacement and upgrading of all software (inclusive of firmware) and hardware (compute, memory, storage, and networking), at all classification levels and ILs, such that the Contractor's JWCC Offerings are on par with the Contractor's equivalent Commercial Offerings. The Contractor shall provide a Lifecycle Management Plan (CDRL A018) which demonstrates how it will meet this requirement.	The Government will assess the sufficiency of the Lifecycle Management Plan (CDRL A018). The Government will perform a periodic review of hardware replacement and upgrade to verify and validate whether Contractor is adhering to the Lifecycle Management Plan (CDRL A018). The Government will perform periodic inspection of software versions and security patching to verify whether the Contractor is adhering to the Contractor Lifecycle Management Plan (CDRL A018).	An automated analytics report is generated at a parametrically specified interval to measure the migration and availability of hardware and network generational replacements and software upgrades as they are produced/occur.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
163	5.5.6.3	<p>The Contractor shall achieve Commercial Parity, as soon as possible, but no later than 18 months after JWCC Contract award. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.</p>	<p>The Government will assess whether the cloud offerings at contract award, less the exception(s) authorized by the JWCC KO and service(s) deprecated by the target date, match the services available for authorization at each IL and classification level 18 months post contract award.</p>	<p>An automated report is generated which compares all offerings in every domain. Parity is achieved in under 6 months and sustained for the duration of the contract.</p>
164	5.5.6.4	<p>Each Contractor Commercial Offering that becomes available for licensing, purchase, or consumption following the JWCC Contract award, shall be submitted to the Government for authorization, at all classification levels and ILs, according to the following procedures and timelines:</p> <p>For CSOs requiring FedRAMP approval:</p> <ul style="list-style-type: none"> ● The Contractor must submit the CSO to the Joint Authorization Board (JAB) for authorization within 30 days of the CSO becoming Commercially Available. ● The Contractor must submit the CSO to DISA for authorization within 30 days of FedRAMP approval. <p>For CSOs requiring IC approval:</p> <ul style="list-style-type: none"> ● The Contractor must submit the CSO to the cognizant security authority for authorization within 30 days of the CSO becoming Commercially Available. <p>Each Commercial Offering shall be added to the JWCC Catalog IAW G11 at the classification level and IL for which it is authorized. If an exception is required the Exception Request must be processed prior to adding it to or modifying it on JWCC Catalog. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.</p>	<p>The Government will assess whether the Contractor provides the Government a complete authorization package within 30 days of new cloud offering availability, or has an approved exception.</p>	<p>An automated report is generated which identifies all offerings' event history, including authorization lifecycle details. Additionally services are made available the same day.</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
165	5.5.6.5	For any of the JWCC Offerings, across each classification level and IL, the same API calls and Contractor Portal (UI) actions shall result in the same expected behavior, except when restrictions due to classification level or IL prohibit Commercial Parity. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.	The Government may audit at any time during contract performance to determine whether API calls and Contractor Portal (UI) actions result in the expected behavior.	All APIs are available identically across all domains requiring no more than an environment variable and account identification to change between domains.
166	5.5.6.6	The Contractor shall provide Commercial Parity of CSOs and specialized hardware availability between Data Centers at each classification level and IL such that workloads are able to scale and migrate horizontally within a classification level and IL. In addition, the Contractor shall ensure that JWCC users have the ability to configure JWCC workloads for “high availability” as defined in NIST SP 800-113. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.	The Government will assess whether data centers are capable of scaling and migrating JWCC workloads horizontally, to the degree to which service parity exists, at each classification level and IL and validate users can configure the services for high availability.	An automated report is generated at a parametrically established interval identifying the maximal scaling and horizontal workload support. Additionally the Contractor makes available features which enable users to test failover between data centers in an easy and repeatable manner to support testing their developed capabilities and contingency operations.
167	5.5.6.7	All JWCC Offerings shall be at or below the Contractor’s Commercial Catalog pricing.	The Government will assess whether pricing provided by the Contractor is consistent with their commercial offerings.	Pricing for offerings that is lower than what is typically commercially available.
168	5.5.6.8	This requirement number is reserved for ease of administration.	N/A	N/A
169	5.5.6.9	Third-Party Marketplace Offerings are not considered Commercial Offerings for the purposes of Commercial Parity and, therefore, need not be identified in JWCC Exception Request (CDRL A024).	The Government will confirm this is not included in any Exception Requests.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
170	5.5.7	Modern and Elastic Computing, Storage, and Network Infrastructure. The Contractor must enable self-service automated provisioning of compute, storage, and network infrastructure that is constantly updated -- to include, but not limited to processing architectures, servers, storage options, and platform software -- at scale to meet consumption, rapid development, and deployment in support of mission needs.	Summary Requirement	N/A
171	5.5.7.1	The Contractor shall provide all CSOs, including those that are optimized for specific compute-based activities (e.g. evolving GPU and application specific integrated circuits (ASIC) processing architectures, quantum computing applications, and future evolving computational integrated circuit devices).	The Government will assess industry trends in modern scalar compute architectures to determine that the offerings are pacing with commercial parity in both physical hardware and software modernization.	An automated report is generated at a parametrically established interval identifying the trends in industry for cloud capabilities and competitor (boutique, focused and general) comparisons.
172	5.5.7.2	The Contractor shall provide for durable elastic growth for storage capabilities (e.g. Online, Nearline, and Offline Storage options; object, block, and file-based storage; as well as managed database and NoSQL (non-structured query language) services), at the speed of deployment that is commensurate with Commercial Offering deployment speeds. This shall apply to all classification levels and ILs. Any performance tiering options shall be explicitly identified in the Contractor's JWCC Catalog.	The Government will assess, via audit at the Government's discretion, whether the Contractor's storage and performance behavior characteristics at each classification level and IL, regardless of elastic growth, are commensurate with those of the Contractor's commercial offerings.	An automated report is generated at a parametrically established interval identifying the trends in industry for cloud capabilities and competitor (boutique, focused and general) comparisons.
173	5.5.7.3	The Contractor shall have more than one queryable storage JWCC Offering that can support data on the order of hundreds of Terabytes, intra-Availability Zones, and inter-Availability Zones. The Contractor shall provide at least one storage JWCC Offering that can perform create, read, update, and delete functions on data on the order of hundreds of Terabytes. Create, read, update, and delete operations at all classification levels and ILs shall be commensurate with the Contractor's Commercial Offerings.	The Government will assess, via audit at the Government's discretion, whether the Contractor's queryable storage and the performance behavior characteristics, at each classification level and IL, are commensurate with the Contractor's commercial offerings.	An automated report is generated at a parametrically established interval identifying the maximal storage capacity, by storage type (on-line, near-line, off-line, other) for each security domain. Additionally, the ability to support operations on the Petabyte scale.
174	5.5.7.4	The Contractor shall provide an API Gateway service that allows JWCC users the ability to develop, deploy, secure, manage, and scale the Government's APIs as needed.	The Government will assess whether the Contractor's API Gateway service provided to the Government allows for the ability to develop, deploy, secure, manage, and scale JWCC user-created APIs.	The ability to automatically recommend API parameters, configurations, and optimizations based on historical utilization, available connector

