DEPARTMENT OF DEFENSE
JOINT WARFIGHTING CLOUD CAPABILITY
PERFORMANCE WORK STATEMENT

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 cloud 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 cloud 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 offerings (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 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 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	June 30, 2022 through June 29, 2025
Option Period I	June 30, 2025 through June 29, 2026
Option Period II	June 30, 2026 through June 29, 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 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. All personnel performing on 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, JWICS, SAPs, etc.	Access is required in the offering and support of SECRET cloud services and support to the JWCC Contract.
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 the offering and support of TOP SECRET cloud services and support to the JWCC Contract. Access to SCI caveats and information, and SAPs may be required based on the issued TOs.
Tactical Edge Offerings and Support	Up to TS/SCI	Access will be defined based on the TE device classification	Access is required in the offering and support of CLASSIFIED cloud services to the JWCC Contract
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
ATTN: MP61, Industrial Security
Command Building
6910 Cooper Ave.
Fort Meade, MD 20755-7088

Defense Information Systems Agency
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, 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.

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 a Bachelor of Arts/Bachelor of Science degree in a technical or managerial discipline, a PgMP or PMP certification, and at least 15 years of experience managing complex IT programs.

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 current Joint Travel Regulation (JTR), 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 for those Contract Line Item Numbers (CLINs) required within Attachment J-7: SBPCD that are identified as CLINs under which small businesses are expected to perform. Additionally, the Contractor shall report all small business performance under

the JWCC Contract using the electronic Subcontracting Reporting System (eSRS), IAW FAR Subpart 19.704 and Attachment J-6: Small Business Subcontracting Plan.

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 to compliance with the Government's security requirements. The Contractor shall rapidly implement alterations or configuration changes to Contractor-owned, Contractor-operated, infrastructure and capabilities that are supporting JWCC to address critical security vulnerabilities or national security requirements at the Government's direction. For the purpose of this subsection, 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 For the purpose of this section (1.5.15), "rapidly" means within eight hours or less from Government notification. All Government-directed alterations or configuration changes will be coordinated between the Government and the Contractor prior to implementation.

1.5.15.3 Depending on the urgency of the circumstances, a Government-directed alteration or configuration change may initially be provided by oral direction from the JWCC KO. 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 a written agreement between the Government and the Contractor as soon as practicable.

1.5.15.4 Throughout the entire PoP the Contractor shall maintain control, as defined in section 1.5.15.5, over its JWCC infrastructure for all UNCLASSIFIED and CLASSIFIED 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 offerings (excluding third-party marketplace offerings)

d. Hardware and software components of all points of presence

1.5.15.5 "Control", for PWS section 1.5.15, means the Contractor satisfies either of the following:

a. The Contractor is the Owner, as defined in section 1.5.15.6, as evidenced by the Contractor's self-certification; or

b. The Contractor has a fully executed agreement with the Owner, as defined in 1.5.15.6, of the assets of the cloud infrastructure (Control Agreement), as evident by self-certification, with the Owner granting the Contractor the following rights, at a minimum:

i. Unrestricted physical access to the JWCC infrastructure; and

ii. The ability to rapidly affect changes to the controlled infrastructure.

Further, the Control Agreement shall be binding for at least 364 days following each respective JWCC Contract ordering period or, if shorter than 364 days beyond the JWCC Contract ordering period, the end of the term shall result in the Contractor becoming the Owner, as defined in section 1.5.15.6.

Contractors who lose Control during performance are subject to termination for cause per FAR 52.212-4.

Control Agreement(s) may not be terminated by the Owner without at least 120 days notice to the Government. The Contractor shall make a good faith effort to modify all existing Control Agreement(s) no later than 180 days after the JWCC Contract award, to include a provision that the Control Agreement may not be terminated by the Owner without at least 120 days notice to the JWCC KO.

Contractors who lose Control during performance are subject to termination for cause per FAR 52.212-4.

1.5.15.6 "Owner" means the person or entity that has legal title to, or claim of right over, the assets of the infrastructure, which includes, at a minimum, the rights listed in subsections 1.5.15.5.b.i and 1.5.15.5.b.ii, above. The Owner must have a legally binding agreement evidencing ownership of infrastructure.

1.5.15.7 At any time, and with any frequency throughout the PoP, the Government may request additional documentation to prove compliance with section 1.5.15, including any proof of ownership, Control Agreement(s), and/or any other agreements or instruments that are identified in subsections 1.5.15.4.a through 1.5.15.4.d.

1.5.15.8 The JWCC KO may, at any time, request evidence that any Control Agreement has not been terminated or altered to conflict 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 owners by automating the initial provisioning of cloud resources in JWCC.

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). The XaaS and cloud services 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 PARITY. Equivalency of the hardware, services, pricing, interfaces, and capabilities offered between the Contractor's JWCC offerings and the Contractor's commercially available offerings in CONUS across all security domains, and at all classification levels and ILs.

2.1.27 CONFIDENTIALITY. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

2.1.28 CONTINENTAL UNITED STATES (CONUS). The 48 connected States that make up the United States and the District of Columbia.

2.1.29 CONTRACTOR. The supplier or vendor awarded a JWCC Contract.

2.1.30 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.

2.1.30.1. The JWCC KO is the authorized and warranted individual for the JWCC IDIQ acquisition environment contracts.

2.1.30.2. The JWCC TO KO are the authorized and warranted individuals for TOs issued under the JWCC IDIQ acquisition environment contracts.

2.1.31 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.

2.1.32 CRYPTOGRAPHIC CERTAINTY. As defined in C3PO.

2.1.33 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)

2.1.34 DATA CENTER. As defined in C3PO.

2.1.35 DAY. Calendar day, unless specified otherwise.

2.1.36 DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the JWCC PWS.

2.1.37 DELIVERABLE. Any provided response to a requirement or set of requirements that is presented to a customer as work complete.

2.1.38 ELASTIC. The ability to quickly expand or contract resources to meet changing demands without worrying about capacity planning and usage loading.

2.1.39 FAILOVER. As defined in C3PO.

2.1.40 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.

2.1.41 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.

2.1.42 FIRST-PARTY MARKETPLACE OFFERINGS. Contractor-owned, Contractor-operated CSO provided directly to the client.

2.1.43 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.

2.1.44 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).

2.1.45 HYPERVISOR. 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.

2.1.46 IMPACT LEVEL 2 (IL 2). As defined in C3PO.

2.1.47 IMPACT LEVEL 4 (IL 4). As defined in C3PO.

2.1.48 IMPACT LEVEL 5 (IL 5). As defined in C3PO.

2.1.49 IMPACT LEVEL 6 (IL 6). As defined in the CC SRG.

2.1.50 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.

2.1.51 INFRASTRUCTURE. As defined in C3PO.

2.1.52 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).