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				information, and industry best practices.
175	5.5.7.5	When an authorized user requests a cloud resource within the Contractor's Portal (UI), or via an API, the response time shall be commensurate with the Contractor's Commercial Offerings.	The Government will assess, via audit at the Government's discretion, whether the response time of each classification level and IL to determine the extent to which the cloud service offerings response times meet commercial parity.	Response times which are quicker than the average commercial response time.
176	5.5.7.6	The Contractor shall provide the ability to generate individual IaaS compute instances, for which the time required to go from stopped state (e.g. powered off) to receiving and processing user instructions (less any operating system boot time) for any individual IaaS compute instance shall be less than 10 seconds.	The Government will assess, via audit at the Government's discretion, whether the time until the IaaS compute instance is capable of processing user instructions at each classification level and IL is less than 10 seconds and commensurate with the Contractor's commercial offering.	The ability to start an instance inclusive of additional software load times (i.e. operating system boot time) which is less than 10 seconds.
177	5.5.8	Fortified Security: The Contractor must provide fortified security capabilities that enable enhanced cyber defenses for strong IAM and security from the application layer through the data layer. Fortified security capability requirements include continuous monitoring and auditing, automated threat identification, resilience and elasticity, encryption at rest and in transit, secure data transfer capabilities, and an operating environment that meets or exceeds DoD INFOSEC requirements. This security shall be tested regularly and include independent DoD testing, review, and audit.	Summary Requirement	N/A
178	5.5.8.1	The Contractor shall provide encryption and logical separation for any of the Contractor's CSOs available under the JWCC Contract, IAW C3PO and the following additional requirements:	Summary Requirement	N/A
179	5.5.8.1.1	The Contractor shall ensure that encryption appropriate to the applicable classification level or IL, for data at rest and in transit, is the default setting for all of the Contractor's CSOs available under the JWCC Contract such that the DoD can maintain confidentiality, as defined in the definitions, as the default configuration.	The Government will inspect any data at rest and in transit to ensure that the specified encryption requirements are IAW C3PO. Additionally the Government will assess service offerings to ensure that encryption is configured by default.	All data has multi-layer protection applied, while not impacting the performance profile of the operation.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
180	5.5.8.1.2	<p>The Contractor shall provide multi-layer encryption for all of the Contractor’s CSOs such that content, including any at-rest containers, shall remain encrypted until explicitly invoked via executable, and then once again be encrypted when operational processing is complete. The Contractor shall provide multi-layer encryption to maintain data confidentiality and support dual encryption such that it includes two or more independent layers of encryption. Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.</p>	<p>The Government will assess, via audit at the Government’s discretion, whether the Contractor’s documentation of multi-layer encryption methodology uses encryption algorithms and procedures as specified in C3PO.</p>	<p>All CSOs, including containers, have multi-layer protection applied which meets CSfC requirements and does not impact the performance profile of the operation.</p>
181	5.5.8.1.3	<p>The Contractor shall ensure that all of its CSOs available under the JWCC Contract, at all classification levels and ILs, provide the capability for DoD data to be encrypted at rest, with exclusive DoD control of encryption keys and key management, such that the DoD has the capability to cryptographically erase data, as defined in the definitions. The Contractor shall provide:</p> <ul style="list-style-type: none"> a. JWCC user-managed encryption keys; b. Encryption key management as a service; and c. Support for use of both Contractor-provided and Government-provided Hardware Security Modules (HSMs) (whether in-line, within the Contractor’s Cloud Environment, or externally located) for cryptographic operations. 	<p>The Government will assess, via audit at the Government’s discretion, whether the key management processes and tools provided by the Contractor are sufficient to ensure that any JWCC user is capable of administering and applying encryption keys independent of the Contractor. The Government will also assess JWCC user-managed encryption keys and cryptographic erasure by attempting to access data encrypted with a deleted key. The Government will assess whether the JWCC user has the capability to use HSMs.</p>	<p>Apply the most modern trusted levels of protection such that the fundamental Government requirement remains fully compliant and operable, with the additional protections applied in concert as a non-interfering or disruptive supplementation.</p>
182	5.5.8.2	<p>Cross-Domain Solution. The Contractor shall provide a CDS that provides secure and highly deterministic one-way data transfer capability between the Contractor’s logical enclaves and environments within the Contractor’s CSOs under the JWCC Contract, to external destinations, and across all classification levels, while limiting any threats. The Contractor shall minimally provide CDSs that supports low to high (from a lower impact/classification level to a higher impact/classification level) for both the Management Plane and production plan and high to low (from a higher impact/classification level to a lower impact/classification level) for the Production Plane, per sections 5.5.8.2.1 through 5.5.8.2.5 of this PWS.</p>	<p>Summary Requirement</p>	<p>N/A</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
183	5.5.8.2.1	All CDSs provided must be compliant with C3PO and the latest version of Cross-Domain Solution (CDS) Design and Implementation Requirements: 2020 Raise the Bar (RTB) Baseline Release (or current version) and achieve authorization by the DoD ISMRC.	The Government will assess whether the Contractor's provided CDS(s) are compliant with C3PO, 2020 Raise the Bar (RTB) Baseline Release. Additionally, the Government will assess whether the Contractor provides the DoD ISMRC a complete authorization package.	N/A
184	5.5.8.2.2	The CDS shall allow specific Government-controlled JWCC role-based accounts to overrule automated security measures to securely transfer information that may be flagged as malicious. This shall allow the specific Government-controlled JWCC role-based accounts-holders to accept risk as appropriate for flagged data transfers.	The Government will assess, via audit at the Government's discretion, whether the CDS, as authorized, allows for role-based accounts to overrule automated security measures.	All CDS offerings have a dynamic control panel with flow management to allow the Government to apply any exception actions in real-time.
185	5.5.8.2.3	The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the management plane to ensure the Contractor can securely migrate security updates to higher classification domains in a timely, consistent, repeatable, and secure manner, and maintain Commercial Parity.	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from low to high between all security domains and classification levels on the management plane.	The Contractor uses the CDS to ensure patching occurs at all levels within hours of release and to ensure service and feature parity through the use of their DevSecOps process.
186	5.5.8.2.4	The Contractor shall provide a CDS that supports data transfer from low to high between all classification levels and ILs on the production plane to support Government data transfer needs, including Development, Security, and Operations (DevSecOps).	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from low to high between all classification levels and ILs on the production plane prior to initial operations.	The CDS offerings support all data traffic regardless of the plane the information natively operates within (e.g. management plane, production plane, or other plane).
187	5.5.8.2.5	The Contractor shall provide a CDS that supports data transfer from high to low between all classification levels and ILs on the production plane to support Government data transfer needs.	The Government will verify whether the Contractor provided CDS(s), as authorized, allows data transfer from high to low between all classification levels on the production plane prior to initial operations.	The CDS offerings support all data traffic regardless of the plane the information natively operates within (e.g. management plane, production plane, or other plane).
188	5.5.8.3	The Contractor shall provide a secure data transfer capability for deterministic (maintaining integrity and predictable), authenticated, and encrypted, data transfers between the Contractor's logical enclaves and environments within its own cloud infrastructure and Offerings, to external destinations, including multi-environment peering gateways, and across all ILs within a classification level, while limiting any threats.	The Government will assess, via audit at the Government's discretion, whether the JWCC user(s) has the ability to securely transfer data to various endpoints both internal and external to the Contractor.	The capability will seamlessly interoperate with external destinations and dynamically determine the protection posture such that if acceptable it executes the requested process, otherwise it

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				provides a detailed exit report to the requesting user for potential remediation of the failed conditions and terminates the request while also allowing for a manual administrator override.
189	5.5.8.4	Authentication, Authorization, and IAM. With respect to authentication, authorization, and IAM the Contractor shall provide the following:	Summary Requirement	N/A
190	5.5.8.4.1	The Contractor shall provide customizable granularity for role-based, identity-based, attribute-based, access control (R-, I-, ABAC) policy configurations within a workspace, including workspace administration, provisioning of new cloud services, management of existing services, and the ability to assign permissions to Contractor pre-defined and allow for the creation and assignment of JWCC user specified roles.	The Government will assess, via audit at the Government's discretion, whether granular control access is available for I-, R-, ABAC (collectively referred to as PBAC) across all services, users, data and resources.	All cloud actions are fully controlled under an exhaustive PBAC model.
191	5.5.8.4.2	The Contractor shall provide non-repudiation and user-identity confirmation providing the ability to securely verify user identity, including Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI), at all classification levels and ILs pursuant to requirements in C3PO, the CC SRG, and the authorization for each of the Contractor's CSOs under the JWCC Contract.	The Government will assess, via audit at the Government's discretion, whether all users have non-repudiable identities, as well as whether any user exists without identity credentials. The Government will also assess the ability to create users who utilize MFA and PKI at all classification levels and ILs pursuant to the requirements in C3PO and the CC SRG.	The capability denies all actions attempted by a non-authoritatively identified non-repudiable role, and immediately establishes a notification of such an attempt to the appropriate reporting manager (Human, non-human actor).
192	5.5.8.4.3	The Contractor shall provide the ability to generate and issue time-limited, role-based authentication tokens that will allow a JWCC user to assume a set of attributes, roles, or a combination thereof within a specific workspace, the Cloud Environment, or a combination thereof.	The Government will assess, via audit at the Government's discretion, the ability for a JWCC user to establish and use time-limited, role-based authentication tokens within a specific workspace.	The capability will support temporally programmable PBAC (all dimensions, e.g. I-R-ABAC) credentials.
193	5.5.8.4.4	The Contractor's CSOs shall support modern authentication protocols and methods (e.g. Security Assertion Markup Language (SAML), Open Authorization (OAuth), Fast Identity Online (FIDO2)) such that the Government can integrate/use Federated Identity solutions with the Contractor's CSOs under the JWCC Contract at each classification level and IL.	The Government will assess, via audit at the Government's discretion, whether the Contractor can associate a DoD provided identity to a user within the Contractor's cloud service using modern authentication protocols and methods.	The capability will support all future emerging authentication protocols, while maintaining a fully backward compatible operations posture.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
194	5.5.8.5	Automated INFOSEC and Access Control. In conjunction with the requirements established in C3PO, the Contractor shall provide automated tools for INFOSEC and access control with the attributes described below:	Summary Requirement	N/A
195	5.5.8.5.1	The Contractor shall provide the capability for the Government to audit both the physical location and logical separation, as defined in C3PO, of any CSO and Government data, at each classification level and IL, to ensure compliance with C3PO.	The Government will assess, via audit at the Government's discretion, whether the Contractor has provided sufficient tools that provide the Government the ability to obtain accurate information regarding the physical location and the logical isolation of selected host services to ensure compliance with C3PO. Optionally the Government will audit the physical location.	The capability will have a persistent mapping of all service physical locations and the specific logical isolation/partitioning that is applied. Additionally visualization tools which support the audit and are able to be dynamically scoped are available for the users/auditors to document and use as part of the audit process.
196	5.5.8.5.2	The Contractor shall provide automated tools for breach identification, notification, and remediation, to support breach and incident response requirements described in C3PO.	The Government will audit whether the Contractor has provided automated identification, notification, and remediation tools to allow the JWCC user fulfill incident response requirements.	A fully automated programmable breach detection and remediation capability to allow for routine response protocols that optionally utilizes AI/ML services to predict and respond to breaches.
197	5.5.8.5.3	The Contractor shall provide Self-Service and automated tools for handling data spills of CLASSIFIED or other controlled information, at each classification level and IL, to support data spillage activities as described in DoDM 5200.01 and C3PO.	The Government will test the capability at its discretion to assess whether its performance supports data spillage remediation and incident reporting requirements.	A capability to auto alert and notify a designated authority of a potential cloud-based data spillage and provide the ability to suspend the offending action, user, or any combination thereof.
198	5.5.8.5.4	The Contractor shall provide self-service tools, at each classification level and IL, to allow JWCC users to access data and analysis generated by threat detection systems so that JWCC customers, DoD cybersecurity investigators and auditors, including contractor staff serving in those capacities, can review, assess, protect, and defend their deployed and provisioned CSOs.	The Government will assess whether the self-service tools can support the capability to review, assess, protect, and defend deployed/provisioned CSOs as described in C3PO at each classification level and IL.	An automated capability to assess the threat surfaces and exposure points in the cloud environment and present a systematic analysis that can be either programmatically processed or inspected

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
				and reviewed by humans.
199	5.5.8.5.5	The Contractor shall provide identification and notification of threats to JWCC users and system owners immediately upon discovery, to support incident response tasks as described in C3PO.	The Government will assess whether the Contractor provides identification and notification of threats immediately upon discovery.	An automated capability to present viable remediation techniques to any identified threat for user action or configuration for automated remediation.
200	5.5.9	Advanced Data Analytics. The Contractor shall provide advanced data analytics CSOs, as minimally outlined herein and below, that securely enable data-driven and improved decision making at the strategic level (across security domains) to the TE (within a single security domain). The Contractor shall provide advanced data analytics CSOs that support batch and streaming analytics, predictive analytics, and AI/ML. Advanced data analytics CSOs shall be available at all classification levels and ILs, extensible to the TE, to include DDIL environments and on multiple disparate datasets. Advanced data analytics CSOs shall, at a minimum, be able to import, process, and export streaming and batch data in common data formats.	Summary Requirement	N/A
201	5.5.9.1	The Contractor shall provide data analytics CSO's (e.g., streaming analytics, predictive analytics, and AI/ML).	Summary Requirement	N/A
202	5.5.9.1.1	The Contractor shall provide data analytics JWCC Offerings capable of operating at all classifications and ILs, and on TE Devices, such that operators can label data, train and develop models, and use model/algorithm outputs in mission relevant environments with mission relevant data, commensurate with the JWCC timeline (5.5.1, above). Exceptions to this requirement must be submitted IAW JWCC Exception Request (CDRL A024) and subsequently approved by the JWCC KO.	The Government will assess whether the Contractor has provided data analytics offering capable of operating at all classifications and ILs and TE Devices, less the exceptions approved by the KO, and commensurate with the JWCC schedule ref 5.5.1.	A fully equipped AI/ML, and other analytic learning tools, suite of tools, platforms, or any combination thereof, to allow advanced processing of data for insight and findings. All tools are also available at the tactical edge in connected and disconnected modes.
203	5.5.9.1.2	The Contractor's advanced data analytics CSOs shall be capable of operating across multiple datasets in disparate workspaces to allow for information sharing and learning across multiple DoD Components/Agencies.	The Government will assess, via audit at the Government's discretion, whether the Contractor has provided advanced data analytics	A capability to identify all compatible data sets and the specific aligned "data items" (e.g.: data engineering and

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
			offerings capable of operating across data centers in disparate workspaces by linking multiple disparate data sources (from one or more workspaces) to a single workspace and executing a simple AI/ML pipeline.	normalization) across the JWCC data universe. Additionally capabilities which aid data wrangling and suggest likely mappings between disparate data sets for accelerated analysis.
204	5.5.9.1.3	The Contractor shall provide advanced data analytics CSOs able to fully operate with or without network connectivity and in DDIL environments, such that TE Devices shall be capable of continued data analytics activities (including AI/ML) when network connectivity is contested, congested, or unavailable, commensurate with the JWCC timeline (5.5.1, above).	The Government will assess, commensurate with the device's availability under the JWCC schedule (ref. 5.5.1), whether TE Devices have data analytics capabilities (including AI/ML) in varying states of connectivity (e.g., contested, congested, or unavailable). The Government may, at its sole discretion, assess continued capability at any time.	A complete cloud stack that can operate in a small footprint TE Device that is in a DDIL mode.
205	5.5.9.1.4	The Contractor's data analytics JWCC Offerings shall be capable of supporting data import and export in common formats (at minimum these formats shall include CSV, JSON, XML, and streaming data).	The Government will assess, via audit at the Government's discretion, whether the Contractor has met this requirement by using sample data in multiple formats in the Contractor's data analytics offerings. The Contractor's tools will be assessed for data integrity inclusive of the consistency of output of the data structure and content.	A mediated adapter capability that can autosense, or be programmatically patterned, to allow unknown (no prior exposure) data structures and formats to be consumed.
206	5.5.10	Tactical Edge. The Contractor shall provide TE Offerings and TE Devices across the range of military operations while balancing portability, capability, and cost. TE Devices shall operate seamlessly across network connectivity levels, including DDIL environments, at all classification levels and ILs IAW C3PO.	Summary Requirement	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
207	5.5.10.1	<p>The Contractor shall provide, as a JWCC Offering, a minimum of one form factor of TE Devices that is man-portable and is capable of being carried by an individual(s), mounted to a vehicle, or both, which the Contractor will have certified as meeting MIL-STD-810H (Environmental Engineering Considerations and Laboratory Tests), such that the form factor of TE Devices enables the use of JWCC resources across the range of military operations (e.g. deployable afloat, aloft, ashore, and globally). This form factor of TE Devices shall be authorized to host data at each classification level and IL.</p>	<p>The Government will assess whether a man-portable TE Device form factor is certified as meeting MIL-STD-810H, is capable of being carried and mounted to a vehicle and is authorized to host data at each (or up to all) classification levels and ILs. The Government will test the TE Devices at its discretion.</p>	<p>A diverse range of MIL-STD-810H TE footprints such as: lightweight (tablet or smaller), highly portable (laptop), small portable (desktop or small luggable 1-person carry) server, moderate non-portable (2+ person movable) server, large human-machine assisted portable (mini, mainframe, vehicle mounted, or facility located), and huge machine (e.g. semi-truck or large container vehicle movable data center).</p>
208	5.5.10.2	<p>The Contractor shall provide a modular, rapidly deployable data center that can be connected to Government-provided power, connected to Government-provided networking uplinks when available, use Government transportation, and be deployed on U.S. soil, CONUS or OCONUS, or on Government-owned platforms (e.g. aircraft carriers, maritime operations center, airfields, and division headquarters). The deployable data center shall be authorized to host data at each classification level and IL and up to all classification levels and ILs following the physical and logical separation requirements in C3PO.</p>	<p>The Government will assess whether the modular, rapidly deployable data center is authorized to host data at each classification level and IL, or at all classification levels and ILs in relevant mission environments. The data center will be demonstrated to the Government for acceptance and the Government will test it at its discretion.</p>	<p>A configurator tool is available to generate a known working configuration of a rapidly deployable data center, to include past configuration options and non-existing assemblies that are guaranteed to work.</p>
209	5.5.10.3	<p>The Contractor's TE Offerings shall function in DDIL environments as if connected, with the only features and functionality missing being those that rely on real time interconnection services. TE Offerings shall include the ability to configure and manage any CSO deployed or provisioned on or to the TE Device, and operate using local resources.</p>	<p>The Government will test the TE computing and storage functionality in simulated DDIL environments, at its discretion, to ensure the ability to configure and manage any provisioned CSOs and operate using local resources (e.g., local virtual machines and or containers should continue to operate).</p>	<p>The TE Devices are capable of modular adapter components that can be hot swapped to dynamically change the available service sets for the configuration.</p>
210	5.5.10.4	<p>The Contractor's TE Offerings shall be configurable such that a JWCC user can configure the parameters for synchronization with Contractor-provided services. These parameters shall, at a minimum, include automated or manual, bidirectional or unidirectional synchronization options, the ability to control synchronization priority order, and the ability to</p>	<p>The Government will assess, via audit at the Government's discretion, whether the TE Devices meet the minimum parameters for synchronization to include automated or manual, bidirectional or unidirectional, synchronization options, the</p>	<p>The TE Devices are equipped with programmatic sensing capability that can be threshold triggered to perform synchronization based on complex parametric and</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
		throttle use of available bandwidth for synchronization.	ability to control synchronization priority order and throttle use of available synchronization bandwidth for synchronization.	algorithmic situations. (e.g. all network traffic is idle and operational exposure is not a consideration).
211	5.5.10.5	The Contractor shall provide TE Device and component signature specifications for Electromagnetic (EM), acoustic, thermal, and any other device specific emanations in all operational states to enable the Government to control the magnitude of these signatures (TE Device Specifications, CDRL A017).	The Government will assess whether the Contractor provided TE Device signature data is sufficient and complete. The Government reserves the right to verify the signature specifications against device testing.	The TE Devices will have componentry that can auto generate complete device signature data and can further control, augment, or any combination thereof, the signature to lowered states without significant impact to performance.
212	5.5.10.6	The Contractor's TE Offerings shall follow the cybersecurity requirements defined in C3PO.	The Government will assess, at its discretion, whether TE offerings and devices meet conformance requirements in C3PO.	The TE Devices will exceed one or more of C3PO requirements.
213	5.5.10.7	The Contractor's TE Offerings shall be capable of both in-band and out-of-band configuration and maintenance for all TE Devices.	The Government will assess whether the TE solutions ability to perform both in-band maintenance and whether the materials are provided for the Government to perform out-of-band configuration and maintenance capabilities without the Contractor's intervention.	All TE configuration and maintenance activities are fully available both in-band and out-of-band.
214	5.5.10.8	The Contractor's TE Offerings shall support cryptographic key management, IAW Section 5.5.8.1.3 and C3PO, both on and off the TE Device, at the user's discretion.	The Government will assess tactical edge solutions conformance to support of key management, IAW C3PO, both on and off the device at the discretion of the user will be tested.	N/A
215	5.5.10.9	The Contractor shall provide delivery of TE Devices to CONUS locations only and allow for the Government to pick up TE Device(s) at a Contractor facility in CONUS. Locations for pickup and any services and fees associated with delivery may shall be separately identified and priced in the JWCC Catalog.	TE Devices delivered to CONUS locations, and IAW services and fees in the relevant catalog or available for pick up at the defined Contractor's facility.	N/A