2.1.53 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)

2.1.54 INVESTIGATION. As defined in C3PO.

2.1.55 JWCC CATALOG. The Contractor provided listing of all its JWCC offerings, with the associated JWCC price for each offering, and the DoD Authorization (Provisional Authorization) for each offering and the offering's applicable classification level and IL, which is viewable by DoD users only.

2.1.56 JWCC MARKETPLACE. A mechanism (e.g. portal, console), provided by the Contractor, for fulfilling orders, provisioning, and deploying the approved JWCC Catalog 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 offerings (e.g. Cloud Support Packages).

2.1.57 LOGICAL SEPARATION. As defined in C3PO.

2.1.58 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.

2.1.59 MANAGEMENT PLANE. Portion of the Contractor's cloud environment that a user has no access to.

2.1.60 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.

2.1.61 MIGRATION. The act of moving an application and/or data from one infrastructure or platform to another infrastructure or platform.

2.1.62 MITIGATION. As defined in C3PO.

2.1.63 MEMORIALIZED CONTRACTOR COMMERCIAL CATALOG. An unchangeable/unmodified snapshot, at the time of proposal submission, of the Contractor's complete listing of its publicly available commercial offerings with associated commercial pricing and proposed JWCC pricing.

2.1.64 MODERN. Relating to the present or recent times as opposed to the remote past or antiquated technology.

2.1.65 NEARLINE STORAGE. Storage that is not immediately available, but can be brought online quickly without human intervention.

2.1.66 NEARSIDER. An individual that has physical access to the hardware but does not have logical access to the actual data.

2.1.67 NETWORK. As defined in C3PO.

2.1.68 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.

2.1.69 OFFERING. Any item that is proposed by the Contractor for inclusion in the JWCC Catalog (e.g. service offerings, cloud offerings, CSOs, cloud support packages, TE offerings, cloud services, cloud capabilities, advisory and assistance services)

2.1.70 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.

2.1.71 ONLINE STORAGE. Storage that is immediately accessible to applications without human intervention.

2.1.72 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.

2.1.73 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.

2.1.74 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 1.5.15.5 of the JWCC PWS, where JWCC is accessible to DoD.

2.1.75 PRODUCTION PLANE. Portion of the Contractor's cloud environment infrastructure that a user has access to.

2.1.76 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)

2.1.77 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.

2.1.78 PURGE. Apply physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques. (NIST SP 800-88 Revision 1).

2.1.79 QUALITY ASSURANCE. The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.80 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the methodology to be used for surveillance of the Contractor's performance.

2.1.81 QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service meets contractual requirements.

2.1.82 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).

2.1.83 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.

2.1.84 ROBUST INFRASTRUCTURE. Infrastructure that is responsive, resilient, redundant, and reliable.

2.1.85 ROLE. A job function, with associated system access privileges, to which people or other system entities may be assigned in a system.

2.1.86 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.

2.1.87 SCALABILITY. The ability to increase or decrease resources commensurate with demand.

2.1.88 SELF-SERVICE. The ability of a user to access data and perform actions without any human interaction or third-party approval.

2.1.89 SERVER. As defined in C3PO.

2.1.90 SERVICE MODEL. The highest-level categorization of cloud services as based on the type of computing capability that is provided. (NIST SP 500-322)

2.1.91 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.

2.1.92 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

2.1.93 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.

2.1.94 SUBCONTRACTOR. A party that enters into a contract with the Contractor. The Government does not have privity of contract with subcontractors.

2.1.95 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).

2.1.96 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.

2.1.97 TESTING. See Independent Verification and Validation and C3PO (as applicable for security requirements).

2.1.98 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.

2.1.99 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.

2.1.100 TRAFFIC. As defined in C3PO.

2.1.101 UNCLASSIFIED INFRASTRUCTURE. As defined in C3PO.

2.1.102 USER. Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

2.1.103 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.

2.1.104 VIRTUAL MACHINE (VM). Software that emulates a computer's physical hardware.

2.1.105 VULNERABILITY. As defined in C3PO.

2.1.106 WORK DAY. The number of hours per day the Contractor provides services IAW the JWCC Contract.

2.1.107 WORK WEEK. Monday through Friday, unless otherwise specified.

2.1.108 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.

2.1.109 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
COMSEC	Communications Security
CONUS	Continental United States

COR	Contracting Officer's Representative
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
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.<u>CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES</u>:

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 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 provide a Contractor Program Management Plan (CPMP) (CDRL A021) 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:

5.1.6.1 The Contractor shall provide a monthly Contract Progress Report (CDRL A001) for overall performance under the JWCC Contract and access to all TO Progress Reports (CDRL A012) for PM performance. The Contract Progress Report shall include, but not be limited to, the following:

5.1.6.1.1 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.

5.1.6.1.2 The report shall include, at a minimum, the DoD utilization metrics and the percentage as compared to the Contractor's total commercial and non-commercial utilization and capacity, broken out by CSO and CLIN per month, year, and life of the JWCC Contract for the following metrics:

5.1.6.1.2.1 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.

5.1.6.1.2.2 Compute. Number of physical (not virtualized) compute (CPU and/or 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.

5.1.6.1.2.3 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.

5.1.6.1.2.4 Additionally, the report shall identify the base (e.g. base 2 or base 10) for all measured values using bytes.

5.1.6.1.3 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.

5.1.6.1.4 A report on usage, by TO, for any GFP (CDRL A015).

5.1.6.1.5 A report on ordering, by TO, for any TE offering and any associated TE devices (CDRL A012).

5.1.6.1.6 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.

5.1.6.1.7 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).

5.1.6.1.8 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 (CDRL A014).

5.1.6.1.9 Any issues, challenges, problems, risk areas, or requests for JWCC COR support.

5.1.6.2 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 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.

5.1.6.3 The Contractor shall arrange, execute, and facilitate meetings when requested by the JWCC PMO, or as required, in support of the JWCC Contract.

5.1.6.3.1 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:

5.1.6.3.1.1 Overall JWCC Contract execution, management and operating status update;

5.1.6.3.1.2 Discussion, as necessary, of any upcoming JWCC Catalog changes in offerings (as captured in CDRL A022), including addition, modification, deletion or deprecation;

5.1.6.3.1.3 Specific recommendations to better optimize JWCC Contract offerings, operations, and deployment based on empirical evidence, with projections for implementation of those recommendations;

5.1.6.3.1.4 Recommendation to improve communication between the Contractor and the JWCC COR;

5.1.6.3.1.5 Status of, and any issues regarding, use of and interfacing with ATAT;

5.1.6.3.1.6 Identification of JWCC Contract issues or problems, with regard to management or operations of the JWCC Contract, and the associated risks and mitigation plan;

5.1.6.3.1.7 Advising on the utilization of JWCC Contract and how it aligns to the commercial trends and practices;

5.1.6.3.1.8 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;

5.1.6.3.1.9 Discussion of any previous quarter C3PO required reports submitted to the JWCC COR;

5.1.6.3.1.10 Any Government agenda items provided to the Contractor for inclusion in the scheduled IPR.

5.1.6.3.2 Technical Exchange Meetings (TEMs). As requested by the JWCC COR, the Contractor shall arrange, facilitate and execute TEMs. TEMs can discuss any current or upcoming TOs, any future cloud offerings the Contractor will have available for purchase, and/or 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.

5.1.6.3.3 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.

5.1.6.4 Ordering Guide Inputs.

5.1.6.4.1 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 TE offerings, cloud support packages, and online marketplace offerings, to include BYOL offerings, to be included in the JWCC Ordering Guide.

5.1.6.4.1.1 Contractor's PoC information and e-mail for contracting related issues.

5.1.6.4.1.2 Contractor's email address for distribution of TOs (if different from above).

5.1.6.4.1.3 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 that are authorized for DoD consumption under the JWCC Contract.

5.1.6.4.1.4 Any specific process the Contractor may have for requesting TE offerings that deviates from the normal fulfillment process.

5.1.6.4.1.5 Any specific process the Contractor may have for requesting Cloud Support Packages.

5.1.6.4.1.6 The Contractor's inputs to the Ordering Guide shall be delivered to the Government (CDRL A007).

5.1.6.4.1.7 The Memorialized Contractor Commercial Catalog, an unchangeable/unmodified snapshot, at the time of award, of the Contractor's complete listing of its publicly available CSOs with associated commercial pricing and proposed JWCC pricing. In addition, all Federal Government Authorizations (FedRAMP, Provisional Authorization(s), ATOs, and AOs) of each offering and the associated classification level and IL.

5.1.6.5 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 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 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.

5.1.6.6 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).

5.1.6.7 Delivery. All materials shall be provided error free and presented in a professional manner.

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 obtain near-immediate support (initiate the response within 5 minutes of request receipt and service the response within 10 minutes of request receipt) to address any issues or failures that arise from an attempt to establish an offering (provisioning) as ordered within a valid JWCC account. This PoC shall be available 24 hours a day, 7 days a week, 365 days a week, 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.

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.

5.1.6.10 Portability Test. The JWCC Contract will require the ability to move information (data and files) from a cloud environment to another environment (cloud or otherwise) of the Government's choosing. The Contractor is required to provide the Government with all of the necessary details to understand how each portability test is constructed using cloud offerings to achieve the necessary outcome, based on the below scenarios:

5.1.6.10.1 General portability test scenario description. The portability test exercises the Contractor's ability to extract information from the Contractor's cloud environment. The Government is providing the following notional examples for the specific purpose of pricing the portability test. These scenarios are not representative of any future workloads nor is this intended to be indicative of any future work. For each portability test scenario, the Contractor shall explain its process for immediate transfer of all information and time-phased or continuous slow-paced extraction methods. If there are additional approaches that provide a pricing advantage, the Contractor is encouraged to clearly identify those additional processes and procedures that can be used to achieve an

improved pricing outcome. The need for any changes in performance based on sizing shall be explained within the process.

5.1.6.10.1.1 Scenario 1 – Small Portability Test

5.1.6.10.1.1.1 Test 1.1 – Transfer 100 Gigabytes of raw storage

5.1.6.10.1.1.2 Test 1.2 – Transfer 100 Gigabytes of multiple files across multiple pricing “regions/zones.” The pricing "regions/zones should contain equal sizing and amounts of information.

5.1.6.10.1.1.3 Test 1.3 – Transfer 100 Gigabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers, and other information constructs.

5.1.6.10.1.2 Scenario 2 – Medium Portability Test

5.1.6.10.1.2.1 Test 2.1 – Transfer 100 Terabytes of raw storage

5.1.6.10.1.2.2 Test 2.2 – Transfer 100 Terabytes of multiple files across multiple pricing “regions/zones.” The pricing regions/zones should contain equal sizing and amounts of information.

5.1.6.10.1.2.3 Test 2.3 – Transfer 100 Terabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers and other information constructs.

5.1.6.10.1.3 Scenario 3 – Large Portability Test

5.1.6.10.1.3.1 Test 3.1 –Transfer 100 Petabytes of raw storage

5.1.6.10.1.3.2 Test 3.2 – Transfer 100 Petabytes of multiple files across multiple pricing “regions/zones.” The pricing regions/zones should contain equal sizing and amounts of information.

5.1.6.10.1.3.3 Test 3.3 – Transfer 100 Petabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers and other information constructs.

5.1.6.10.1.4 Scenario 4 – Huge Portability Test

5.1.6.10.1.4.1 Test 3.1 – Transfer 100 Exabytes of raw storage

5.1.6.10.1.4.2 Test 3.2 – Transfer 100 Exabytes of multiple files across multiple pricing "regions/zones." The pricing regions/zones should contain equal sizing and amounts of information.

5.1.6.11 Portability Plan. The Contractor shall provide a Portability Plan (CDRL A006) that describes the process for each Portability Test Scenario. The Contractor is required to provide the Government with all of the necessary details to understand how each portability test is constructed and shall explicitly identify the JWCC Catalog offerings necessary to conduct a test and achieve the necessary outcome per scenario. All scenarios represented in PWS Section 5.1.6.11 Portability Test shall be detailed in the Portability Plan. For each portability test scenario, the Contractor shall explain its process for immediate transfer of all information and time-phased (or continuous slow-paced) extraction models.

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.

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) 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.

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 offering and potential 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 UNCLASSIFIED offerings at ILs 2, 4, and 5 at JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) UNCLASSIFIED offerings, including UNCLASSIFIED TE offerings. At 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 offerings meet all security requirements outlined in C3PO.

5.5.1.3 Classified Secret Timeline. The Contractor shall provide 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) SECRET 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 offerings meet all security requirements outlined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254.

5.5.1.4 Classified Top Secret Timeline. The Contractor shall provide 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) TS 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 offerings. The Contractor shall ensure all 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).

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 offerings IAW DoDD 5205.07, DoDM 5200.01, and the Joint Special Access Program Implementation Guide (JSIG). These 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.

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 offerings, on or before the delivery of that CLASSIFIED infrastructure and 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 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.

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 Catalog 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 compute, network, and storage resources and services to any other data center within each 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 offering 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 offering 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 offering 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 offering 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 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/or 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 and/or all CSOs. 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 and historical billing data and pricing data, including: by CSOs, Cloud Support Packages, specified by workspace, under the entire JWCC Contract.

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 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 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.

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.