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
216	5.5.10.10	The Contractor shall submit authorization packages for the first unit of all variations of TE Devices for Authorization at each classification level and IL.	The Government will assess the current state of the TE Device authorization. Any TE Devices and services that have not been previously authorized must include all documentation required for the AO to authorize the device(s)/CSO(s) for use.	All TE Devices are pre-qualified with a full authorization, including the first delivery item.
217	5.5.10.11	For each TE Device the Contractor will offer in the JWCC Catalog, the Contractor shall provide to the JWCC PMO a sample of each TE Device per classification level and IL, with the associated authorization package, such that the Government can perform verification and validation of the device(s) prior to official acceptance as part of the JWCC Catalog. Upon completion of testing, the Government will either order the appropriate TE Offerings(s) from the JWCC Catalog or return all sample TE Devices from the test.	The Government will receive each TE Device submitted, conduct DoD authorization activities. Upon completion of testing, the Government will either order the appropriate TE offering(s) from the JWCC Catalog or return all sample TE Devices from the test.	All TE Devices are pre-qualified with a full authorization, including the first delivery item. This may require pre-coordination with the Government prior to the first order.
218	5.5.10.12	When TE Devices are returned to the Contractor, the Contractor shall either dispose of the TE Device IAW the CC SRG and the Attachment J-3: JWCC DD254 or follow the procedures and requirements in C3PO for reuse.	The Government will assess the Contractor's ability to dispose of or, wipe and reconfigure TE Devices and to audit management controls surrounding these practices.	N/A
219	5.5.11	Advisory and Assistance Services. The Contractor shall provide advisory and assistance services under the Cloud Support Package CLINs in the JWCC Contract to advise and assist with cloud architecture, usage, optimization, provisioning, and configuration for all JWCC Offerings, including TE Offerings. Cloud Support Packages shall encompass, but not be limited to, advisory and assistance services, help desk services, training, and documentation support. Cloud Support Packages shall be available for all JWCC Offerings at all classification levels and ILs.	Summary Requirement	N/A
220	5.5.11.1	The Contractor shall provide advisory and assistance services that include integration, aggregation, orchestration, secure design, and troubleshooting of JWCC Offerings and can be applied to all classification levels and ILs.	The Government will assess whether the offered advisory and assistance services ensure coverage of all the Contractor's offered cloud services under the JWCC Contract, inclusive of TE Devices. The Government will assess whether the available advisory and assistance packages can be applied to all security domains, and at each classification and IL and meet the security requirements of the DD254.	All advisory and assistance support packages are equivalent for all security domains, and classification levels and ILs.

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
221	5.5.11.2	<p>The Contractor shall provide training materials and make training available for all of the CSOs on the JWCC Catalog at all classification levels and ILs. Separate training and documentation are required for TE Offerings. The Contractor shall include, at a minimum:</p> <ul style="list-style-type: none"> a. Training materials and training for all CSOs provided on the JWCC Catalog at all classification levels and ILs. b. Materials that help users and administrators understand how to successfully provision services and employ best practices for JWCC Offerings. Users and administrators shall be able to retain such materials upon completion of the training (CDRLs A004 and A005). c. Separate training and training materials shall be provided for each TE Offering, inclusive of supportability training (e.g. end user maintenance, packaging, handling, storage and transportation, infrastructure requirements), at all classification levels and ILs. d. Any training the Contractor provides shall demonstrate, through tabulated results, the relevance, thoroughness, and efficacy of the training using industry standard methods and tools. e. All training materials shall be current and the Contractor shall provide updated training materials with the release of new versions of any CSO that is made available to JWCC users. 	<p>The Government will assess whether the offered training and associated materials meet the following criteria:</p> <p>applicability and thoroughness for each service at all classification levels and ILs, including tactical edge.</p> <p>Provide tabulated results on relevance, thoroughness, and efficacy of training.</p>	<p>All training materials are equivalent between security domains, and classification levels and ILs and are fully comprehensive in content.</p>
222	5.5.11.3	<p>If a Cloud Support Package is constrained by the number of hours available to users, the Contractor shall provide a Self-Service mechanism for users to quickly determine how many hours of the available support package have been consumed.</p>	<p>The Government will assess whether the Cloud Support Package services available under the Cloud Support Package line items on the contract for every service offering. The Government will also assess whether the Contractor provides a self-service resource to determine remaining hours on time constrained services.</p>	<p>The advisory and assistance services include multi-vendor interoperability solutioning.</p>
223	5.5.11.4	<p>The Contractor shall provide, as part of the JWCC Catalog, separate options for in-person and remote instructor-led training and support services provided by the Contractor in CONUS and OCONUS locations. All training and support services shall be offered at the locations as described in the JWCC Offering or as required by the TO.</p>	<p>The Government will assess whether the JWCC Catalog for in-person and remote instructor-led training and support services in CONUS are listed independently from those catalog items for training and support services in OCONUS locations.</p>	<p>N/A</p>

Item	PWS Citation	Performance Requirement	Minimum Acceptable Quality Level	Performance Objective
224	5.5.11.5	The Contractor shall provide, as part of the JWCC Catalog, an option for self-paced training.	The Government will assess whether the JWCC catalog has an item for self-paced training.	N/A
225	5.5.11.6	The Contractor shall provide options for equipment repair/replacement and data recovery from TE Device failure or performance degradation, with minimal mission impact, such as the ability to replace failed hardware at the unit level or full TE Device in a manner that is appropriate for the form factor of the device and range of impacted military operations and best effort data recovery.	The Government will evaluate whether the Contractor's offered services under the JWCC Contract include TE data recovery and equipment repair/replacement options.	An immediate replacement/recovery model for TE Devices has no impact on mission operations.