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 and/or cybersecurity needs.

5.5.4.11 The Contractor shall provide an IaC CSO, which allows the deployment and/or provisioning of one or more other CSOs. This IaC CSO will use pre-made standardized configurations and/or customizable configurations. This IaC CSO shall also include a simple mechanism to deprovision any and all CSOs it deployed and/or provisioned.

5.5.4.12 The Contractor shall not bundle any offerings in a manner that restricts a JWCC user's ability to acquire individual offerings. Any bundled offerings shall also be available as discrete offerings.

5.5.4.13 The Contractor shall not require any third-party services that require separate billing and/or licensing in order to meet the JWCC requirements or minimum requirements for using any JWCC CSO. For purposes of this requirement, 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 will not be considered a third-party service that requires separate billing and/or licensing.

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 and/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 provide immediate notification to 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. The Contractor shall compile a report for any notification that violated the maximum notification period according to negotiated SLAs as memorialized in the JWCC Contract. The JWCC COR shall be included on all notifications.

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 and/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 offerings it provides under the JWCC Contract.

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 and/or Statutory reporting compliance mandates. Such logs shall be generated and available using, at a minimum, both XML and 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 The Contractor shall provide an audit trail of all activities and actions (e.g., "Scenarios," as defined in C3PO) as required under the CC SRG. Each consolidated log location, as described in C3PO, shall contain all logs from all JWCC workspaces within the Contractor's JWCC cloud environment at each classification level and IL. 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 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 for the output (e.g. files, screen displays, etc.). At a minimum, this shall include a user accessible dashboard and the file types PDF and CSV. This shall allow users to indicate one or more output methods for a generated report.

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 account and/or organizational structure (i.e. Enterprise, Department, Office, Team) to determine cloud spend by organizational structure and/or user.

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 Catalog 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 as detailed in sub-section 5.5.4.3 Portability Plan (CDRL A006).

5.5.5.1 The Contractor shall provide the Government the ability to rapidly and securely provision/deploy first-party offerings and third-party offerings via the Contractor-provided JWCC Marketplace, as defined below, with baseline template configurations, onto JWCC infrastructure at all classification levels and ILs. Third-party offerings 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 offerings and third-party offerings listed on the JWCC Catalog. All JWCC 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 makes them available for JWCC users to fulfill orders, provision, or deploy. 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 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 offerings 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 to a third-party marketplace offering being price-free, each offering shall be approved by the JWCC KO. All third-party offerings that are available in the JWCC Marketplace shall be offered price-free and BYOL basis as appropriate, excluding the cost of IaaS resources. These 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 offerings 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 offerings 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 offerings 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 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 approved offerings shall be populated within 24 hours of JWCC KO approval.

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 offering, or any combination of offerings, to enable 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 and IL to ensure there is no spillage related to budgets for CLASSIFIED programs. The Contractor's Calculator shall be consistent with the JWCC Contract pricing and the JWCC Catalog, based on the pricing and availability of the offerings at the classification levels and ILs 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 Contractor shall provide a Portability Plan (CDRL A006) as follows:

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.

5.5.6 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. Offerings shall include generational replacement and upgrades of hardware and software, as well as specialized hardware offerings to support advanced capabilities such that the offerings in the JWCC Catalog are the same or equivalent in form, fit, and function as the offerings made commercially available. Any exception(s) to this requirement must be approved by the JWCC KO.

5.5.6.1 The Contractor shall ensure the provisioning of each 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 offering at each classification level and IL such that the Government can validate provisioning performance for each offering (e.g. provisioning a new workspace, user, or service offering, or deploying such offerings within JWCC).

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 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's offerings available under the JWCC Contract, across each classification level and IL, 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 approved by the JWCC KO.

5.5.6.4 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).

5.5.6.5 For any of the offerings available under the JWCC Contract, across each classification level and IL, the same API calls and/or Contractor Portal (UI) actions shall result in the same expected behavior, except when restrictions due to classification level and/or IL prohibit commercial parity.

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.

5.5.6.7 All offerings shall be at or below the Contractor's commercial catalog pricing.

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 Tensor Processing Unit (TPU) processing architectures, quantum computing applications).

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 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 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.

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 commercially available 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 cloud service offerings 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. 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.

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 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.

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 cloud service offerings 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) operations on the production plane, as described and/or required in 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 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/or 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 and/or roles within a specific workspace and/or the cloud environment.

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/or 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 offering 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), less exceptions 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 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 an offering in the JWCC Catalog, a minimum of one form factor of TE devices that is man-portable, capable of being carried and/or mounted to a vehicle, 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/or 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 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 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 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 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 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 offerings on the JWCC Catalog 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/or OCONUS locations. All training and support services shall be offered at the locations as described in the 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 and/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 as offerings.

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 logistics challenges in delivering, maintaining, and/or returning TE devices or capabilities.

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 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, and/or embedded training (e.g. TE device training that is self-paced and embedded on the device for use in the field).

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 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
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 provide a Contractor Program Management Plan (CPMP) (CDRL A021) 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:	The Government will assess the CPMP for sufficiency of addressing each requirement of the contract.	N/A

9	5.1.6.1	The Contractor shall provide a monthly Contract Progress Report (CDRL A001) for overall performance under the JWCC Contract and access to all TO Progress Reports (CDRL A012) for PM performance. The Contract Progress Report shall include, but not be limited to, the following:	Summary Requirement	
10	5.1.6.1.1	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 the data provided to describe TO execution value and expenditure.	The TO has robust data describing every facet of execution, financial, and management aspects.
11	5.1.6.1.2	The report shall include, at a minimum, the DoD utilization metrics and the percentage as compared to the Contractor's total commercial and non-commercial utilization and capacity, 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 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	5.1.6.1.2.1	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	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.

		utilization as a percentile comparison.		
13	5.1.6.1.2.2	Compute - Number of physical (not virtualized) compute (CPU and/or 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.
14	5.1.6.1.2.3	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.	Real time analytics will present a continuous reading of the JWCC utilization rates and the comparison to industry and total Government consumption.
15	5.1.6.1.2.4	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
16	5.1.6.1.3	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 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.

		the life of the JWCC Contract.		
17	5.1.6.1.4	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.
18	5.1.6.1.5	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.
19	5.1.6.1.6	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.
20	5.1.6.1.7	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
21	5.1.6.1.8	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 (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
22	5.1.6.1.9	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.

23	5.1.6.2	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 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
24	5.1.6.3	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
25	5.1.6.3.1	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,	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.

		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:		
26	5.1.6.3.1.1	Overall JWCC Contract execution, management and operating status update;	Summary Requirement	N/A
27	5.1.6.3.1.2	Discussion, as necessary, of any upcoming JWCC Catalog changes in offerings (as captured in CDRL A022), including addition, modification, deletion or deprecation;	The Government will assess the veracity of contractor catalog modification management.	N/A
28	5.1.6.3.1.3	Specific recommendations to better optimize JWCC Contract 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.
29	5.1.6.3.1.4	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
30	5.1.6.3.1.5	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.