TECHNICAL EXHIBIT 2
DELIVERABLES SCHEDULE

CDRL	Deliverable Name
A001	Contract Monthly Progress Report
A002	Contractor Cloud Portal Process
A003	Contract Security Management Plan
A004	System Administrator Training Material
A005	Role-Based User Training Material
A006	Portability Plan
A007	Contract Ordering Guide Annex
A008	Quality Control Plan
A009	Security Authorization Package
A010	Small Business Reporting
A011	RESERVED
A012	Task Order Monthly Progress Report
A013	Meeting Materials
A014	System and Organization Control (SOC) Audit Reporting
A015	GFP Reporting

A016	JWCC Marketplace Security Practices
A017	Tactical Edge Device Specifications
A018	Lifecycle Management Plan
A019	Roadmap/Integrated Master Timeline
A020	Quarterly Progress Report for Decentralized Ordering
A021	Contractor Program Management Plan
A022	JWCC Catalog with Change Report
A023	Commercial Catalog with Change Report
A024	JWCC Exceptions

Attachment J-11

Account Tracking and Automation Tool (ATAT) Multi-Cloud Provisioning Application
Programming Interface (API)

The ATAT API (v0.1.0) can be found at https://github.com/dod-ccpo/atat-csp-orchestration/blob/main/provisioning/atat_provisioning.yaml. Note that it is subject to the Government's change control process at any time prior to the JWCC Award Date, after which it will be finalized at v1.0.0. Following this, future modifications will be subject to a change control process.

Attachment L-1

**Joint Warfighting Cloud Capability (JWCC)
SUBCONTRACTING PLAN FORMAT**
Updated September 30, 2021

Solicitation or Contract Number:	
Contractor:	Address:
Approximate Contract Value: \$	

() Individual Plan () Master Plan () Commercial Plan

This plan follows the format for addressing the eleven elements as shown at Federal Acquisition Regulation (FAR) 52.219-9(d). Please be sure to address all eleven elements.

(1) – GOALS

State the percentage of total planned subcontracting dollars that will go to all Small Business (SB) concerns, Historically Underutilized Business Zone (HUBZone) SB concerns, Small Disadvantaged Business (SDB) concerns, Woman-Owned SB (WOSB) concerns, Veteran-Owned SB (VOSB) concerns, and Service-Disabled Veteran-Owned SB (SDVOSB) concerns.

NOTE: For contracts containing options, the percentage goals and dollars must be shown separately for EACH year.

All subcontracts that contribute to contract performance must be included, and a proportionate share of products and services that are normally allocated as indirect costs may be included.

Subcontracts awarded to an Alaska Native Corporation (ANC) or Indian tribe must be counted towards the subcontracting goals for SB and SDB concerns, regardless of the size or Small Business Administration (SBA) certification status of the ANC or Indian tribe.

Category	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5
SB*	%	%	%	%	%
HUBZone SB	%	%	%	%	%
SDB**	%	%	%	%	%
WOSB	%	%	%	%	%
VOSB	%	%	%	%	%
SDVOSB	%	%	%	%	%

(2) – STATEMENT OF DOLLARS

The following dollar values correspond to the percentage goals in (1).

Category	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5
Total contract value	\$	\$	\$	\$	\$
Total planned subcontracting dollars	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to SB*	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to HUBZone SB	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to SDB**	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to WOSB	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to VOSB	\$	\$	\$	\$	\$
Dollars planned to be subcontracted to SDVOSB	\$	\$	\$	\$	\$

_____ Subcontracting opportunities exist for Historically Black Colleges and Universities (HBCUs) and Minority Institutions (MIs)

_____ Subcontracting opportunities do not exist for HBCUs and MIs

(3) – DESCRIPTION OF PRINCIPAL TYPES OF SUPPLIES AND SERVICES TO BE SUBCONTRACTED AND TYPES OF BUSINESSES SUPPLYING THEM (Check all that apply)

<u>PRINCIPAL SUPPLY/SERVICE</u>	<u>SB*</u>	<u>HUB Zone SB</u>	<u>SDB**</u>	<u>WOSB</u>	<u>VOSB</u>	<u>SDVOSB</u>

(4) – METHOD USED TO DEVELOP GOALS

Explain how you arrived at your percentage goals and dollars for subcontracting to SB, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB.

(5) – METHOD USED TO IDENTIFY POTENTIAL SUBCONTRACTING SOURCES (Check all that apply)

- System for Award Management (SAM) database
- Company Source Lists.
- Veteran Service Organizations
- National Minority Purchasing Council Vendor Information Service.
- U.S. Department of Commerce Minority Business Development Agency’s Research and Information Service.

_____ SB, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB Service/Trade Associations.

_____ SBA's Lists of Certified SDB and HSB Concerns.

_____ SB and Minority Business trade fairs or conferences

_____ Other: Explain –

(6) – INDIRECT COSTS (Check which applies.)

_____ Indirect costs ***have not*** been included in establishing subcontracting goals.

_____ Indirect costs ***have*** been included in establishing subcontracting goals.

If included, describe how you determine the proportionate share of indirect costs incurred with:

SB*: _____

HUBZone SB: _____

SDB***: _____

WOSB: _____

VOSB: _____

SDVOSB: _____

(7) – ADMINISTRATION OF SUBCONTRACTING PROGRAM

The following individual employed by the offeror will administer this subcontracting plan:

Name: _____ Title: _____

Telephone: _____ Address: _____

Email: _____

Description of Duties _____

(8) – EQUITABLE OPPORTUNITY TO COMPETE (Check which apply.)

Describe your efforts to ensure that SB, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB will have an equitable opportunity to compete for subcontracts. These efforts include, but are not limited to, the following activities:

Outreach Efforts to Obtain Sources:

- Contacting minority and small business service and trade associations
- Contacting business development organizations
- Attending small and minority business procurement conferences and trade fairs
- Using SAM database to research sources
- Other: Explain -

Internal Efforts to Guide and Encourage Purchasing Personnel:

- Presenting workshops, seminars, and training programs
- Establishing, maintaining, and using SB, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB source lists, guides, and other data for soliciting subcontracts
- Other: Explain -

(9) – INCLUSION OF FAR CLAUSE 52.219-8, “UTILIZATION OF SMALL BUSINESS CONCERNS,” IN SUBCONTRACTS

Place a check by each statement as assurance that the following will be done:

- I agree to include FAR Clause 52.219-8, “Utilization of Small Business Concerns,” in all subcontracts that offer further subcontracting opportunities.
- I will require all subcontractors (except SB concerns) that receive subcontracts in excess of \$550,000 to adopt a subcontracting plan similar to this one that complies with the eleven elements in FAR 52.219-9.

(10) – REQUIREMENT TO COOPERATE IN STUDIES AND SUBMISSION OF REPORTS

Place a check by each statement as assurance that the following will be done:

- I agree to cooperate in any studies or surveys as may be required.
- I agree to submit periodic reports so the government can determine the extent of compliance with the subcontracting plan.
- I agree to submit the Individual Subcontract Report (ISR) and/or the Summary Subcontract Report (SSR), in accordance with paragraph 1 of the clause at FAR 52.219-9 using the Electronic Subcontracting Reporting System (eSRS) at <http://www.esrs.gov>. The reports will provide information on subcontract awards to SB concerns (including ANCs and Indian tribes that are not SBs), VOSB concerns, SDVOSB concerns, HUBZone SB concerns, SDB concerns (including ANCs and Indian tribes that have not been certified by SBA as SDBs), WOSB concerns, and HICUs and MIs. Reporting will be in accordance with the clause at FAR 52.219-9, or as provided in agency regulations.
- I agree to ensure that my subcontractors with subcontracting plans agree to submit the ISR and/or the SSR using eSRS.
- I will provide this prime contract number, its DUNS number, and the e-mail address of our company official responsible for acknowledging receipt of or rejecting the ISRs, to all first-tier subcontractors with subcontracting plans so they can enter this information into the eSRS when submitting their ISRs.
- I will require that each subcontractor with a subcontracting plan provide the prime contract number, its own DUNS number, and the e-mail address of the subcontractor’s official responsible for acknowledging receipt of or rejecting the ISRs, to its subcontractors with subcontracting plans.

(11) – DESCRIPTION OF TYPES OF RECORDS TO BE MAINTAINED (Check if in agreement)

- I agree to maintain the records such as the following to show with this subcontracting plan (see 19.704(a)(11):
 - a. Source lists, guides, and other data that identify SB, HUBZone SB, SDB, WOSB, VOSB and SDVOSB concerns.
 - b. Records on organizations contacted to locate SB, HUBZone SB, SDB, WOSB, VOSB and SDVOSB sources.
 - c. Records on each subcontract solicitation resulting in an award of more than \$100,000, indicating
 - (1) Whether SB concerns were solicited and, if not, why not.
 - (2) Whether HUBZone SB concerns were solicited and, if not, why not.

- (3) Whether SDB concerns were solicited and, if not, why not.
 - (4) Whether WOSB concerns were solicited and, if not, why not.
 - (5) Whether VOSB concerns were solicited and, if not, why not.
 - (6) Whether SDVOSB concerns were solicited and, if not, why not.
 - (7) If applicable, the reason award was not made to a SB, HUBZone SB, SDB, WOSB, VOSB, or SDVOSB concern.
- d. Records of outreach efforts to contact:
- (1) Trade/service associations.
 - (2) Business development organizations.
 - (3) Conferences and trade fairs to locate SB, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB sources.
- e. Records of internal guidance and encouragement provided to buyers through:
- (1) Workshops, seminars, training, etc.
 - (2) Monitoring performance to evaluate compliance with the program's requirements.
- f. On a contract-by-contract basis, records to support award data submitted to the government, including the name, address, and business size of each subcontractor.

(12) – ASSURANCES OFFEROR WILL MAKE GOOD FAITH EFFORT TO USE THE SMALL BUSINESS OFFERORS USED IN PREPARING BID OR PROPOSAL

Assurances that the offeror will make a good faith effort to acquire articles, equipment, supplies, services, or materials, or obtain the performance of construction work from the small business concerns that the offeror used in preparing the bid or proposal, in the same or greater scope, amount, and quality used in preparing and submitting the bid or proposal. Responding to a request for a quote does not constitute use in preparing a bid or proposal. An offeror used a small business concern in preparing the bid or proposal if--

- (i) The offeror identifies the small business concern as a subcontractor in the bid or proposal or associated small business subcontracting plan, to furnish certain supplies or perform a portion of the contract; or
- (ii) The offeror used the small business concern's pricing or cost information or technical expertise in preparing the bid or proposal, where there is written evidence of an intent or understanding that the small business concern will be awarded a subcontract for the related work if the offeror is awarded the contract;

(13) – Assurances that the contractor will provide the contracting officer with a written explanation if the contractor fails to acquire articles, equipment, supplies, services or materials or obtain the performance of construction work

as described in (12) of this section. This written explanation will be submitted to the contracting officer within 30 days of contract completion.

(14) – Assurances that the contractor will not prohibit a subcontractor from discussing with the contracting officer any material matter pertaining to payment to or utilization of a subcontractor;

(15) Assurances that the offeror will pay its small business subcontractors on time and in accordance with the terms and conditions of the subcontract, and notify the contracting officer if the offeror pays a reduced or an untimely payment to a small business subcontractor (see [52.242-5](#)).

This subcontracting plan was prepared by:

Signature: _____

Printed name: _____

Title: _____

Phone number: _____

Date prepared: _____

* Includes ANCs, Indian tribes, HUBZone SB, SDB, WOSB, VOSB, and SDVOSB when applicable.

** Includes ANCs and Indian tribes.

(End Plan)

Attachment L-2

**Organizational Conflicts of Interest
(OCI) ANALYSIS/ DISCLOSURE FORM**

1. Contract/Task Order Number	2. Program Title	
3. Contractor Name and Address		4. Telephone Number and POC
5. Type of work to be performed under this agreement:		
Other Professional Services - related work requiring analysis and determination:	6. Contract Number and Program Title	
7. Brief Summary/ Description of work performed under Block 6 action:		
8. Relationship between requirements of Block 1 action and work performed under Block 6 action (If None, State Why):		
9. Offeror/Contractor OCI Evaluation and Assessment (If either answer is yes, attach a copy of the SOW and complete Block 10): (a) Does Actual OCI exist? () Yes () No (b) Does Potential OCI exist? () Yes () No		
10. Summary of actual/potential OCI, including actions planned to avoid, neutralize, or mitigate conflict or potential conflict:		
11. Typed Name of Responsible Official	12. Signature	13. Date
14. Typed Name of Contracting Officer	15. Approval Signature	16. Date

INSTRUCTIONS FOR COMPLETING OCI ANALYSIS/ DISCLOSURE FORM

Blocks 1 through 5: Self explanatory

Block 6: Fill in the number and the short, official title by which the contract or subcontract requiring analysis and determination is formally known. This is work that has already been awarded, is being performed by your company, and requires a comparison with the work described in Blocks 1 – 5.

NOTE: One OCI Analysis/ Disclosure Form shall be submitted for EACH related contract or subcontract currently being performed.

Block 7: Provide a brief, but specific, narrative summary of the SOW and work performed on the contract or subcontract listed in Block 6, including the period of performance and the value.

Block 8: Provide a brief, but specific, narrative summary of ANY relationship between the work to be performed under the action listed in Block 1 and the previous work performed under the action listed in Block 6. Please be as specific as possible by citing the specific RFP/SOW paragraph where possible.

Block 9: Place an “X” in the appropriate () for your responses.

Block 10: If you answer yes to either 9(a) or to 9(b), provide a summary of the actual or potential OCI.

Blocks 11, 12, and 13: Provide the name of your company official with the responsibility for and/or authority to discuss and commit the company on matters related to OCI issues. That official should then sign and date each form.

Attachment L-4

**COMPANY NON-DISCLOSURE AGREEMENT FOR
THE JOINT WARFIGHTING CLOUD CAPABILITY(JWCC)**

This Non-Disclosure Agreement is signed by _____ a duly authorized officer of _____ (Potential Offeror) with authority to obligate Potential Offeror to this Agreement.

Upon signing this agreement, Potential Offeror will be granted access to nonpublic information, specifically documents identified in Request for Proposal (RFP) HQ003421R0327, that are marked CONTROLLED UNCLASSIFIED INFORMATION (CUI), Potential Offeror agrees that it will not use or disclose any such information to anyone other than its personnel. Potential Offeror further agrees that Potential Offeror will use its best efforts to ensure that Potential Offeror personnel and others that are participating in the preparation of a proposal in response to the RFP, will not use or disclose any such nonpublic information unless authorized by the DoD.

CERTIFICATE OF NONDISCLOSURE

Non-Disclosure Obligations

I, **(Individual Name)**, am a duly authorized officer of _____ (hereinafter "Potential Offeror"), an authorized representative of the Potential Offeror who has indicated in writing that it intends to submit a proposal in response to RFP HQ003421R0327, for Joint Warfighting Cloud Capability for the Department of Defense (DoD). Potential Offeror is not obligated to submit a proposal; but does agree to the following:

WHEREAS it is the intention of DoD/WHS to protect and prevent access to and disclosure of nonpublic information, specifically documents marked CONTROLLED UNCLASSIFIED INFORMATION(CUI), to anyone other than employees of the United States Government and others who have a need to know, unless so authorized in writing by the DoD; and

WHEREAS DOD/WHS acknowledges that Potential Offeror (and its designees) will require access to such nonpublic information in order to submit a proposal in response to RFP; and

WHEREAS CUI information must be handled in a manner that provides assurance that unauthorized persons do not gain access,

NOW THEREFORE, Potential Offeror agrees as follows:

- a. Potential Offeror shall not seek access to nonpublic information beyond what is identified in the RFP;