31	5.1.6.3.1.6	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.
32	5.1.6.3.1.7	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.
33	5.1.6.3.1.8	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
34	5.1.6.3.1.9	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
35	5.1.6.3.1.10	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
36	5.1.6.3.2	Technical Exchange Meetings (TEMs). As requested by the JWCC COR, the Contractor shall arrange, facilitate and execute TEMs. TEMs can discuss any current or upcoming TOs, any future cloud offerings the Contractor will have available for purchase, and/or 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

37	5.1.6.3.3	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
38	5.1.6.4	Ordering Guide Inputs.	Summary Requirement	N/A
39	5.1.6.4.1	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 TE offerings, cloud support packages, and online 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.	Fully automated, intuitive navigation and self-help environment that is routinely updated without annex submissions.
40	5.1.6.4.1.1	Contractor's PoC information and e-mail for contracting related issues.	The Government will assess if email addresses and POCs are accurate.	N/A
41	5.1.6.4.1.2	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
42	5.1.6.4.1.3	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 that are authorized for DoD	The Government will assess if the link is accurate and operational at each classification level.	N/A

		consumption under the JWCC Contract.		
43	5.1.6.4.1.4	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
44	5.1.6.4.1.5	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
45	5.1.6.4.1.6	The Contractor's inputs to the Ordering Guide shall be delivered to the Government (CDRL A007).	The Government will assess if the ordering guide annex sufficiently describes the process.	N/A
46	5.1.6.4.1.7	The Memorialized Contractor Commercial Catalog, an unchangeable/unmodified snapshot, at the time of award, of the Contractor's complete listing of its publicly available CSOs with associated commercial pricing and proposed JWCC pricing. In addition, all Federal Government Authorizations (FedRAMP, Provisional Authorization(s), ATOs, and AOs) of each offering and the associated classification level and IL.	The Government will assess if the Memorialized Contractor Commercial Catalog is reflective of the Commercial Catalog at time of award.	N/A

47	5.1.6.5	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 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 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.	N/A
48	5.1.6.6	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	The Government will assess if the Contractors catalog submission meets the requirements of the JWCC contract.	N/A

		changes on a periodic basis (CDRL A022).		
49	5.1.6.7	Delivery. All materials shall be provided error free and presented in a professional manner.	The Government will assess deliverables for error-free and professional appearance.	N/A
50	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
51	5.1.6.8.1	The Contractor shall provide a PoC as part of the QCP to allow any JWCC user to obtain near-immediate support (initiate the response within 5 minutes of request receipt and service the response within 10 minutes of request receipt) to address any issues or failures that arise from an attempt to establish an offering (provisioning) as ordered within a valid JWCC account. This PoC shall be available 24 hours a day, 7 days a week, 365 days a week, worldwide without any charges or expense to the Government. The modalities of contact	The Government will assess if the QC PoC information is compliant with the requirement.	N/A

		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.		
52	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.	The Government will assess if the contractor has provided the appropriate information regarding TE Loss, Destruction, or Interoperability.	N/A
53	5.1.6.10	Portability Test. The JWCC Contract will require the ability to move information (data and files) from a cloud environment to another environment (cloud or otherwise) of the Government's choosing. The Contractor is required to provide the Government with all of the necessary details to understand how each portability test is constructed using cloud offerings to achieve the necessary outcome, based on the below scenarios:	The Government will assess the results of the Portability Test to determine if the desired outcome has been achieved.	N/A
54	5.1.6.10.1	Scenario 1 – Small Portability Test	Summary requirement	N/A
55	5.1.6.10.1.1	Test 1.1 – Transfer 100 Gigabytes of raw storage	Test Details	N/A
56	5.1.6.10.1.2	Test 1.2 – Transfer 100 Gigabytes of multiple files across multiple pricing "regions/zones." The pricing "regions/zones should contain equal sizing and amounts of information.	Test Details	N/A

57	5.1.6.10.1.3	Test 1.3 – Transfer 100 Gigabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers, and other information constructs.	Test Details	N/A
58	5.1.6.10.1.2	Scenario 2 – Medium Portability Test	Summary requirement	N/A
59	5.1.6.10.1.2.1	Test 2.1 – Transfer 100 Terabytes of raw storage	Test Details	N/A
60	5.1.6.10.1.2.2	Test 2.2 – Transfer 100 Terabytes of multiple files across multiple pricing “regions/zones.” The pricing regions/zones should contain equal sizing and amounts of information	Test Details	N/A
61	5.1.6.10.1.2.3	Test 2.3 – Transfer 100 Terabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers and other information constructs.	Test Details	N/A
62	5.1.6.10.1.3	Scenario 3 – Large Portability Test	Summary requirement	N/A
63	5.1.6.10.1.3.1	Test 3.1 –Transfer 100 Petabytes of raw storage	Test Details	N/A
64	5.1.6.10.1.3.2	Test 3.2 – Transfer 100 Petabytes of multiple files across multiple pricing “regions/zones.” The pricing regions/zones should contain equal sizing and amounts of information.	Test Details	N/A
65	5.1.6.10.1.3.3	Test 3.3 – Transfer 100 Petabytes of composite information, which includes basic file data, system configuration data, application source code, deployable containers and	Test Details	N/A

		other information constructs.		
66	5.1.6.10.1.4	Scenario 4 – Huge Portability Test	Summary requirement	N/A
67	5.1.6.10.1.4.1	Test 3.1 – Transfer 100 Exabytes of raw storage	Test Details	N/A
68	5.1.6.10.1.4.2	Test 3.2 – Transfer 100 Exabytes of multiple files across multiple pricing "regions/zones." The pricing regions/zones should contain equal sizing and amounts of information.	Test Details	N/A
69	5.1.6.11	Portability Plan. The Contractor shall provide a Portability Plan (CDRL A006) that describes the process for each Portability Test Scenario. The Contractor is required to provide the Government with all of the necessary details to understand how each portability test is constructed and shall explicitly identify the JWCC Catalog offerings necessary to conduct a test and achieve the necessary outcome per scenario. All scenarios represented in PWS Section 5.1.6.11 Portability Test shall be detailed in the Portability Plan. For each portability test scenario, the Contractor shall explain its process for immediate transfer of all information and time-phased (or continuous slow-paced) extraction models.	The Government will assess the Portability Plan to determine if the Contractor has a robust and sufficiently complete process to manage extrication of Government information.	N/A
70	5.2	Activities to Assess and Authorize Contractor's Cloud Infrastructure and Offerings	Summary Requirement	N/A

71	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.	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
72	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
73	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
74	5.3	Multi-Cloud Solution Technical Exchange Meetings (TEMs)	Summary Requirement	N/A
75	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

76	5.4	System and Organization Control (SOC 1) Type II Reporting	Summary Requirement	N/A
77	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.
78	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
79	5.5.1	Timeline. Delivery of XaaS, including TE offerings, will follow the timelines as listed below, unless otherwise specified.	Summary Requirement	N/A
80	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	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	The Roadmap/Integrated Master Timeline fully details the duration of the contract with no offerings left unaccounted.

		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 and potential future offering to track successful or unsuccessful outcomes presented in the Roadmap/Integrated Master Timeline for delivery and operability.	for in the Roadmap/Integrated Master Timeline, including current, future, deprecated, and removed items.	
81	5.5.1.2	Unclassified Timeline. The Contractor shall provide UNCLASSIFIED offerings at ILs 2, 4, and 5 at JWCC Contract award, such that the DoD will have the ability to deploy and use (immediately upon DoD Provisional Authorization) UNCLASSIFIED offerings, including UNCLASSIFIED TE offerings. At 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 offerings meet all security requirements outlined in C3PO.	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.
82	5.5.1.3	Classified Secret Timeline. The Contractor shall provide 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) SECRET offerings, including SECRET TE offerings. Within 60 days post-JWCC Contract award,	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	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.

		the Contractor shall have provided all documentation and artifacts required for the AO to grant Provisional Authorization. The Contractor shall ensure all offerings meet all security requirements outlined in C3PO, DoDM 5200.01, and the Attachment J-3: JWCC DD254.	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.	
83	5.5.1.4	Classified Top Secret Timeline. The Contractor shall provide 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) TS 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 offerings. The Contractor shall ensure all 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).	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	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.

			any services that have not been previously authorized, all documentation required is delivered to the AO, within 180 days after JWCC Contract award.	
84	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 offerings IAW DoDD 5205.07, DoDM 5200.01, and the Joint Special Access Program Implementation Guide (JSIG). These 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.	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.	The process for security compliance is fully automated and presented in a continuously updated report for each offering and TE offering.
85	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 offerings, on or before the delivery of that CLASSIFIED infrastructure and offerings. The CDSs for the production plane shall be provided to the DoD	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	The process for requirements compliance is fully automated and presented in a continuously updated report for each CDS.

		within 180 days after the delivery of the associated CLASSIFIED infrastructure and 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.	made available to the ISMRC for authorization.	
86	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 Catalog 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.

87	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
88	5.5.2.1	The Contractor shall provide dynamic scalability and resiliency through industry standard mechanisms and activities	The Government will perform testing of offerings deployed and operating within JWCC for scalability,	The offerings will be automatically scalable and resilient.

		to ensure the DoD has the ability to maintain continuous operations.	resiliency, performance, cybersecurity, and cyber survivability.	
89	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.
90	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
91	5.5.2.3.1	Every data center shall be capable of automated replication and failover of compute, network, and storage resources and services to any other data center within each 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 and/or physical exercise, 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 facility is unacceptable.)	All failovers are fully automated and there is no appreciable downtime (99.99999%) for any offering
92	5.5.2.3.2	The Contractor shall, at time of award, provide no fewer than two physical data centers offering UNCLASSIFIED CSOs within the Customs	The Government will assess whether the Contractor has at least two data centers meeting the requirements above	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.

		Territory of the United States, as defined in FAR 2.101.	that provide UNCLASSIFIED CSOs. The Government reserves the right to inspect any facility used to host JWCC workloads.	
93	5.5.2.3.3	The Contractor shall, upon delivery of SECRET CSOs, provide no fewer than two physical data centers offering 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.
94	5.5.2.3.4	The Contractor shall, upon delivery of TS CSOs, provide no fewer than two physical data centers offering 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
95	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 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	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.

		Energy, and within the Customs Territory of the U.S., as defined in FAR 2.101.		
96	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.
97	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.
98	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
99	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 to peer with the DoD on each continent. If the DoD adds new locations, the Contractor shall peer with	The Government will assess, through review of documentation and/or site inspection, whether the Contractor has points of presence on all continents, with the exception of Antarctica, and that those points of	All Points of Presence support maximal bandwidth capability offered and dynamic automated peering services are available.

		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.	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.	
100	5.5.4	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/or 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 and/or all CSOs. 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	Summary Requirement	N/A

		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).		
101	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.	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.
102	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	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.

			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/or disable services.	
103	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.
104	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
105	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

106	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.
107	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 change storage type based on AI/ML learning algorithms trained on access and interaction data based on file type, location, and/or other policy information.
108	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.
109	5.5.4.4.5	Reading accrual and historical billing data and pricing data, including: by CSOs, Cloud Support Packages, specified by workspace, under the entire JWCC Contract.	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.
110	5.5.4.4.6	Setting billing and usage thresholds and adding automated notifications to workspace owners and the	The Government will assess the sufficiency of the API to support all of the	Automated parametric response triggers are programmatically executed

		TO COR as well as a capability to configure the discontinuation of service upon the billing and usage threshold breach.	requirements, separately and collectively. The Government reserves the right to perform periodic testing of these capabilities.	on achieving specific conditions.
111	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.
112	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 and potential and/or actual impact on current operations.	All APIs are fully self-documented. All API changes are both human and machine consumable for automated change analysis.
113	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	The Government will assess whether the Contractor has adhered to notification time frames for API changes.	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.

		change. Additionally, the Contractor shall make available this same information to all DoD personnel and other authorized JWCC users.		
114	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.)	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.
115	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.	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.

116	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 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 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: Creation & management of access credentials for accounts and environments in which CSOs can be provisioned. Creation and management of portfolios which manage groups of accounts and environments. Creation of the necessary account for the Contractor's Portal(s) (UI). Obtaining actual and projected costs per CLIN, environment, workloads, and portfolio. Setting billing limits with notifications on CLINs,	The Government will assess whether ATAT calls to the Contractor's ATAT Multi-Cloud Provisioning API implementation(s) to create and manage portfolios, accounts and/or environments 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/or portfolio and set billing limits and notifications on environments, workloads, and portfolios.	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.

		environments, workloads, and portfolios.		
117	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 the published API requirements within the required timelines.	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.
118	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.	The Contractor's API implementation supports continuous operations for scale, and all parametric permutations at all classification levels and ILs.
119	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.
120	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 and/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.