Attachment L-4

- b. As to any nonpublic information to which Potential Offeror has or is given access pursuant to this agreement, c; and
- c. If Potential Offeror becomes aware of any improper release, use or disclosure of such nonpublic information, Potential Offeror shall advise the DoD/WHs in writing as soon as possible.
- d. The Potential Offeror further agrees to properly store any nonpublic information given to Potential Offeror pursuant to this agreement until destruction is required. Destruction/deletion of any files and/or physical copies of documents containing nonpublic information given to Potential offeror pursuant to this agreement shall occur upon the earlier of: 1. the due date for submission of Proposals identified in the RFP if Potential Offeror does not submit a proposal, or 2. the date of notification of awardee of the JWCC contract if Potential Offeror submits a proposal.
- e. Potential Offeror will ensure that its designees also agree to paragraph 4 of this agreement prior to sharing any nonpublic information to which Potential Offeror has or is given access pursuant to this agreement.
- f. Potential Offeror understands that any unauthorized use, release or disclosure of nonpublic information in violation of this Non-Disclosure Agreement will subject Potential Offeror to administrative, civil or criminal remedies, as may be authorized by law.
- g. The provisions of this Agreement also are consistent with and do not supersede, conflict with, or otherwise alter the Potential Offeror 's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

Potential Offeror: _____ DATE: _____

By: _____

(Signature)

PRINTED NAME: _____

TITLE: _____

Attachment L-7

Small Business Participation Commitment Document (SBPCD)

1. Prime Contractor Size:

Indicate the applicable size and socioeconomic categories -- all that apply:

- { } Other than Small Business
- { } Small Business
 - { } Small Disadvantaged Business (SDB)
 - { } Woman-Owned Small Business (WOSB)
 - { } Historically Underutilized Business Zone (HUBZone) Small Business
 - { } Veteran-Owned Small Business
 - { } Service Disabled Veteran Owned Small Business (SDVOSB)

2. Minimum Quantitative Requirement (MQR) -- Participation of Small Businesses*

**Small Business Participation, reporting applies*

For the JWCC Contract, the Contractor is allowed to accrue small business participation across all Task Orders placed against all CLINs in aggregate within an established reporting period. However, the participation accrual shall not overlap (double count) participation across reporting periods, nor shall any single reporting period exceed 365 calendar days. For every \$1,000,000.00 expended ordered, with no less than 1% accrued spent from all Task Orders placed against under-all Contract Line Item Numbers shall be directed towards small business participation goals throughout the life of the IDIQ contract, as identified below. In execution, the JWCC Contracting Officer will determine whether the Contractor has met the small business participation goals identified below based on the actual value of all orders placed annually. If the MQR will be negatively affected during contract performance the contractor shall notify the Contracting officer and provide a plan which will address how the contractor will fulfill it's MQR commitment. All funds directed to a small business concern must be discreetly and uniquely reported to a single small business category.

Business Category	Dollar Value	Percentage
Small Business	\$	%
Small Disadvantaged Business	\$	%
Woman-Owned Small Business	\$	%
HUBZone Small Business	\$	%
Veteran-Owned Small Business	\$	%
Service-Disabled Veteran-Owned Small Business	\$	_____ %
Total Small Business Participation (do not double count concerns that qualify under multiple categories):	\$	%

3. Small Business Participants *

** Changes must be pre-approved by Contracting Officer per Section H clause in the contract*

Company Name & DUNS	Business Category(ies) <i>(SB, WOSB, SDB, VOSB, SDVOSB)</i>	Product(s)/Service(s) to be Provided	NAICS Code	Nature of Commitment

Instructions for completing the Table shown above: For each proposed small business participant, provide Company Name and DUNS No.; Business Category(ies) such SB, WOSB, SDB, VOSB, SDVOSB; and Product(s) or Service(s) Provided. Offerors must list the task(s) as identified in the PWS; NAICS Code – Provide the North American Industry Classification System Number associated with this work and; ~~All Offerors must~~ provide the Nature of the Commitment (such as, letter of commitment, signed teaming agreements, joint ventures, mentor protégé agreements, etc). Commitment documents must be provided with signature page(s).

All supporting documentation is excluded from the page count. Supporting documents will not be incorporated into any resulting contract.

NOTE: The SBPCD is an enforceable, contractual requirement which will be incorporated in the resultant IDIQ awarded contract. It will require periodic progress reporting by the Contractor to facilitate Government monitoring of the prime contractor's performance in meeting their MQR in the event of an award. Offerors are to propose annual reporting for their MQR above.

CONTRACT DATA REQUIREMENTS LIST <i>(1 Data Item)</i>						<i>Form Approved</i> <i>OMB No. 0704-0188</i>			
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.									
A. CONTRACT LINE ITEM NO. SEE BLK 16		B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER X					
D. SYSTEM/ITEM JWCC			E. CONTRACT/PR NO.			F. CONTRACTOR TBD			
1. DATA ITEM NO. A021	2. TITLE OF DATA ITEM Contractor Program Management Plan				3. SUBTITLE N/A				
4. AUTHORITY (Data Acquisition Document No.) DI-MGMT-81117A			5. CONTRACT REFERENCE PWS 5.1.6.1			6. REQUIRING OFFICE SEE BLK 16			
7. DD 250 REQ XX	9. DIST STATEMENT REQUIRED	10. FREQUENCY AS NECESSARY		12. DATE OF FIRST SUBMISSION DATO		14. DISTRIBUTION			
8. APP CODE N/A	SEE BLK 16	11. AS OF DATE N/A	13. DATE OF SUBSEQUENT SUBMISSION SEE BLK 16			a. ADDRESSEE		b. COPIES	
16. REMARKS Block A. CLIN X008 Block 4: The content requirements of the DID are tailored to require the delivery of the elements in accordance with PWS Section 5.1.6.1, with sufficient detail such that the Government can assess and understand how the Contractor intends to meet all requirements outlined in the PWS. The Contractor Program Management Plan (CPMP) shall be in contractor format. No classified information shall be submitted in the CPMP. Block 6: HaCC Block 9: All products produced as a result of this CDRL shall have a Distribution Statement of "D", unless an Original or Derivative Classifier promotes the document to a classified disposition, and requires a Distribution Statement other than "D", at which time the appropriate markings and Distribution statements shall be applied. Block 13: The Government shall have fifteen (15) calendar days after receiving for review and comment of the CPMP. Revise and resubmit the updated CPMP to the Government for approval five calendar days after receiving comments. Subsequent submissions are as required until the CPMP is approved. Block 14: Electronically delivered-reproducible Microsoft Office format (unless otherwise approved by the Government) to the JWCC Contracting Officer's Representative (COR).						Draft		Final	
								Reg	Repro
15. TOTAL →						0	0	0	
G. PREPARED BY JWCC PMO			H. DATE		I. APPROVED BY			J. DATE	

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE

INSTRUCTIONS FOR COMPLETING DD FORM 1423

(See DoD 5010.12-M for detailed instructions.)

FOR GOVERNMENT PERSONNEL

- Item A.** Self-explanatory.
- Item B.** Self-explanatory.
- Item C.** Mark (X) appropriate category: TDP - Technical Data Package; TM - Technical Manual; Other - other category of data, such as "Provisioning," "Configuration Management," etc.
- Item D.** Enter name of system/item being acquired that data will support.
- Item E.** Self-explanatory (to be filled in after contract award).
- Item F.** Self-explanatory (to be filled in after contract award).
- Item G.** Signature of preparer of CDRL.
- Item H.** Date CDRL was prepared.
- Item I.** Signature of CDRL approval authority.
- Item J.** Date CDRL was approved.
- Item 1.** See DoD FAR Supplement Subpart 4.71 for proper numbering.
- Item 2.** Enter title as it appears on data acquisition document cited in Item 4.
- Item 3.** Enter subtitle of data item for further definition of data item (optional entry).
- Item 4.** Enter Data Item Description (DID) number, military specification number, or military standard number listed in DoD 5010.12-L (AMSDL), or one-time DID number, that defines data content and format requirements.
- Item 5.** Enter reference to tasking in contract that generates requirement for the data item (e.g., Statement of Work paragraph number).
- Item 6.** Enter technical office responsible for ensuring adequacy of the data item.
- Item 7.** Specify requirement for inspection/acceptance of the data item by the Government.
- Item 8.** Specify requirement for approval of a draft before preparation of the final data item.
- Item 9.** For technical data, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDD 5230.24).
- Item 10.** Specify number of times data items are to be delivered.
- Item 11.** Specify as-of date of data item, when applicable.
- Item 12.** Specify when first submittal is required.
- Item 13.** Specify when subsequent submittals are required, when applicable.
- Item 14.** Enter addressees and number of draft/final copies to be delivered to each addressee. Explain reproducible copies in Item 16.
- Item 15.** Enter total number of draft/final copies to be delivered.
- Item 16.** Use for additional/clarifying information for Items 1 through 15. Examples are: Tailoring of documents cited in Item 4; Clarification of submittal dates in Items 12 and 13; Explanation of reproducible copies in Item 14.; Desired medium for delivery of the data item.