121	5.5.4.11	The Contractor shall provide an IaC CSO, which allows the deployment and/or provisioning of one or more other CSOs. This IaC CSO will use pre-made standardized configurations and/or customizable configurations. This IaC CSO shall also include a simple mechanism to deprovision any and all CSOs it deployed and/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.
122	5.5.4.12	The Contractor shall not bundle any offerings in a manner that restricts a JWCC user's ability to acquire individual offerings. Any bundled offerings shall also be available as discrete 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.
123	5.5.4.13	The Contractor shall not require any third-party services that require separate billing and/or licensing in order to meet the JWCC requirements or minimum requirements for using any JWCC CSO. For purposes of this requirement, 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 will not be considered a third-party service that requires separate billing and/or licensing.	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.

124	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 and/or cloud operations. The following minimum requirements apply to all environments, including network and TE devices:	Summary Requirement	N/A
125	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.	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: Incident escalation mechanisms are clearly observable and course of action adjustments are captured. Full logging is enabled for each incident and all remediation actions are captured in persistent logs	Service Incident Event Management is fully automated and 100% activity is logged and analyzed for optimization opportunities and auditing for security best practices.
126	5.5.4.14.2	The Contractor shall provide immediate notification to 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	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.

		level, for each Service Incident Event. The Contractor shall compile a report for any notification that violated the maximum notification period according to negotiated SLAs as memorialized in the JWCC Contract. The JWCC COR shall be included on all notifications.		
127	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.
128	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 and/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.	The Government will assess whether: 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. Compliance with Contractor's stated Service Level Objectives (SLO), as	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.

			stipulated in the Contractor's SLAs, will be analyzed for deviation above the objective thresholds.	
129	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.
130	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.
131	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.	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.
132	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 core cloud services (i.e. unplanned disconnected operations) the service provides via multiple modes notifications to a set of identified administrators

133	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 and/or Statutory reporting compliance mandates. Such logs shall be generated and available using, at a minimum, both XML and 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.
134	5.5.4.15.1	The Contractor shall provide an audit trail of all activities and actions (e.g., “Scenarios,” as defined in C3PO) as required under the CC SRG. Each consolidated log location, as described in C3PO, shall contain all logs from all JWCC workspaces within the Contractor’s JWCC cloud environment at each classification level and IL. 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.
135	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	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	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.

		features shall be accessible from the Contractor's Portal (UI), at each classification level and IL, and include sample code.	documentation from the Contractor's Portal (UI), at each classification level and IL, and included sample code.	
136	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 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.
137	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

138	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.
139	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/or organization.
140	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.	The API is able to support parallel processing of simultaneous connections
141	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.
142	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	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/or organization.

		an overall picture of financial data.		
143	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 retrial is provided.
144	5.5.4.16.1.7	The ability to support reporting to multiple presentation modes for the output (e.g. files, screen displays, etc.). At a minimum, this shall include a user accessible dashboard and the file types PDF and CSV. This shall allow users to indicate one or more output methods for a generated report.	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 of presentation.
145	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.
146	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.
147	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.

148	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
149	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.
150	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	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.

			optional by enabling and then disabling the suspension mode and exceeding the prior set threshold.	
151	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.	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.
152	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-redact information in unauthorized domains and/or summarize data according to administrator configurable reporting policies.
153	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	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	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).

		projected total cost for a given PoP.	both current and anticipated configurations, as well as adjustments to services.	
154	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.
155	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: Reporting based on account and/or organizational structure (i.e. Enterprise, Department, Office, Team) to determine cloud spend by organizational structure and/or user. Reporting based on type of services consumed to determine spending based on type of services consumed (e.g. storage, compute, data transfer, security). Reporting based on cost to determine services' impacts to spend rate.	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).

156	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.
157	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. Additionally, the Contractor shall provide independent verification and validation of its OSCAL exports quarterly and 60 days after major OSCAL version release.	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.
158	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	Summary Requirement	N/A

		and into the cloud as detailed in sub-section 5.5.4.3 Portability Plan (CDRL A006).		
159	5.5.5.1	The Contractor shall provide the Government the ability to rapidly and securely provision/deploy first-party offerings and third-party offerings via the Contractor-provided JWCC Marketplace, as defined below, with baseline template configurations, onto JWCC infrastructure at all classification levels and ILs. Third-party offerings 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
160	5.5.5.1.1	The Contractor-provided JWCC Marketplace shall support the ability for JWCC users to deploy the first-party offerings and third-party offerings listed on the JWCC Catalog. All JWCC 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 makes them available for JWCC users to fulfill orders, provision, or deploy. 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 makes them	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.

		available on the JWCC Marketplace. The Contractor shall make all security information and process outputs available for Government audit and review.		
161	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 and BYOL at each classification level and IL, as applicable.	The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.
162	5.5.5.1.3	The Contractor shall not apply additional cost to any third-party marketplace offering. This makes all third-party offerings 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 to a third-party marketplace offering being price-free, each offering shall be approved by the JWCC KO. All third-party offerings that are available in the JWCC Marketplace shall be offered price-free and BYOL basis as appropriate, excluding the cost of IaaS resources. These 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.	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.	N/A

163	5.5.5.1.3.1	For third-party offerings 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 offerings 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.	The Government will assess whether any BYOL or price-free third-party offering has additional Terms and Conditions beyond the Government provided license.	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.
164	5.5.5.1.4	The Contractor shall ensure all third-party offerings that are available in the JWCC Marketplace support centralized/integrated billing with the Contractor.	The Government will assess whether third-party offering cost accrual is integrated into the workspace billing and does not include licensing costs/fees.	The capability will be able to integrate all billing into a single comprehensive bill that retains fidelity of user identified specific items.
165	5.5.5.1.5	JWCC users' ability to order any discrete 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/organizations/accounts.
166	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 approved offerings shall be populated within 24 hours of JWCC KO approval.	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

167	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 offering, or any combination of offerings, to enable JWCC users to properly estimate forecasted cloud spending for budgetary planning.	Summary Requirement	N/A
168	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.
169	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.

170	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).
171	5.5.5.2.4	The Contractor's Calculator shall be separately available at each classification level and IL to ensure there is no spillage related to budgets for CLASSIFIED programs. The Contractor's Calculator shall be consistent with the JWCC Contract pricing and the JWCC Catalog, based on the pricing and availability of the offerings at the classification levels and ILs 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).	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.	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).
172	5.5.5.3	The Contractor shall provide a Portability Plan (CDRL A006) as follows:	Summary Requirement	N/A

173	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 information required to equivalently replicate the operational environment.	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.
174	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 and/or reinstate all removed items to validate successful disposition after confirming data transfer completion and identify any "success", which indicates eradication failure.