FOR THE CONTRACTOR

Item 17. Specify appropriate price group from one of the following groups of effort in developing estimated prices for each data item listed on the DD Form 1423.

a. Group I. Definition - Data which is not otherwise essential to the contractor's performance of the primary contracted effort (production, development, testing, and administration) but which is required by DD Form 1423.

Estimated Price - Costs to be included under Group I are those applicable to preparing and assembling the data item in conformance with Government requirements, and the administration and other expenses related to reproducing and delivering such data items to the Government.

b. Group II. Definition - Data which is essential to the performance of the primary contracted effort but the contractor is required to perform additional work to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, or quality of the data item.

Estimated Price - Costs to be included under Group II are those incurred over and above the cost of the essential data item without conforming to Government requirements, and the administrative and other expenses related to reproducing and delivering such data item to the Government.

c. Group III. Definition - Data which the contractor must develop for his internal use in performance of the primary contracted effort and does not require any substantial change to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, and quality of the data item.

Estimated Price - Costs to be included under Group III are the administrative and other expenses related to reproducing and delivering such data item to the Government.

d. Group IV. Definition - Data which is developed by the contractor as part of his normal operating procedures and his effort in supplying these data to the Government is minimal.

Estimated Price - Group IV items should normally be shown on the DD Form 1423 at no cost.

Item 18. For each data item, enter an amount equal to that portion of the total price which is estimated to be attributable to the production or development for the Government of that item of data. These estimated data prices shall be developed only from those costs which will be incurred as a direct result of the requirement to supply the data, over and above those costs which would otherwise be incurred in performance of the contract if no data were required. The estimated data prices shall not include any amount for rights in data. The Government's right to use the data shall be governed by the pertinent provisions of the contract.

CONTRACT DATA REQUIREMENTS LIST <i>(1 Data Item)</i>						<i>Form Approved</i> <i>OMB No. 0704-0188</i>			
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.									
A. CONTRACT LINE ITEM NO. SEE BLK 16		B. EXHIBIT A		C. CATEGORY: TDP _____ TM _____ OTHER X					
D. SYSTEM/ITEM JWCC			E. CONTRACT/PR NO.			F. CONTRACTOR TBD			
1. DATA ITEM NO. A021	2. TITLE OF DATA ITEM Contractor Program Management Plan				3. SUBTITLE N/A				
4. AUTHORITY (Data Acquisition Document No.) DI-MGMT-81117A			5. CONTRACT REFERENCE PWS 5.1.6.1			6. REQUIRING OFFICE SEE BLK 16			
7. DD 250 REQ XX	9. DIST STATEMENT REQUIRED	10. FREQUENCY AS NECESSARY		12. DATE OF FIRST SUBMISSION DATO		14. DISTRIBUTION			
8. APP CODE N/A	SEE BLK 16	11. AS OF DATE N/A	13. DATE OF SUBSEQUENT SUBMISSION SEE BLK 16			a. ADDRESSEE		b. COPIES	
16. REMARKS Block A. CLIN X008 Block 4: The content requirements of the DID are tailored to require the delivery of the elements in accordance with PWS Section 5.1.6.1, with sufficient detail such that the Government can assess and understand how the Contractor intends to meet all requirements outlined in the PWS. The Contractor Program Management Plan (CPMP) shall be in contractor format. No classified information shall be submitted in the CPMP. Block 6: HaCC Block 9: All products produced as a result of this CDRL shall have a Distribution Statement of "D", unless an Original or Derivative Classifier promotes the document to a classified disposition, and requires a Distribution Statement other than "D", at which time the appropriate markings and Distribution statements shall be applied. Block 13: The Government shall have fifteen (15) calendar days after receiving for review and comment of the CPMP. Revise and resubmit the updated CPMP to the Government for approval five calendar days after receiving comments. Subsequent submissions are as required until the CPMP is approved. Block 14: Electronically delivered-reproducible Microsoft Office format (unless otherwise approved by the Government) to the JWCC Contracting Officer's Representative (COR).						Draft		Final	
								Reg	Repro
15. TOTAL →						0	0	0	
G. PREPARED BY JWCC PMO			H. DATE		I. APPROVED BY		J. DATE		

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE

CONTRACT DATA REQUIREMENTS LIST

(1 Data Item)

A. CONTRACT LINE ITEM NO. SEE BLK 16	B. EXHIBIT A	C. CATEGORY: TDP _____ TM _____ OTHER <input checked="" type="checkbox"/>
D. SYSTEM/ITEM JWCC	E. CONTRACT/PR NO.	F. CONTRACTOR TBD

16. REMARKS (Continued)

INSTRUCTIONS FOR COMPLETING DD FORM 1423

(See DoD 5010.12-M for detailed instructions.)

FOR GOVERNMENT PERSONNEL

- Item A.** Self-explanatory.
- Item B.** Self-explanatory.
- Item C.** Mark (X) appropriate category: TDP - Technical Data Package; TM - Technical Manual; Other - other category of data, such as "Provisioning," "Configuration Management," etc.
- Item D.** Enter name of system/item being acquired that data will support.
- Item E.** Self-explanatory (to be filled in after contract award).
- Item F.** Self-explanatory (to be filled in after contract award).
- Item G.** Signature of preparer of CDRL.
- Item H.** Date CDRL was prepared.
- Item I.** Signature of CDRL approval authority.
- Item J.** Date CDRL was approved.
- Item 1.** See DoD FAR Supplement Subpart 4.71 for proper numbering.
- Item 2.** Enter title as it appears on data acquisition document cited in Item 4.
- Item 3.** Enter subtitle of data item for further definition of data item (optional entry).
- Item 4.** Enter Data Item Description (DID) number, military specification number, or military standard number listed in DoD 5010.12-L (AMSDL), or one-time DID number, that defines data content and format requirements.
- Item 5.** Enter reference to tasking in contract that generates requirement for the data item (e.g., Statement of Work paragraph number).
- Item 6.** Enter technical office responsible for ensuring adequacy of the data item.
- Item 7.** Specify requirement for inspection/acceptance of the data item by the Government.
- Item 8.** Specify requirement for approval of a draft before preparation of the final data item.
- Item 9.** For technical data, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDD 5230.24).
- Item 10.** Specify number of times data items are to be delivered.
- Item 11.** Specify as-of date of data item, when applicable.
- Item 12.** Specify when first submittal is required.
- Item 13.** Specify when subsequent submittals are required, when applicable.
- Item 14.** Enter addressees and number of draft/final copies to be delivered to each addressee. Explain reproducible copies in Item 16.
- Item 15.** Enter total number of draft/final copies to be delivered.
- Item 16.** Use for additional/clarifying information for Items 1 through 15. Examples are: Tailoring of documents cited in Item 4; Clarification of submittal dates in Items 12 and 13; Explanation of reproducible copies in Item 14.; Desired medium for delivery of the data item.

FOR THE CONTRACTOR

Item 17. Specify appropriate price group from one of the following groups of effort in developing estimated prices for each data item listed on the DD Form 1423.

a. Group I. Definition - Data which is not otherwise essential to the contractor's performance of the primary contracted effort (production, development, testing, and administration) but which is required by DD Form 1423.

Estimated Price - Costs to be included under Group I are those applicable to preparing and assembling the data item in conformance with Government requirements, and the administration and other expenses related to reproducing and delivering such data items to the Government.

b. Group II. Definition - Data which is essential to the performance of the primary contracted effort but the contractor is required to perform additional work to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, or quality of the data item.

Estimated Price - Costs to be included under Group II are those incurred over and above the cost of the essential data item without conforming to Government requirements, and the administrative and other expenses related to reproducing and delivering such data item to the Government.

c. Group III. Definition - Data which the contractor must develop for his internal use in performance of the primary contracted effort and does not require any substantial change to conform to Government requirements with regard to depth of content, format, frequency of submittal, preparation, control, and quality of the data item.

Estimated Price - Costs to be included under Group III are the administrative and other expenses related to reproducing and delivering such data item to the Government.

d. Group IV. Definition - Data which is developed by the contractor as part of his normal operating procedures and his effort in supplying these data to the Government is minimal.

Estimated Price - Group IV items should normally be shown on the DD Form 1423 at no cost.

Item 18. For each data item, enter an amount equal to that portion of the total price which is estimated to be attributable to the production or development for the Government of that item of data. These estimated data prices shall be developed only from those costs which will be incurred as a direct result of the requirement to supply the data, over and above those costs which would otherwise be incurred in performance of the contract if no data were required. The estimated data prices shall not include any amount for rights in data. The Government's right to use the data shall be governed by the pertinent provisions of the contract.