175	5.5.6	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. Offerings shall include generational replacement and upgrades of hardware and software, as well as specialized hardware offerings to support advanced capabilities such that the offerings in the JWCC Catalog are the same or equivalent in form, fit, and function as the offerings made commercially available. Any exception(s) to this requirement must be approved by the JWCC KO.	Summary Requirement	N/A
176	5.5.6.1	The Contractor shall ensure the provisioning of each 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 offering at each	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

		classification level and IL such that the Government can validate provisioning performance for each offering (e.g. provisioning a new workspace, user, or service offering, or deploying such offerings within JWCC).		monitor real time operations and service status.
177	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 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 transition and availability of hardware and network generational replacements and software upgrades as they are produced/occur.
178	5.5.6.3	The Contractor's offerings available under the JWCC Contract, across each classification level and IL, 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 approved by the JWCC KO.	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.	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.

179	5.5.6.4	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).	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.	An automated report is generated which identifies all offerings' event history, including authorization lifecycle details. Additionally services are made available the same day.
180	5.5.6.5	For any of the offerings available under the JWCC Contract, across each classification level and IL, the same API calls and/or Contractor Portal (UI) actions shall result in the same expected behavior, except when restrictions due to classification level and/or IL prohibit commercial parity.	The Government may audit at any time during contract performance to determine whether API calls and/or 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.
181	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.	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.

182	5.5.6.7	All 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.
183	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
184	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 Tensor Processing Unit (TPU) processing architectures, quantum computing applications).	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.
185	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.	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.

		Any performance tiering options shall be explicitly identified in the Contractor's JWCC Catalog.		
186	5.5.7.3	The Contractor shall have more than one queryable storage offering that can support data on the order of hundreds of Terabytes, intra-availability zones, and inter-availability zones. Offering(s) shall 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 offering.	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.
187	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 information, and industry best practices.
188	5.5.7.5	When an authorized user requests a cloud resource within a Contractor's Portal (UI), or via an API, the response time shall be commensurate with the Contractor's commercial offering.	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.

189	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.
190	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
191	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
192	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 Government will inspect any data at rest and in transit to ensure that the specified encryption requirements are IAW	All data has multi-layer protection applied, while not impacting the performance profile of the operation.

		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.	C3PO. Additionally the Government will assess service offerings to ensure that encryption is configured by default.	
193	5.5.8.1.2	The Contractor shall provide multi-layer encryption for all of the Contractor's cloud service offerings 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. 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.	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.	All CSOs, including containers, have multi-layer protection applied which meets CSfC requirements and does not impact the performance profile of the operation.

194	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: JWCC user-managed encryption keys; Encryption key management as a service offering available under the JWCC Contract; and 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.	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.	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.
195	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 cloud service offerings 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)	Summary Requirement	N/A

		for both the management plane and production plan and high to low (from a higher impact/classification level to a lower impact/classification level) operations on the production plane, as described and/or required in sections 5.5.8.2.1 through 5.5.8.2.5 of this PWS.		
196	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
197	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.
198	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	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	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.

		timely, consistent, repeatable, and secure manner, and maintain commercial parity.	on the management plane.	
199	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).
200	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).
201	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 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 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.
202	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

203	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/or 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.
204	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).
205	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 and/or roles within a specific workspace and/or the cloud environment.	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.

206	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.
207	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
208	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.
209	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	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.

			response requirements.	
210	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 and/or user.
211	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/or 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 and reviewed by humans.
212	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.
213	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	Summary Requirement	N/A

		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.		
214	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
215	5.5.9.1.1	The Contractor shall provide data analytics offering 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), less exceptions 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 COR, and commensurate with the JWCC schedule ref 5.5.1.	A fully equipped AI/ML, and other analytic learning tools, suite of tools and/or platforms, to allow advanced processing of data for insight and findings. All tools are also available at the tactical edge in connected and disconnected modes.
216	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	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.

			executing a simple AI/ML pipeline.	
217	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.
218	5.5.9.1.4	The Contractor's data analytics 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.
219	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

220	5.5.10.1	The Contractor shall provide, as an offering in the JWCC Catalog, a minimum of one form factor of TE devices that is man-portable, capable of being carried and/or mounted to a vehicle, 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.	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.	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).
221	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/or up to all classification levels and ILs following the physical and logical separation requirements in C3PO.	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.	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.

222	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 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).	The TE devices are capable of modular adapter components that can be hot swapped to dynamically change the available service sets for the configuration.
223	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.	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 ability to control synchronization priority order and throttle use of available synchronization bandwidth for synchronization.	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 operational exposure is not a consideration).
224	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 further can control and/or augment the signature to lowered states without significant impact to performance.

225	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.
226	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.
227	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
228	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.	N/A
229	5.5.10.10	The Contractor shall submit authorization packages for the first unit of all variations of TE devices for	The Government will assess the current state of the TE device authorization. Any TE devices and services	All TE devices are pre-qualified with a full authorization, including the first delivery item.

		Authorization at each classification level and IL.	that have not been previously authorized must include all documentation required for the AO to authorize the device(s)/CSO(s) for use.	
230	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.	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.
231	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
232	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 offerings, including TE	Summary Requirement	N/A

		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 offerings at all classification levels and ILs.		
233	5.5.11.1	The Contractor shall provide advisory and assistance services that include integration, aggregation, orchestration, secure design, and troubleshooting of 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.

234	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: Training materials and training for all CSOs provided on the JWCC Catalog at all classification levels and ILs. Materials that help users and administrators understand how to successfully provision services and employ best practices for offerings on the JWCC Catalog users and administrators shall be able to retain such materials upon completion of the training (CDRLs A004 and A005). 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. Any training the Contractor provides shall demonstrate, through tabulated results, the relevance, thoroughness, and efficacy of the training using industry standard methods and tools. All training materials shall be current and the	The Government will assess whether the offered training and associated materials meet the following criteria: applicability and thoroughness for each service at all classification levels and ILs, including tactical edge. Provide tabulated results on relevance, thoroughness, and efficacy of training.	All training materials are equivalent between security domains, and classification levels and ILs and are fully comprehensive in content.

		Contractor shall provide updated training materials with the release of new versions of any CSO that is made available to JWCC users.		
235	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.	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.	The advisory and assistance services include multi-vendor interoperability solutioning.
236	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/or OCONUS locations. All training and support services shall be offered at the locations as described in the 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.	N/A
237	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.	N/A
238	5.5.11.6	The Contractor shall provide options for equipment repair/replacement and data recovery from TE device failure and/or performance degradation, with minimal mission impact, such as the	The Government will evaluate whether the Contractor's offered services under the JWCC Contract include TE data recovery and equipment	An immediate replacement/ recovery model for TE devices has no impact on mission operations.

		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.	repair/replacement options.	

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 Materials
A005	Role-Based User Training Materials
A006	Portability Plan
A007	Contract Ordering Guide Annex
A008	Quality Control Plan
A009	Security Authorization Package
A010	Small Business Reporting
A011	Portability Test
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	Catalog Modification Report
A023	JWCC Catalog Delivery